Cisco IronPort AsyncOS 7.1 for Web User Guide

November, 2010

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

Text Part Number: OL-23207-01
CONTENTS

CHAPTER 1

Getting Started with the Web Security Appliance 1-1

What's New in This Release 1-1

New Feature: Web Reporting and Web Tracking 1-2
New Feature: Centralized Reporting 1-2
New Feature: Anonymized Usernames on Reporting Pages 1-3
Enhanced: Reports 1-3

What's New in Version 7.0 1-3

New Feature: Cisco AnyConnect Secure Mobility 1-3
New Feature: Application Visibility and Control 1-4
New Feature: Safe Search and Site Content Rating Enforcement 1-5
New Feature: Bandwidth Control for Streaming Media 1-5
New Feature: HTTP Instant Messaging Controls 1-6
New Feature: SaaS Access Control 1-6
New Feature: Sophos Anti-Virus Scanning 1-7
New Feature: Transparent User Identification for Novell eDirectory 1-7
New Feature: Outbound Malware Scanning 1-7
New Feature: Application Scanning Bypass 1-8
New Feature: Allow User One Login at a Time 1-8
New Feature: WBRs Threat Details 1-9
New Feature: What's New In This Release 1-9
Enhanced: Per Identity Authentication Settings 1-9
Enhanced: PAC File Hosting 1-9
Enhanced: Reports 1-10
Enhanced: Advancedproxyconfig CLI Command 1-10
Contents

Enhanced: Logging 1-10
How to Use This Guide 1-11
Before You Begin 1-11
Typographic Conventions 1-12
Where to Find More Information 1-13
  Documentation Set 1-13
  IronPort Technical Training 1-13
  Knowledge Base 1-13
  Cisco Support Community 1-14
  Cisco IronPort Customer Support 1-15
  Third Party Contributors 1-15
IronPort Welcomes Your Comments 1-15
Web Security Appliance Overview 1-16

CHAPTER 2

Using the Web Security Appliance 2-1
  How the Web Security Appliance Works 2-1
    Web Proxy 2-1
    The L4 Traffic Monitor 2-2
  Administering the Web Security Appliance 2-2
    System Setup Wizard 2-3
    Accessing the Web Security Appliance 2-3
    Using the Command Line Interface (CLI) 2-4
      Using an Ethernet Connection 2-4
      Using a Serial Connection 2-5
    The SenderBase Network 2-5
      Sharing Data 2-6
    Reporting and Logging 2-6
  Navigating the Web Security Appliance Web Interface 2-7
    Logging In 2-9
Contents

Browser Requirements 2-10
Support Languages 2-10
Reporting Tab 2-11
Web Security Manager Tab 2-11
Security Services Tab 2-12
Network Tab 2-13
System Administration Tab 2-13
Committing and Clearing Changes 2-14
Committing and Clearing Changes in the Web Interface 2-14
Committing Changes 2-15
Clearing Changes 2-15
Committing and Clearing Changes in the CLI 2-16

CHAPTER 3

Deployment 3-1
Deployment Overview 3-1
Preparing for Deployment 3-2
Appliance Interfaces 3-3
Management Interface 3-4
Data Interfaces 3-4
L4 Traffic Monitor Interfaces 3-5
Example Deployment 3-5
Deploying the Web Proxy in Explicit Forward Mode 3-6
Configuring Client Applications 3-7
Connecting Appliance Interfaces 3-7
Testing an Explicit Forward Configuration 3-7
Deploying the Web Proxy in Transparent Mode 3-7
Connecting Appliance Interfaces 3-8
Connecting the Appliance to a WCCP Router 3-8
Configuring the Web Security Appliance 3-9
Contents

Configuring the WCCP Router 3-9
Example WCCP Configurations 3-11
  Example 1 3-11
  Example 2 3-12
  Example 3 3-14
Working with Multiple Appliances and Routers 3-15
Using the Web Security Appliance in an Existing Proxy Environment 3-15
  Transparent Upstream Proxy 3-15
  Explicit Forward Upstream Proxy 3-16
Deploying the L4 Traffic Monitor 3-16
  Connecting the L4 Traffic Monitor 3-17
  Configuring an L4 Traffic Monitor Wiring Type 3-18
Physical Dimensions 3-18

CHAPTER 4

Installation and Configuration 4-1
  Before You Begin 4-1
    Connecting a Laptop to the Appliance 4-2
    Connecting the Appliance to the Network 4-2
    Gathering Setup Information 4-4
      DNS Support 4-6
  System Setup Wizard 4-6
    Accessing the System Setup Wizard 4-8
    Step 1. Start 4-8
    Step 2. Network 4-9
    Step 3. Security 4-22
    Step 4. Review 4-26

CHAPTER 5

Web Proxy Services 5-1
  About Web Proxy Services 5-1
## Contents

- **Web Proxy Cache** 5-2
- **Configuring the Web Proxy** 5-3
- **Working with FTP Connections** 5-8
  - Using Authentication with Native FTP 5-9
  - Working with Native FTP in Transparent Mode 5-10
  - Configuring FTP Proxy Settings 5-11
- **Bypassing the Web Proxy** 5-15
  - How the Proxy Bypass List Works 5-17
  - Using WCCP with the Proxy Bypass List 5-18
- **Bypassing Application Scanning** 5-18
- **Proxy Usage Agreement** 5-18
- **Configuring Client Applications to Use the Web Proxy** 5-19
- **Working with PAC Files** 5-19
  - **PAC File Format** 5-21
  - Creating a PAC File for Remote Users 5-22
  - Specifying the PAC File in Browsers 5-22
  - Entering the PAC File Location 5-22
    - Detecting the PAC File Location Automatically 5-23
- **Adding PAC Files to the Web Security Appliance** 5-24
  - Specifying the PAC File URL 5-25
  - Uploading PAC Files to the Appliance 5-28
  - Understanding WPAD Compatibility with Netscape and Firefox 5-29
- **Advanced Proxy Configuration** 5-30
  - Authentication Options 5-32
  - Caching Options 5-39
  - DNS Options 5-42
  - EUN Options 5-44
  - NATIVEFTP Options 5-44
  - FTPOVERHTTP Options 5-47
CHAPTER 6

Working with Policies 6-1

Working with Policies Overview 6-1

Policy Types 6-3
  Identities 6-3
  Decryption Policies 6-4
  Routing Policies 6-4
  Access Policies 6-4
  IronPort Data Security Policies 6-5
  External DLP Policies 6-5
  Outbound Malware Scanning Policies 6-6
  SaaS Application Authentication Policies 6-6

Working with Policy Groups 6-6
  Creating Policy Groups 6-7
  Using the Policies Tables 6-7

Policy Group Membership 6-10
  Authenticating Users versus Authorizing Users 6-10
    Working with Failed Authentication and Authorization 6-11
  Working with All Identities 6-12
  Policy Group Membership Rules and Guidelines 6-12

Working with Time Based Policies 6-13
  Creating Time Ranges 6-14

Working with User Agent Based Policies 6-16
  Configuring User Agents for Policy Group Membership 6-16
  Exempting User Agents from Authentication 6-18
CHAPTER 7

Identities 7-1

Identities Overview 7-1

Evaluating Identity Group Membership 7-2

Understanding How Authentication Affects Identity Groups 7-4

Understanding How Authentication Affects HTTPS and FTP over HTTP Requests 7-6

Understanding How Authentication Scheme Affects Identity Groups 7-9

Matching Client Requests to Identity Groups 7-10

Allowing Guest Access to Users Who Fail Authentication 7-13

Identifying Users Transparently 7-16

Understanding Transparent User Identification 7-17

Rules and Guidelines 7-18

Configuring Transparent User Identification 7-19

Creating Identities 7-20

Configuring Identities in Other Policy Groups 7-28

Example Identity Policies Tables 7-31

Example 1 7-31

Example 2 7-33

CHAPTER 8

Access Policies 8-1

Access Policies Overview 8-1

Access Policy Groups 8-2

Understanding the Monitor Action 8-3

Evaluating Access Policy Group Membership 8-4

Matching Client Requests to Access Policy Groups 8-5

Creating Access Policies 8-7

Controlling HTTP and Native FTP Traffic 8-11

Tracing Policies 6-18
Protocols and User Agents  8-14
URL Categories  8-15
Applications  8-15
Object Blocking  8-16
Web Reputation and Anti-Malware  8-17
Blocking Specific Applications and Protocols  8-18
Blocking on Port 80  8-18
  Policy: Protocols and User Agents  8-18
  Policy: URL Categories  8-20
  Policy: Objects  8-21
Blocking on Ports Other Than 80  8-21

CHAPTER  9
Working with External Proxies  9-1
  Working with External Proxies Overview  9-1
  Routing Traffic to Upstream Proxies  9-2
  Adding External Proxy Information  9-3
  Evaluating Routing Policy Group Membership  9-5
    Matching Client Requests to Routing Policy Groups  9-6
  Creating Routing Policies  9-8

CHAPTER  10
Decryption Policies  10-1
  Decryption Policies Overview  10-1
    Decryption Policy Groups  10-3
    Personally Identifiable Information Disclosure  10-4
    Understanding the Monitor Action  10-5
  Digital Cryptography Terms  10-6
  HTTPS Basics  10-8
    SSL Handshake  10-9
  Digital Certificates  10-9
<table>
<thead>
<tr>
<th>Chapter 10</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Validating Certificate Authorities</strong></td>
<td>10-10</td>
</tr>
<tr>
<td><strong>Validating Digital Certificates</strong></td>
<td>10-12</td>
</tr>
<tr>
<td><strong>Decrypting HTTPS Traffic</strong></td>
<td>10-13</td>
</tr>
<tr>
<td>- <strong>Mimicking the Server Digital Certificate</strong></td>
<td>10-15</td>
</tr>
<tr>
<td>- <strong>Working with Root Certificates</strong></td>
<td>10-16</td>
</tr>
<tr>
<td>- <strong>Using Decryption with the AVC Engine</strong></td>
<td>10-19</td>
</tr>
<tr>
<td>- <strong>Using Decryption with AOL Instant Messenger</strong></td>
<td>10-19</td>
</tr>
<tr>
<td>- <strong>Converting Certificate and Key Formats</strong></td>
<td>10-20</td>
</tr>
<tr>
<td><strong>Enabling the HTTPS Proxy</strong></td>
<td>10-21</td>
</tr>
<tr>
<td><strong>Evaluating Decryption Policy Group Membership</strong></td>
<td>10-27</td>
</tr>
<tr>
<td>- <strong>Matching Client Requests to Decryption Policy Groups</strong></td>
<td>10-28</td>
</tr>
<tr>
<td><strong>Creating Decryption Policies</strong></td>
<td>10-30</td>
</tr>
<tr>
<td><strong>Controlling HTTPS Traffic</strong></td>
<td>10-34</td>
</tr>
<tr>
<td><strong>Importing a Trusted Root Certificate</strong></td>
<td>10-37</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 11</th>
<th>Outbound Malware Scanning 11-1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Outbound Malware Scanning Overview</strong></td>
<td>11-1</td>
</tr>
<tr>
<td>- <strong>User Experience with Blocked Requests</strong></td>
<td>11-2</td>
</tr>
<tr>
<td>- <strong>Outbound Malware Scanning Policy Groups</strong></td>
<td>11-2</td>
</tr>
<tr>
<td><strong>Evaluating Outbound Malware Scanning Policy Group Membership</strong></td>
<td>11-3</td>
</tr>
<tr>
<td>- <strong>Matching Client Requests to Outbound Malware Scanning Policy Groups</strong></td>
<td>11-4</td>
</tr>
<tr>
<td><strong>Creating Outbound Malware Scanning Policies</strong></td>
<td>11-6</td>
</tr>
<tr>
<td><strong>Controlling Upload Requests Using Outbound Malware Scanning Policies</strong></td>
<td>11-11</td>
</tr>
<tr>
<td><strong>Logging</strong></td>
<td>11-14</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 12</th>
<th>Data Security and External DLP Policies 12-1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Security and External DLP Policies Overview</strong></td>
<td>12-1</td>
</tr>
<tr>
<td>- <strong>Bypassing Upload Requests Below a Minimum Size</strong></td>
<td>12-3</td>
</tr>
</tbody>
</table>
User Experience with Blocked Requests  12-3
Working with Data Security and External DLP Policies  12-4
  Data Security Policy Groups  12-4
  External DLP Policy Groups  12-6
Evaluating Data Security and External DLP Policy Group Membership  12-7
  Matching Client Requests to Data Security and External DLP Policy Groups  12-8
Creating Data Security and External DLP Policies  12-10
Controlling Upload Requests Using IronPort Data Security Policies  12-15
  URL Categories  12-17
  Web Reputation  12-17
  Content Blocking  12-17
Defining External DLP Systems  12-20
Controlling Upload Requests Using External DLP Policies  12-25
Logging  12-27

CHAPTER 13  Achieving Secure Mobility  13-1
  Achieving Secure Mobility Overview  13-1
  Working with Remote Users  13-2
  Enabling Secure Mobility  13-3
  Transparently Identifying Remote Users  13-5
  Logging  13-6
  Configuring Secure Mobility Using the CLI  13-7

CHAPTER 14  Controlling Access to SaaS Applications  14-1
  SaaS Access Control Overview  14-1
  Understanding How SaaS Access Control Works  14-2
    Authenticating SaaS Users  14-4
Contents

Authentication Requirements  14-4
Enabling SaaS Access Control  14-5
   Understanding the Single Sign-On URL  14-5
Using SaaS Access Control with Multiple Appliances  14-6
Configuring the Appliance as an Identity Provider  14-7
Creating SaaS Application Authentication Policies  14-11

CHAPTER  15
Notifying End Users  15-1
   Notifying End Users of Organization Policies  15-1
   Configuring General Settings for Notification Pages  15-3
   Working With IronPort End-User Notification Pages  15-5
      Configuring IronPort Notification Pages  15-5
      Editing IronPort Notification Pages  15-8
         Rules and Guidelines for Editing IronPort Notification Pages  15-12
         Using Variables in Customized IronPort Notification Pages  15-13
      Working with User Defined End-User Notification Pages  15-14
         Configuring User Defined End-User Notification Pages  15-17
   End-User Acknowledgement Page  15-18
      Configuring the End-User Acknowledgement Page  15-20
   Configuring the End-User URL Filtering Warning Page  15-21
   Working with IronPort FTP Notification Messages  15-23
   Custom Text in Notification Pages  15-23
      Supported HTML Tags in Notification Pages  15-23
      Custom Text and Logos: Authentication, and End-User Acknowledgement Pages  15-24
Notifying End Users  15-1
   Notifying End Users of Organization Policies  15-1
   Configuring General Settings for Notification Pages  15-3
   Working With IronPort End-User Notification Pages  15-5
      Configuring IronPort Notification Pages  15-5
      Editing IronPort Notification Pages  15-8
         Rules and Guidelines for Editing IronPort Notification Pages  15-12
         Using Variables in Customized IronPort Notification Pages  15-13
      Working with User Defined End-User Notification Pages  15-14
         Configuring User Defined End-User Notification Pages  15-17
   End-User Acknowledgement Page  15-18
      Configuring the End-User Acknowledgement Page  15-20
   Configuring the End-User URL Filtering Warning Page  15-21
   Working with IronPort FTP Notification Messages  15-23
   Custom Text in Notification Pages  15-23
      Supported HTML Tags in Notification Pages  15-23
      Custom Text and Logos: Authentication, and End-User Acknowledgement Pages  15-24
Notification Page Types  15-25

CHAPTER  16
URL Filters  16-1
   URL Filters Overview  16-1
Dynamic Content Analysis Engine 16-3
Uncategorized URLs 16-4
Matching URLs to URL Categories 16-4
The URL Categories Database 16-5
Configuring the URL Filtering Engine 16-5
Filtering Transactions Using URL Categories 16-6
  Configuring URL Filters for Access Policy Groups 16-7
  Configuring URL Filters for Decryption Policy Groups 16-10
  Configuring URL Filters for Data Security Policy Groups 16-13
Custom URL Categories 16-16
Filtering Adult Content 16-20
  Logging Adult Content Access 16-22
Redirecting Traffic 16-23
Warning Users and Allowing Them to Continue 16-24
  User Experience When Warning Users 16-26
Creating Time Based URL Filters 16-26
Viewing URL Filtering Activity 16-27
  Understanding Unfiltered and Uncategorized Data 16-28
  Access Log File 16-28
Regular Expressions 16-28
  Forming Regular Expressions 16-29
  Regular Expression Character Table 16-30
URL Category Descriptions 16-32

Understanding Application Visibility and Control 17-1
Controlling Applications Overview 17-1
  User Experience with Blocked Requests 17-3
AVC Engine Updates 17-3
Enabling the AVC Engine 17-3
# Table of Contents

## Understanding Application Control Settings  17-4
- Working with Browse View  17-5
- Working with Search View  17-7
- Rules and Guidelines  17-9
- Configuring Application Control Settings  17-9

## Controlling Bandwidth  17-11
- Configuring Overall Bandwidth Limits  17-11
- Configuring User Bandwidth Limits  17-12
  - Configuring the Default Bandwidth Limit for an Application Type  17-13
  - Overriding the Default Bandwidth Limit for an Application Type  17-13
  - Configuring Bandwidth Controls for an Application  17-15

## Controlling Instant Messaging Traffic  17-17

## Viewing AVC Activity  17-19

## Access Log File  17-19

---

# Chapter 18

## Web Reputation Filters  18-1

### Web Reputation Filters Overview  18-1
- The Web Reputation Database  18-1
  - Maintaining the Database Tables  18-2

### Web Reputation Scores  18-2

### Enabling Web Reputation Filters  18-3

### Understanding How Web Reputation Filtering Works  18-4
- Web Reputation in Access Policies  18-4
- Web Reputation in Decryption Policies  18-5

### Configuring Web Reputation Scores  18-5
- Configuring Web Reputation for Access Policies  18-6
- Configuring Web Reputation for Decryption Policies  18-7
- Configuring Web Reputation for IronPort Data Security Policies  18-8

### Viewing Web Reputation Filtering Activity  18-9
CHAPTER 19

Anti-Malware Services 19-1

Anti-Malware Overview 19-1
   Malware Category Descriptions 19-2
IronPort DVS™ (Dynamic Vectoring and Streaming) Engine 19-4
   Maintaining the Database Tables 19-5
   Understanding How the DVS Engine Works 19-5
Working with Multiple Malware Verdicts 19-6
   Different Scanning Engines 19-6
   Same Scanning Engine 19-6
Webroot Scanning 19-7
McAfee Scanning 19-8
   Matching Virus Signature Patterns 19-8
   Heuristic Analysis 19-9
   McAfee Categories 19-9
Sophos Scanning 19-10
Configuring Anti-Malware Scanning 19-10
Viewing Anti-Malware Scanning Activity 19-15
   Monitoring Scanning Activity 19-15
   Access Log File 19-15

CHAPTER 20

Authentication 20-1

Authentication Overview 20-1
   Client Application Support 20-3
   Working with Upstream Proxy Servers 20-3
   Authenticating Users 20-4
   Working with Failed Authentication 20-4
Understanding How Authentication Works 20-5
  Basic versus NTLMSSP Authentication Schemes 20-7
How Web Proxy Deployment Affects Authentication 20-8
  Explicit Forward Deployment, Basic Authentication 20-9
  Transparent Deployment, Basic Authentication 20-10
  Explicit Forward Deployment, NTLM Authentication 20-12
  Transparent Deployment, NTLM Authentication 20-13
Working with Authentication Realms 20-14
  Creating Authentication Realms 20-15
  Editing Authentication Realms 20-15
  Deleting Authentication Realms 20-16
Working with Authentication Sequences 20-16
  Creating Authentication Sequences 20-17
  Editing Authentication Sequences 20-18
  Deleting Authentication Sequences 20-19
Appliance Behavior with Multiple Authentication Realms 20-19
Testing Authentication Settings 20-20
  Testing Process 20-21
    LDAP Testing 20-21
    NTLM Testing 20-21
  Testing Authentication Settings in the Web Interface 20-22
  Testing Authentication Settings in the CLI 20-23
Configuring Global Authentication Settings 20-23
  Sending Authentication Credentials Securely 20-37
    Uploading Certificates and Keys to Use with Credential Encryption and SaaS Access Control 20-38
    Accessing HTTPS and FTP Sites with Credential Encryption Enabled 20-38
  Allowing Users to Re-Authenticate 20-39
    Using Re-Authentication with Internet Explorer 20-40
Contents

Using Re-Authentication with PAC Files  20-41
Tracking Authenticated Users  20-42
LDAP Authentication  20-43
  Changing Active Directory Passwords  20-43
  LDAP Authentication Settings  20-44
  LDAP Group Authorization  20-47
NTLM Authentication  20-51
  Working with Multiple Active Directory Domains  20-51
  NTLM Authentication Settings  20-52
  Joining the Active Directory Domain  20-53
Supported Authentication Characters  20-56
  Active Directory Server Supported Characters  20-56
  LDAP Server Supported Characters  20-58

CHAPTER  21
L4 Traffic Monitor  21-1
  About L4 Traffic Monitor  21-1
  How the L4 Traffic Monitor Works  21-1
  The L4 Traffic Monitor Database  21-3
  Configuring the L4 Traffic Monitor  21-3
    Configuring L4 Traffic Monitor Global Settings  21-4
      Updating L4 Traffic Monitor Anti-Malware Rules  21-4
    Configuring L4 Traffic Monitor Policies  21-5
      Valid Formats  21-8
  Viewing L4 Traffic Monitor Activity  21-9
    Monitoring Activity and Viewing Summary Statistics  21-9
    L4 Traffic Monitor Log File Entries  21-10

CHAPTER 22
Reporting  22-1
  Reporting Overview  22-1
Contents

Working with Usernames in Reports 22-2
Report Pages 22-2
Using the Reporting Tab 22-3
Changing the Time Range 22-3
Searching Data 22-5
Working with Columns on Report Pages 22-5
Configuring Columns on Report Pages 22-8
Printing and Exporting Reports from Report Pages 22-10
Exporting Report Data 22-10
Enabling Centralized Reporting 22-12
Scheduling Reports 22-13
Adding a Scheduled Report 22-13
Editing Scheduled Reports 22-15
Deleting Scheduled Reports 22-15
On-Demand Reports 22-15
Archiving Reports 22-16
SNMP Monitoring 22-16
MIB Files 22-17
Hardware Objects 22-18
Hardware Traps 22-18
SNMP Traps 22-19
CLI Example 22-20

CHAPTER 23
Web Security Appliance Reports 23-1
Web Security Appliance Reports Overview 23-2
Overview Page 23-2
Users Page 23-5
User Details Page 23-7
Web Sites Page 23-10
URL Categories Page  23-12
  Using The URL Categories Page in Conjunction with Other Reporting Pages  23-16
Application Visibility Page  23-16
Anti-Malware Page  23-18
  Malware Category Report Page  23-20
  Malware Threat Report Page  23-21
Client Malware Risk Page  23-22
  Client Detail Page  23-24
Web Reputation Filters Page  23-29
L4 Traffic Monitor Data Page  23-31
Reports by User Location Page  23-33
Web Tracking Page  23-35
System Capacity Page  23-40
  How to Interpret the Data You See on System Capacity Page  23-43
System Status Page  23-44

CHAPTER  24  Logging  24-1
  Logging Overview  24-1
    Log File Types  24-2
    Web Proxy Logging  24-8
  Working with Log Subscriptions  24-9
    Log File Name and Appliance Directory Structure  24-11
    Rolling Over Log Subscriptions  24-11
    Working with Compressed Log Files  24-12
    Viewing the Most Recent Log Files  24-13
    Configuring Host Keys  24-13
    Adding and Editing Log Subscriptions  24-14
    Deleting a Log Subscription  24-19
Access Log File 24-19
  Transaction Result Codes 24-23
  ACL Decision Tags 24-24
  Understanding Scanning Verdict Information 24-30
    Web Reputation Filters Example 24-34
    Anti-Malware Request Example 24-35
    Anti-Malware Response Example 24-35
W3C Compliant Access Logs 24-36
  W3C Log File Headers 24-37
    Working with Log Fields in W3C Access Logs 24-38
Custom Formatting in Access Logs and W3C Logs 24-39
  Configuring Custom Formatting in Access Logs 24-49
  Configuring Custom Formatting in W3C Logs 24-50
Including HTTP/HTTPS Headers in Log Files 24-51
Malware Scanning Verdict Values 24-52
Traffic Monitor Log 24-53
Troubleshooting 24-54

CHAPTER 25
Configuring Network Settings 25-1
  Changing the System Hostname 25-1
  Configuring Network Interfaces 25-2
    Configuring the Data Interfaces 25-3
    Configuring the Network Interfaces from the Web Interface 25-5
  Configuring TCP/IP Traffic Routes 25-7
    Modifying the Default Route 25-7
    Working With Routing Tables 25-8
  Virtual Local Area Networks (VLANs) 25-9
    VLANs and Physical Ports 25-11
    Managing VLANs 25-11
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>Configuring Transparent Redirection</td>
<td>25-17</td>
</tr>
<tr>
<td></td>
<td>Working with WCCP Services</td>
<td>25-17</td>
</tr>
<tr>
<td></td>
<td>Working with the Assignment Method</td>
<td>25-18</td>
</tr>
<tr>
<td></td>
<td>Working with the Forwarding and Return Method</td>
<td>25-19</td>
</tr>
<tr>
<td></td>
<td>IP Spoofing when Using WCCP</td>
<td>25-20</td>
</tr>
<tr>
<td></td>
<td>Adding and Editing a WCCP Service</td>
<td>25-21</td>
</tr>
<tr>
<td></td>
<td>Deleting a WCCP Service</td>
<td>25-25</td>
</tr>
<tr>
<td></td>
<td>Configuring SMTP Relay Hosts</td>
<td>25-26</td>
</tr>
<tr>
<td></td>
<td>Configuring SMTP from the Web Interface</td>
<td>25-26</td>
</tr>
<tr>
<td></td>
<td>Configuring SMTP from the CLI</td>
<td>25-27</td>
</tr>
<tr>
<td></td>
<td>Configuring DNS Server(s)</td>
<td>25-28</td>
</tr>
<tr>
<td></td>
<td>Specifying DNS Servers</td>
<td>25-28</td>
</tr>
<tr>
<td></td>
<td>Split DNS</td>
<td>25-28</td>
</tr>
<tr>
<td></td>
<td>Using the Internet Root Servers</td>
<td>25-29</td>
</tr>
<tr>
<td></td>
<td>Multiple Entries and Priority</td>
<td>25-29</td>
</tr>
<tr>
<td></td>
<td>DNS Alert</td>
<td>25-30</td>
</tr>
<tr>
<td></td>
<td>Clearing the DNS Cache</td>
<td>25-30</td>
</tr>
<tr>
<td></td>
<td>Configuring DNS</td>
<td>25-30</td>
</tr>
</tbody>
</table>

**CHAPTER 26**

**System Administration** | 26-1

- Managing the S-Series Appliance | 26-1
- Saving and Loading the Appliance Configuration | 26-2
- Committing Changes to the Appliance Configuration | 26-3
- Support Commands | 26-3
- Open a Support Case | 26-3
- Remote Access | 26-5
- Packet Capture | 26-6
<table>
<thead>
<tr>
<th>Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting a Packet Capture</td>
<td>26-7</td>
</tr>
<tr>
<td>Editing Packet Capture Settings</td>
<td>26-7</td>
</tr>
<tr>
<td>Working with Feature Keys</td>
<td>26-10</td>
</tr>
<tr>
<td>Feature Keys Page</td>
<td>26-10</td>
</tr>
<tr>
<td>Feature Key Settings Page</td>
<td>26-11</td>
</tr>
<tr>
<td>Expired Feature Keys</td>
<td>26-12</td>
</tr>
<tr>
<td>Administering User Accounts</td>
<td>26-12</td>
</tr>
<tr>
<td>Managing Local Users</td>
<td>26-13</td>
</tr>
<tr>
<td>Adding Local Users</td>
<td>26-14</td>
</tr>
<tr>
<td>Deleting Users</td>
<td>26-15</td>
</tr>
<tr>
<td>Editing Users</td>
<td>26-15</td>
</tr>
<tr>
<td>Changing Passwords</td>
<td>26-16</td>
</tr>
<tr>
<td>Monitoring Users from the CLI</td>
<td>26-16</td>
</tr>
<tr>
<td>Using External Authentication</td>
<td>26-17</td>
</tr>
<tr>
<td>Configuring Administrator Settings</td>
<td>26-20</td>
</tr>
<tr>
<td>Configuring Custom Text at Login</td>
<td>26-20</td>
</tr>
<tr>
<td>Configuring IP-Based Administrator Access</td>
<td>26-20</td>
</tr>
<tr>
<td>Configuring the SSL Ciphers for Administrator Access</td>
<td>26-21</td>
</tr>
<tr>
<td>Configuring the Return Address for Generated Messages</td>
<td>26-21</td>
</tr>
<tr>
<td>Managing Alerts</td>
<td>26-22</td>
</tr>
<tr>
<td>Alerting Overview</td>
<td>26-22</td>
</tr>
<tr>
<td>Alerts: Alert Recipients, Alert Classifications, and Severities</td>
<td>26-23</td>
</tr>
<tr>
<td>Alert Settings</td>
<td>26-24</td>
</tr>
<tr>
<td>IronPort AutoSupport</td>
<td>26-25</td>
</tr>
<tr>
<td>Alert Messages</td>
<td>26-25</td>
</tr>
<tr>
<td>Alert From Address</td>
<td>26-25</td>
</tr>
<tr>
<td>Alert Subject</td>
<td>26-25</td>
</tr>
<tr>
<td>Example Alert Message</td>
<td>26-26</td>
</tr>
<tr>
<td>Managing Alert Recipients</td>
<td>26-27</td>
</tr>
<tr>
<td>Adding New Alert Recipients</td>
<td>26-27</td>
</tr>
</tbody>
</table>
Contents

- Configuring Existing Alert Recipients 26-28
- Deleting Alert Recipients 26-28
- Configuring Alert Settings 26-29
- Editing Alert Settings 26-29

Setting System Time 26-30
- Selecting a Time Zone 26-30
- Editing System Time 26-31
- Configure NTP (Network Time Protocol) 26-31
- Manually Setting System Time 26-32

Installing a Server Digital Certificate 26-32
- Obtaining Certificates 26-33
- Intermediate Certificates 26-34
- Uploading Certificates to the Web Security Appliance 26-35

Upgrading the System Software 26-40
- Upgrading AsyncOS for Web from the Web Interface 26-40
- Upgrading AsyncOS for Web from the CLI 26-41
- Differences from Traditional Upgrading Method 26-41

Configuring Upgrade and Service Update Settings 26-42
- Updating and Upgrading from the IronPort Update Servers 26-43
- Configuring a Static Address for the IronPort Update Servers 26-44
- Upgrading from a Local Server 26-44
- Hardware and Software Requirements for Local Upgrade Servers 26-46
- Configuring the Update and Upgrade Settings from the Web Interface 26-46
- Configuring the Update and Upgrade Settings from the CLI 26-51
- Manually Updating Security Service Components 26-51

CHAPTER 27

Command Line Interface 27-1
- The Command Line Interface Overview 27-1
- Using the Command Line Interface 27-1
Getting Started with the Web Security Appliance

The *IronPort AsyncOS for Web User Guide* provides instructions for setting up, administering, and monitoring the IronPort Web Security appliance. These instructions are designed for an experienced system administrator with knowledge of networking and web administration.

This chapter discusses the following topics:

- What’s New in This Release, page 1-1
- What’s New in Version 7.0, page 1-3
- How to Use This Guide, page 1-11
- Web Security Appliance Overview, page 1-16

What’s New in This Release

This section describes the new features and enhancements in AsyncOS for Web 7.1. For more information about the release, see the product release notes, which are available on the Cisco IronPort Customer Support site at the following URL:


Note: You need a Cisco.com User ID to access the site. If you do not have a Cisco.com User ID, you can register for one here:

You might also find it useful to review release notes for earlier releases to see the features and enhancements that were previously added.

**New Feature: Web Reporting and Web Tracking**

AsyncOS for Web 7.1 supports advanced web reporting and web tracking. Web reporting and tracking aggregates information from individual security components as well as acceptable use enforcement components and records data that can be used to monitor your web traffic patterns and security risks. Web reporting and tracking gives managers visibility and insight into current operational data to help them refine policies, plan infrastructure, and measure productivity.

You can run reports in real time to view an interactive display of system activity over a specific period of time, or you can schedule reports and run them at regular intervals. You can also export raw data to a file.

To use web reporting and tracking, use the Reporting > Web Tracking page.

For more information, see [Web Tracking Page, page 23-35](#).

**New Feature: Centralized Reporting**

AsyncOS for Web 7.1 includes the Centralized Reporting feature which, when the Web Security appliance is managed by a Security Management appliance, allows you to configure the Web Security appliance so that the Security Management appliance maintains the reports.


When you enable Centralized Reporting, only the System Capacity and System Status reports are available on the Web Security appliance. To view the other reports, connect to the Security Management appliance. The Web Security appliance no longer stores data for the other reports.

For more information, see [Enabling Centralized Reporting, page 22-12](#).
Chapter 1    Getting Started with the Web Security Appliance

What’s New in Version 7.0

New Feature: Anonymized Usernames on Reporting Pages

AsyncOS for Web 7.1 allows you to make usernames unrecognizable in all reports. Configure this on the Security Services > Reporting page using the Anonymize usernames in reports setting. However, administrators always see usernames.

Enhanced: Reports

AsyncOS for Web 7.1 includes the following new reports:

- Users
- Web Sites
- Web Tracking

It also includes updated information for many existing reports.

Due to all the reporting changes, when you upgrade to AsyncOS 7.1 for Web, all historical data stored on the Web Security appliance for the on-box reports will be erased. For more information, see the release notes.

For more information, see Chapter 23, ‘Web Security Appliance Reports’.

What’s New in Version 7.0

This section describes new features and enhancements added in the AsyncOS 7.0 for Web release.

New Feature: Cisco AnyConnect Secure Mobility

AsyncOS for Web 7.0 includes support for Cisco Secure Mobility Solution which extends the network perimeter to remote endpoints, enabling the seamless integration of web filtering services offered by the Web Security appliance. Secure Mobility Solution is a collection of features across multiple Cisco products that restores security and control in borderless networks. The Cisco
products that work with Secure Mobility Solution are the Cisco IronPort Web Security appliance, Cisco ASA 5500 series adaptive security appliance, and Cisco AnyConnect secure mobility client.

Using Secure Mobility Solution, mobile and remote users have a seamless experience and are always protected from risks as if they were local users connected within the network.

When Secure Mobility Solution is enabled on the Web Security appliance, you can distinguish remote users from local users. This allows you to perform the following tasks:

- Create Identities and other policies for remote users.
- View reports for remote traffic.
- Enable single sign-on (SSO) for remote users.

To protect remote users using always-on security, first you must enable the Secure Mobility Solution feature on the Web Security appliance. When Secure Mobility Solution is enabled, you can distinguish between remote users from local users when creating Identities.

For more information, see Achieving Secure Mobility, page 13-1.

**New Feature: Application Visibility and Control**

AsyncOS for Web 7.0 enhances the Cisco IronPort Web Usage Controls platform to include the Application Visibility and Control engine (AVC engine) which enables administrators to apply deeper controls to particular application types. The AVC engine is an acceptable use policy component that inspects web traffic to gain deeper understanding and control of web traffic used for applications. Application control gives you more granular control over web traffic than just URL filtering. For example, you can block streaming media from sports sites, but not news sites.

To control applications using the AVC engine, enable the AVC engine when you enable Cisco IronPort Web Usage Controls, and then define application control settings in the Access Policies.

For more information, see Understanding Application Visibility and Control, page 17-1.
New Feature: Safe Search and Site Content Rating Enforcement

AsyncOS for Web 7.0 uses the AVC engine to filter adult content from some web searches and websites. You might want to do this to allow access to these sites, such as google.com and youtube.com, while still restricting potentially unsafe content from reaching users.

AsyncOS for Web offers the following features to filter adult content:

- **Enforce safe searches.** Most search engines allow the safe search feature to be enabled and disabled by end users. You can configure the Web Security appliance so that outgoing search requests appear to search engines as safe search requests. This gives the control to an administrator on the network instead of the end user. You might want to do this to prevent users from bypassing acceptable use policies using search engines.

- **Enforce site content ratings.** Many content sharing sites that serve user-generated photos and videos classify some of their content as adult. They allow users to restrict their own access to the adult content on these sites by either enforcing their own safe search feature or blocking access to adult content, or both. This classification feature is commonly called content ratings.

To enforce safe searches and site content ratings, configure the URL filtering settings for an Access Policy.

For more information, see Filtering Adult Content, page 16-20.

New Feature: Bandwidth Control for Streaming Media

AsyncOS for Web 7.0 uses the AVC engine to control the amount of bandwidth used for streaming media applications. You can define an overall bandwidth limit and per user bandwidth limits. When both the overall limit and user limit applies to a transaction, the most restrictive option applies.

For more information, see Controlling Bandwidth, page 17-11.
New Feature: HTTP Instant Messaging Controls

AsyncOS for Web 7.0 uses the AVC engine to apply control settings to some instant messenger (IM) traffic that runs on top of HTTP. You can block or monitor the IM traffic, and depending on the IM service, you can block particular activities (also known as application behaviors) in an IM session. For example, you can allow an IM session with a particular IM service provider, but block file transfers within that session.

You control IM traffic by configuring Instant Messenger application settings on the Applications Visibility and Control page of Access Policies.

For more information, see Controlling Instant Messaging Traffic, page 17-17.

New Feature: SaaS Access Control

AsyncOS for Web 7.0 includes the SaaS Access Control feature which provides IT administrators with seamless, secure controls necessary for managing access to Software as a Service (SaaS) applications and enforcing security policies. SaaS Access Control allows IT administrators to easily control authentication and authorization for users who need to access SaaS applications.

When you enable Cisco SaaS Access Control, users log into the configured SaaS applications using their network authentication user credentials. That means they use the same user name and password for all SaaS applications as well as network access. You can choose whether users are transparently signed in (single sign-on functionality) or prompted to enter their authentication user name and password.

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

To enable SaaS Access Control, you must configure settings on both the Web Security appliance and the SaaS application. It is very important that the settings you configure on the appliance and SaaS application match each other appropriately.

For more information, see Controlling Access to SaaS Applications, page 14-1.
New Feature: Sophos Anti-Virus Scanning

AsyncOS for Web 7.0 adds the Sophos scanning engine to the list of possible Web Security appliance on-box anti-malware scanning engines. The Sophos engine offers award-winning protection against known and unknown threats using their Genotype and Behavioral Genotype Protection. The Sophos Genotype virus detection technology proactively blocks families of viruses, and Behavioral Genotype Protection automatically guards against zero-day threats by analyzing the behavior of the code before it executes—offering protection from new and existing viruses, trojans, worms, spyware, adware, and other potentially unwanted applications (PUAs).

For more information, see Sophos Scanning, page 19-10.

New Feature: Transparent User Identification for Novell eDirectory

AsyncOS for Web 7.0 allows you to configure the Web Security appliance so that it identifies users by an authenticated user name transparently—that is, without prompting the end user. You might want to do this to:

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

To identify users transparently, you must define at least one LDAP authentication realm that supports Novell eDirectory.

For more information, see Identifying Users Transparently, page 7-16.

New Feature: Outbound Malware Scanning

AsyncOS for Web 7.0 includes protects data and objects leaving the network by providing outbound malware scanning. The IronPort Dynamic Vectoring and Streaming (DVS) engine scans transaction requests as they leave the network in real-time. By working with the IronPort DVS engine, the Web Security appliance allows you to prevent users from unintentionally uploading malicious data.
To restrict malicious data from leaving the network, the Web Security appliance provides the Outbound Malware Scanning policy groups. You define which uploads are scanned for malware, which anti-malware scanning engines to use for scanning, and which malware types to block.

For more information, see Outbound Malware Scanning, page 11-1.

**New Feature: Application Scanning Bypass**

AsyncOS for Web 7.0 allows administrators to easily bypass certain web applications from being scanned by the Web Proxy by checking a checkbox. This can prevent integration issues with web applications that do not interact well with proxies. In version 7.0, you can bypass scanning for Cisco Webex.

For more information, see Bypassing Application Scanning, page 5-18.

**New Feature: Allow User One Login at a Time**

AsyncOS for Web 7.0 allows administrators to control whether or not an authenticated user can access the Internet from multiple machines simultaneously. 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.

To restrict an authenticated user from accessing the Internet from a different machine, configure the User Session Restrictions settings on the Network > Authentication page.

For more information, see Configuring Global Authentication Settings, page 20-23.
New Feature: WBRS Threat Details

AsyncOS for Web 7.0 now provides additional details on the threat which caused a site to have a low reputation. This information is included in end-user notification pages when a user is blocked due to low reputation, as well as the access logs. There is also a new report which displays information on how many transactions have been blocked due to each threat type.

New Feature: What’s New In This Release

AsyncOS for Web 7.0 now provides a way to easily view which features are new or enhanced in the current version of AsyncOS. To do this, choose New in this Release from the Support and Help menu.

Enhanced: Per Identity Authentication Settings

AsyncOS for Web 7.0 now allows you to define authentication surrogate type settings (either cookie or IP address) per Identity instead of globally for all Identities.

You might want to define different surrogate types for different Identities if you want to use IP addresses for almost all users, but use cookie surrogates on systems like kiosks which are shared among many users.

For more information, see Creating Identities, page 7-20.

Enhanced: PAC File Hosting

Effective in AsyncOS for Web 7.0, you can use any port to serve PAC files stored on the Web Security appliance. In previous versions, you could only specify ports for serving PAC files that were not listed as an HTTP port to proxy on the Security Services > Web Proxy page.

For more information, see Adding PAC Files to the Web Security Appliance, page 5-24.
Enhanced: Reports

AsyncOS for Web 7.0 includes the following new reports:

- Application Visibility
- Reports by User Location
- System Capacity

It also includes updated information for many existing reports.

For more information, see Application Visibility page, page 23-16, Reports by User Location page, page 23-33, and System Capacity page, page 23-40.

Enhanced: Advanced proxyconfig CLI Command

AsyncOS for Web 7.0 includes many new commands for fine tuning the Web Proxy and how it handles transactions. For example, you can configure the Web Proxy so that matching LDAP usernames is not case sensitive when matching policy groups to a transaction.

For more information, see Advanced Proxy Configuration, page 5-30.

Enhanced: Logging

AsyncOS 7.0 for Web includes the following new types of log files:

- **AVC Engine Logs.** Records debug messages from the AVC engine.
- **AVC Engine Framework Logs.** Records messages related to communication between the Web Proxy and the AVC engine.
- **Mobile User Security Daemon Logs.** Records the interaction between the Web Security appliance and the AnyConnect client, including the status check.
- **SaaS Auth Logs.** Records messages related to the SaaS Access Control feature.
- **Sophos Logs.** Records the status of anti-malware scanning activity from the Sophos scanning engine.
Chapter 1      Getting Started with the Web Security Appliance

How to Use This Guide

How to Use This Guide

- **Sophos Integration Framework Logs.** Records messages related to communication between the Web Proxy and the Sophos scanning engine.

- **UDS Logs.** 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 Solution as well as integrating with the Novell eDirectory server for transparent user identification.

Also, new log fields are available in the access logs and W3C access logs for AVC engine and WBRS threat details.

For more information, see Chapter 24, 'Logging,' on page 1.

Before You Begin

Before you read this guide, review the *IronPort Quickstart Guide* and the latest product release notes for your appliance. In this guide, it is assumed that you have unpacked the appliance, physically installed it in a rack, and turned it on.
If you have already cabled your appliance to your network, ensure that the default IP address for the IronPort appliance does not conflict with other IP addresses on your network. The IP address that is pre-configured on the Management port is 192.168.42.42.

<table>
<thead>
<tr>
<th>Typeface</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AaBbCc123</strong></td>
<td>The names of commands, files, and directories; on-screen computer output.</td>
<td>Please choose an IP interface for this Listener.</td>
</tr>
<tr>
<td><strong>AaBbCc123</strong></td>
<td>User input, in contrast to on-screen computer output.</td>
<td>mail3.example.com&gt; commit Please enter some comments describing your changes: []&gt; Changed the system hostname</td>
</tr>
<tr>
<td><strong>AaBbCc123</strong></td>
<td>Book titles, new terms, emphasized words, and command line variables; for command line variables, the italicized text is a placeholder for the actual name or value.</td>
<td>Read the <em>IronPort Quickstart Guide</em>. Before you begin, please reset your password to a new value. Old password: <strong>ironport</strong> New password: <strong>your_new_password</strong> Retype new password: <strong>your_new_password</strong></td>
</tr>
</tbody>
</table>

Please choose an IP interface for this Listener.

The `sethostname` command sets the name of the IronPort appliance.

The IronPort appliance *must* be able to uniquely select an interface to send an outgoing packet.
IronPort offers the following resources to learn more about the Web Security appliance.

**Documentation Set**

The documentation for the Web Security appliance includes the following books:

- *IronPort AsyncOS CLI Reference Guide*

Occasionally, this book refers to the other guides for additional information about topics.

**IronPort Technical Training**

Cisco IronPort Systems Technical Training Services can help you acquire the knowledge and skills necessary to successfully evaluate, integrate, deploy, maintain, and support IronPort security products and solutions.

Use one of the following methods to contact Cisco IronPort Technical Training Services:

**Training.** For question relating to registration and general training:

- http://training.ironport.com
- training@ironport.com

**Certifications.** For questions relating to certificates and certification exams:

- http://training.ironport.com/certification.html
- certification@ironport.com

**Knowledge Base**

You can access the Cisco IronPort Knowledge Base on the Cisco IronPort Customer Support site at the following URL:

http://www.cisco.com/web/ironport/knowledgebase.html
You need a Cisco.com User ID to access the site. If you do not have a Cisco.com User ID, you can register for one here:

The Knowledge Base contains a wealth of information on topics related to Cisco IronPort products.

Articles generally fall into one of the following categories:

- **How-To.** These articles explain how to do something with a Cisco IronPort product. For example, a how-to article might explain the procedures for backing up and restoring a database for an appliance.

- **Problem-and-Solution.** A problem-and-solution article addresses a particular error or issue that you might encounter when using a Cisco IronPort product. For example, a problem-and-solution article might explain what to do if a specific error message is displayed when you upgrade to a new version of the product.

- **Reference.** Reference articles typically provide lists of information, such as the error codes associated with a particular piece of hardware.

- **Troubleshooting.** Troubleshooting articles explain how to analyze and resolve common issues related to Cisco IronPort products. For example, a troubleshooting article might provide steps to follow if you are having problems with DNS.

**Cisco Support Community**

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general email and web security issues, as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco and Cisco IronPort users.

You access the Cisco Support Community at the following URL:

https://supportforums.cisco.com
Cisco IronPort Customer Support

You can request Cisco IronPort product support by phone, email, or online 24 hours a day, 7 days a week.

During Customer Support hours — 24 hours a day, Monday through Friday — an engineer will contact you within an hour of your request.

To report a critical issue that requires urgent assistance outside of Customer Support hours, contact Cisco IronPort using one of the following methods:

U.S. Toll-free: 1 (877) 646-4766


If you purchased support through a reseller or another supplier, please contact that supplier directly with your product support issues.

Third Party Contributors

Some software included within IronPort 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 IronPort license agreements.

The full text of these agreements can be found here:

Portions of the software within IronPort 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.

IronPort Welcomes Your Comments

The IronPort 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:
Web Security Appliance Overview

The Web Security appliance is a robust, secure, efficient device that protects corporate networks against web-based malware and spyware programs that can compromise corporate security and expose intellectual property. The Web Security appliance extends IronPort’s SMTP security applications to include protection for standard communication protocols, such as HTTP, HTTPS, and FTP.

Malware (“malicious software”) is software designed to infiltrate or damage a computer system without the owner’s consent. It can be any kind of hostile, intrusive, or annoying software or program code. Web-based malware includes spyware, system monitors, adware, phishing and pharming techniques, keystroke (key) loggers, browser hijackers, trojan horses, and more.

Web-based malware is a rapidly growing threat, responsible for significant corporate downtime, productivity losses and major strains on IT resources. Additionally, companies run the risk of violating compliance and data privacy regulations if their networks become compromised by malware. Companies run the risk of expensive legal costs and exposure of intellectual property.

The best place to stop these threats from entering the network is right at the gateway. The Web Security appliance provides deep application content inspection, by offering a web proxy service and by monitoring layer 4 traffic. The Web Proxy and Layer 4 Traffic Monitor allow organizations to ensure breadth of coverage within their networks. The Web Security appliance provides a powerful web security platform to protect your organization against malware that is optimized for performance and efficacy.
Using the Web Security Appliance

This chapter contains the following topics:

- How the Web Security Appliance Works, page 2-1
- Administering the Web Security Appliance, page 2-2
- Navigating the Web Security Appliance Web Interface, page 2-7
- Committing and Clearing Changes, page 2-14

How the Web Security Appliance Works

The Web Proxy and the L4 Traffic Monitor are independent services. They are enabled and configured separately to provide the highest level of protection against a broad range of web-based malware threats.

The Web Proxy and L4 Traffic Monitor use data that is stored in filtering tables to evaluate and match URL request attributes such as domain names, and IP address path segments with locally maintained database records. If a match occurs, Access Policy settings determine an action to block or monitor the traffic. If no match occurs, processing continues.

Web Proxy

The Web Security appliance Web Proxy supports the following security features:

- Policy groups — Policy groups allow administrators to create groups of users and apply different levels of category-based access control to each group.
IronPort URL Filtering Categories — You can configure how the appliance handles each web transaction based on the URL category of a particular HTTP request.

Web Reputation Filters — Reputation filters analyze web server behavior and characteristics to identify suspicious activity and protect against URL-based malware threats.

Anti-Malware Services — The IronPort DVS™ engine in combination with the Webroot™ and McAfee scanning engines identify and stop a broad range of web-based malware threats.

For detailed information about Web Proxy services, see Web Proxy Services, page 5-1.

The L4 Traffic Monitor

The L4 Traffic Monitor is a configurable service that listens and monitors network ports for rogue activity and blocks malware attempts to infect your corporate network. Additionally, the L4 Traffic Monitor detects infected clients and stops malicious activity from going outside the corporate network.

For detailed information about the L4 Traffic Monitor, see L4 Traffic Monitor, page 21-1.

Administering the Web Security Appliance

You can manage the Web Security appliance using a web-based administration tool. When you first access the appliance, the web interface launches the System Setup Wizard to perform an initial configuration. After running the System Setup Wizard, you can use the web interface or Command Line Interface (CLI) to customize settings and maintain your configuration.

For a description of how to access the CLI and a list CLI supported commands, see Command Line Interface, page 27-1.
System Setup Wizard

The System Setup Wizard is a utility that configures basic settings and enables a set of system defaults. The System Setup Wizard is located on the System Administration tab. For more information about running the System Setup Wizard, see System Setup Wizard, page 4-6.

Note

Running the System Setup Wizard completely reconfigures the Web Security appliance and resets the administrator password. Only use the System Setup Wizard the first time you install the appliance, or if you want to completely overwrite the existing configuration. Running the System Setup Wizard after the appliance is already configured can also interrupt client access to the web. If you choose to run the System Setup Wizard after performing an initial setup, use the System Administration > Configuration File pages to print a configuration summary and archive the current configuration file.

Accessing the Web Security Appliance

To access the appliance and launch the web-based administration utility, open a web browser. For the list of supported web browsers, see Browser Requirements, page 2-10.

Connect to the management interface using one of the following methods:

- IP address and port number
  
  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.

- Hostname and port number
  
  https://hostname:8443
  -or-
  
  http://hostname:8080
where hostname is the name of the appliance, and 8080 is the default admin port setting for HTTP, and 8443 is default admin port for HTTPS.

**Note**
The hostname parameter is assigned during system setup. Before you can connect to the management interface using a hostname, you must add the appliance hostname and IP address to your DNS server database.

For information about how to use and navigate the web interface, see Navigating the Web Security Appliance Web Interface, page 2-7.

### Using the Command Line Interface (CLI)

To administer the appliance using the CLI, you can use one of the following methods:

- **Ethernet connection.** Establish an SSH session using an Ethernet cable. For more information, see Using an Ethernet Connection, page 2-4.

- **Serial connection.** Connect to the appliance COM port using a serial cable. For more information, see Using a Serial Connection, page 2-5.

The Web Security appliance CLI supports a set of commands to access, install, and administer the system. See Command Line Interface, page 27-1 for information about the CLI and a list of supported commands that can be used to access, upgrade, and administer the appliance.

### Using an Ethernet Connection

You can connect the appliance to the network using an Ethernet cable from the M1 Management port to the network, and then using an SSH session from a computer on the network to reach the appliance.

By default, the M1 Management port is assigned the IP address 192.168.42.42. To access the Management port, the personal computer must be assigned an IP address on the same subnet as the Management port, such as 192.168.42.43. The subnet mask is 255.255.255.0. This is the easiest way to connect if it works with your network configuration.
Using a Serial Connection

You can connect directly to the appliance COM port using a null modem cable (9-pin serial) to establish a command line interface (CLI) session. You might want to do this if network connectivity to the appliance using an Ethernet cable is not an option.

To do this, you need the following items:

- 9-pin female-to-female serial cable (null modem)
- Serial console client (such as HyperTerminal or PuTTY)

The communications settings for the serial port are:

- **Bits per second**: 9600
- **Data bits**: 8
- **Parity**: None
- **Stop bits**: 1
- **Flow control**: Hardware

The SenderBase Network

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

Basic SenderBase Network Participation is enabled by default during system setup. The appliance supports three levels of participation in the SenderBase Network:

- **Disabled**: Participation is disabled and none of the data that the appliance collects is sent back to the SenderBase Network servers.
- **Limited**: Basic participation summarizes server name information and sends MD5-hashed path segments to the SenderBase Network servers.
- **Standard.** Enhanced participation sends the entire URL with unobfuscated path segments to the SenderBase Network servers. This option assists in providing a more robust database, and continually improves the integrity of Web Reputation Scores.

To select a level of participation in the SenderBase Network, use the Security Services > SenderBase page.

**Sharing Data**

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

IronPort recognizes the importance of maintaining your privacy, and does not collect or use personal or confidential information such as usernames and passwords. Additionally, the file names and URL attributes that follow the hostname are obfuscated to ensure confidentiality. When it comes to decrypted HTTPS transactions, the SenderBase 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 SenderBase Network, data sent from your IronPort appliance is transferred securely using HTTPS. Sharing data improves IronPort’s ability to react to web-based threats and protect your corporate environment from malicious activity.

**Reporting and Logging**

The Web Security appliance provides several options for capturing data and monitoring system activity. For detailed information about scheduling reports, see Reporting Overview, page 22-1. For more information about working with log files, see Logging, page 24-1.
Navigating the Web Security Appliance Web Interface

The Web Security appliance web interface is a web-based administration tool that allows you to configure and monitor the appliance. The web interface allows you to configure the appliance similar to the Command Line Interface (CLI). However, some features available in the web interface are not available in the CLI and vice versa. For more information about the CLI, see Command Line Interface, page 27-1.

The Web Security appliance web interface contains multiple tabs where you can configure or monitor the appliance. You can set up Access Policies, schedule reports, enable features, and modify settings as necessary. The web interface also includes two menus from which you can perform basic administration tasks.

To use the web interface, open a web browser and log in. For more details, see Accessing the Web Security Appliance, page 2-3. For a list of supported web browsers, see Browser Requirements, page 2-10.

For a list of supported languages, see Support Languages, page 2-10.

The web interface contains the following menus:

- **Options.** From this menu, you can manage your user account. You can logout or change the password you use to log in to the web interface.

- **Help.** From this menu, you can access help from documentation or IronPort Customer Support. For Help tasks, you can access the online help or the Cisco IronPort Customer Support site. For Technical Support tasks, you can send a support request email to IronPort Customer Support or to allow IronPort Customer Support remote access to the Web Security appliance. For more information about the Technical Support tasks, see Support Commands, page 26-3.

The web interface contains the following tabs:

- **Reporting.** Use the pages on this tab to view reports on the appliance by that display dynamic data on website activity and appliance activity and action. For more information, see Reporting Tab, page 2-11.

- **Web Security Manager.** Use the pages on this tab to create and configure Access Policies that define which groups can access which types of websites. For more information, see Web Security Manager Tab, page 2-11.
• **Security Services.** Use the pages on this tab to configure how the appliance monitors and secures the network. For more information, see Security Services Tab, page 2-12.

• **Network.** Use the pages on this tab to define the network in which the appliance is located. For more information, see Network Tab, page 2-13.

• **System Administration.** Use the pages on this tab to configure administrative options, such as users, alerts, system time, and more. You can also enter keys for features you enabled during initial setup. For more information, see System Administration Tab, page 2-13.

Each tab has a list of menu selections from which you can choose. Each menu selection represents a different page in the web interface that further group information and activities. Some pages are grouped together into categories. You navigate among sections of the web interface by hovering the cursor over each tab heading and clicking a menu option from the menu that appears.

You open up other pages in the web interface by clicking on hypertext links and buttons. To find the various links, hover the cursor over text in the web interface. Links appear with an underline under the text when the cursor is over them.

Figure 2-1 on page 9 shows the web interface tabs, pages, and categories. It also shows some sample links and buttons you can click to open up other pages where you can configure the appliance.
Chapter 2  Using the Web Security Appliance  

Navigating the Web Security Appliance Web Interface

Figure 2-1 Web Interface Tabs, Pages, and Categories

Figure 2-1 shows that the Web Security Manager tab contains the Web Proxy category, and the Web Proxy category contains the Identities, Decryption Policies, Routing Policies, Access Policies, and Bypass List pages. The tab also contains the Custom Policy Elements category (with the Custom URL Categories page), and the L4 Traffic Monitor page.

When the documentation refers to specific pages in the web interface, it uses the tab name, following by an arrow and then the page name. For example, Web Security Manager > Access Policies.

Logging In

All users accessing the web interface must log in. Type your username and password, and then click Login to access the web interface. You must use a supported web browser (see Browser Requirements, page 2-10). You can log in with the admin account or any other user account created in the appliance. For more information creating appliance users, see Administering User Accounts, page 26-12.

After you log in, the Reporting > Overview page displays.
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). For example, you can use the following browsers:

- Firefox 1.0 and later
- Internet Explorer 6.02 and later (Windows only)
- Mozilla 1.76 and later
- Netscape 7.1 and later
- Safari 2.0.4 and later (Mac OS X only)

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.

Support Languages

With the appropriate license key, AsyncOS can display its GUI and CLI in any of the following languages:

- English
- French
- Spanish
- German
- Italian
- Korean
- Japanese
• Portuguese (Brazil)
• Chinese (zh-cn and zh-tw)
• Russian

**Reporting Tab**

Use the Reporting tab to monitor the appliance by viewing dynamic data on website activity and appliance activity and action.

The Reporting tab includes the following pages:
• Overview
• Users
• Web Sites
• URL Categories
• Application Visibility
• Anti-Malware
• Client Malware Risk
• Web Reputation Filters
• L4 Traffic Monitor
• Reports by User Location
• Web Tracking
• System Capacity
• System Status
• Scheduled Reports
• Archived Reports

**Web Security Manager Tab**

Use the Web Security Manager tab to create and configure Access Policies that define which groups can access which types of websites.

The Web Security Manager tab includes the following pages:
Navigating the Web Security Appliance Web Interface

- Identities
- SaaS Policies
- Decryption Policies
- Routing Policies
- Access Policies
- Overall Bandwidth Limits
- IronPort Data Security
- Outbound Malware Scanning
- External Data Loss Prevention
- Custom URL Categories
- Defined Time Ranges
- Bypass Settings
- L4 Traffic Monitor

Security Services Tab

Use this tab to configure how the appliance monitors and secures the network.

The Security Services tab includes the following pages:

- Web Proxy
- FTP Proxy
- HTTPS Proxy
- PAC File Hosting
- Identity Provider for SaaS
- Acceptable Use Controls
- Anti-Malware
- Data Transfer Filters
- Mobile User Security
- Web Reputation Filters
- End-User Notification
Network Tab

Use the Network tab to describe the network in which the appliance is located and to define the appliance’s network settings.

The Network tab includes the following pages:

- Interfaces
- Transparent Redirection
- Routes
- Internal SMTP Relay
- Authentication
- Upstream Proxy
- External DLP Servers
- DNS

System Administration Tab

Use the System Administration tab to configure administrative options, such as users, alerts, system time, and more. You can also enter keys for features you enabled during initial setup.

The System Administration tab includes the following pages:

- Policy Trace
- Users
- Alerts
- Log Subscriptions
- Return Addresses
- Time Zone
- Time Settings
Committing and Clearing Changes

When you change the configuration of the Web Security appliance, you must commit the changes before they go into effect. Or, you can choose to clear the changes you have made if you do not want to commit them. How you commit and clear changes depends on the interface you use:

- Web interface
- Command Line Interface

Committing and Clearing Changes in the Web Interface

Commit changes using the Commit Changes button in the upper right corner of the web interface. You can make multiple configuration changes before you commit all of them. When you make a change, the Commit Changes button color is yellow and the button text changes to “Commit Changes” as shown in Figure 2-2.

![Figure 2-2 The Commit Button: Changes Pending](commit-button.png)

When there are no changes to commit, the button color is gray and the button text is “No Changes Pending.” Figure 2-3 shows the web interface when there are no changes to commit.
You also use the **Commit Changes** button to clear the changes made since the last commit or clear.

### Committing Changes

To commit changes made in the web interface:

**Step 1**  
Click the **Commit Changes** button.  
The Uncommitted Changes page appears.

**Uncommitted Changes**

You have uncommitted changes. These changes will not go into effect until you commit them.  

- **Comment (optional):**

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

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

### Clearing Changes

To clear changes made in the web interface:

**Step 1**  
Click the **Commit Changes** button.  
The Uncommitted Changes page appears.

**Step 2**  
Click **Abandon Changes**.
Committing and Clearing Changes in the CLI

Commit changes using the `commit` command. Most configuration changes you make in the Command Line Interface (CLI) are not effective until you issue the `commit` command. You may include comments up to 255 characters. Changes are not verified as committed until you receive confirmation along with a timestamp. The `commit` command applies configuration changes made to appliance since the last `commit` or `clear` command issued.

For more information about using the `commit` command, see Committing Configuration Changes, page 27-6.

Clear changes using the `clear` command. For more information about using the `clear` command, see Clearing Configuration Changes, page 27-7.
This chapter contains the following topics:

- Deployment Overview, page 3-1
- Appliance Interfaces, page 3-3
- Deploying the Web Proxy in Explicit Forward Mode, page 3-6
- Deploying the Web Proxy in Transparent Mode, page 3-7
- Connecting the Appliance to a WCCP Router, page 3-8
- Using the Web Security Appliance in an Existing Proxy Environment, page 3-15
- Deploying the L4 Traffic Monitor, page 3-16
- Physical Dimensions, page 3-18

Deployment Overview

The Web Security appliance is typically installed as an additional layer in the network between clients and the Internet. Depending on how you deploy the appliance, you may or may not need a Layer 4 (L4) switch or a WCCP router to direct client traffic to the appliance.

When you deploy the Web Security appliance, you can enable one or both of the following features:
Secure web proxy. The appliance web proxy service monitors and scans web traffic for malicious content. When you enable the web proxy, you can configure it to be in transparent or explicit forward mode.

L4 Traffic Monitor. The L4 Traffic Monitor detects and blocks rogue traffic across all ports and IP addresses. The L4 Traffic Monitor listens to network traffic that comes in over all ports and IP addresses on the appliance and matches domain names and IP addresses against entries in its own database tables to determine whether to allow outgoing traffic.

By default, both the L4 Traffic Monitor and Web Proxy are enabled in the System Setup Wizard. If you need to disable both or one of these features, you can do so after initial setup from the web interface.

The features you enable determine how you deploy and physically connect the appliance to the network. For more information about how the features you enable affect appliance deployment, see Preparing for Deployment, page 3-2. For more information about the Ethernet ports used to physically connect the appliance to the network, see Appliance Interfaces, page 3-3.

Preparing for Deployment

Before installing the Web Security appliance, read through the following questions and use the responses to each question to help you decide how to deploy the appliance and where to locate it in your network. Each response includes a reference to a different section that covers the response in more detail.

1. Will you deploy the Web Security appliance as a transparent proxy or an explicit forward proxy?

   - Explicit Forward Proxy. Client applications, such as web browsers, are aware of the Web Proxy and must be configured to point to a single Web Security appliance. This deployment requires a connection to a standard network switch. When you deploy the Web Proxy in explicit forward mode, you can place it anywhere in the network. For more information, see Deploying the Web Proxy in Explicit Forward Mode, page 3-6.

   - Transparent Proxy. Clients applications are unaware of the Web Proxy and do not have to be configured to connect to the proxy. This deployment requires an L4 switch or a WCCP v2 router. For more information, see Deploying the Web Proxy in Transparent Mode, page 3-7.
2. Does the network have an existing proxy?
   If yes, it is recommended you deploy the Web Security appliance downstream from an existing proxy server, meaning closer to the clients. The System Setup Wizard refers to this as an upstream proxy configuration.
   For more information, see Using the Web Security Appliance in an Existing Proxy Environment, page 3-15.

3. Will you enable the L4 Traffic Monitor?
   L4 Traffic Monitor deployment is independent of the Web Proxy deployment. You can connect the L4 Traffic Monitor to a network tap or the mirror/span port of a switch.
   For more information, see Deploying the L4 Traffic Monitor, page 3-16.

**Appliance Interfaces**

The Web Security appliance includes six physical Ethernet ports on the back of the system. Each Ethernet port corresponds to a different network interface. The Ethernet ports are grouped into the following types of network interfaces:

- **Management.** The Management interfaces include M1 and M2. However, only the M1 interface is enabled on the appliance. For more information, see Management Interface, page 3-4.

- **Data.** The Data interfaces include P1 and P2. Use the Data interfaces for Web Proxy data traffic. For more information, see Data Interfaces, page 3-4.

- **L4 Traffic Monitor.** The L4 Traffic Monitor interfaces include T1 and T2. Use these interfaces for monitoring and blocking L4 Traffic Monitor traffic. For more information, see L4 Traffic Monitor Interfaces, page 3-5.

Figure 3-1 shows the Ethernet ports on the back of the Web Security appliance blade.
Appliance Interfaces

Figure 3-1 Web Security Appliance Ethernet Ports

Management Interface

Use M1 to administer the appliance. Optionally, you can also configure the M1 interface to handle Web Proxy data traffic. You might want to use the M1 interface for data traffic if your organization does not use a separate management network.

For more information about using the M1 port to set up and manage the appliance, see Connecting a Laptop to the Appliance, page 4-2.

For more information about configuring the network interfaces, see Configuring Network Interfaces, page 25-2.

Data Interfaces

The appliance uses the Data interfaces for Web Proxy data traffic. You can enable and use just the P1 port or both the P1 and P2 ports for data traffic.

- **P1 only enabled.** When only P1 is enabled, connect it to the network for both incoming and outgoing traffic.

- **P1 and P2 enabled.** When both P1 and P2 are enabled, you must connect P1 to the internal network and P2 toward the Internet.
You can only enable and configure the P1 interface for data traffic in the System Setup Wizard. If you want to enable the P2 interface, you must do so after system setup in the web interface or using the `ifconfig` command. For more information about configuring the P2 interface, see Configuring Network Interfaces, page 25-2.

How you physically connect the data interfaces to the network depends on how you deploy the appliance. For more information, see Deploying the Web Proxy in Explicit Forward Mode, page 3-6 and Deploying the Web Proxy in Transparent Mode, page 3-7.

**L4 Traffic Monitor Interfaces**

The appliance uses the T1 and T2 interfaces for listening to traffic on all TCP ports. You can connect just T1 or both T1 and T2 using an Ethernet cable, depending on whether you use simplex or duplex communication.

- **T1 only connected (duplex).** When you configure the appliance to use duplex communication, connect T1 to the network so it receives all incoming and outgoing traffic.

- **T1 and T2 connected (simplex).** When you configure the appliance to use simplex communication, connect T1 to the network so it receives all outgoing traffic (from the clients to the Internet), and connect T2 to the network so it receives all incoming traffic (from the Internet to the clients).

For more information about how to connect the L4 Traffic Monitor ports to the network, see Deploying the L4 Traffic Monitor, page 3-16.

**Example Deployment**

Figure 3-2 on page 6 shows a sample deployment scenario with both the Web Proxy and L4 Traffic Monitor enabled. In this example, the Web Proxy is deployed in transparent mode and only the P1 port is connected to either a L4 switch or a WCCP router.
Deploying the Web Proxy in Explicit Forward Mode

When the appliance is configured as an explicit forward proxy, client applications must be configured to direct its traffic to the appliance. When you want to configure the Web Proxy in explicit forward mode, you must configure the following components:

- Client applications
- Appliance ports

Tip

If your organization needs to use explicit forward mode now, but might need transparent mode in the future, consider deploying the Web Proxy in transparent mode and then choosing L4 switch as the connection type. If you do not have an L4 switch, you can connect the appliance to the network normally and the appliance will work in explicit forward mode. When the Web Proxy is deployed in transparent mode, it can accept both transparently redirected and explicitly forwarded transactions. To use transparent mode in the future, you can connect the appliance to an L4 switch and it will work in transparent mode without needing to change the Web Proxy mode later. However, it is easy to change the deployment mode at any time on the Security Services > Web Proxy page.
Configuring Client Applications

You must configure all client applications, such as web browsers and FTP clients, used on the network to point to the Web Proxy. You can configure each client in the following ways:

- **Manual.** Configure each client application to point the appliance Web Proxy by specifying the appliance hostname or IP address and the port number, such as 3128, used for listening to data traffic.
- **Automatic.** Configure each client application to use a PAC file to detect the appliance Web Proxy automatically. Then you can edit the PAC file to specify the appliance Web Proxy information. PAC files work with web browsers only. For more information, see Working with PAC Files, page 5-19.

Connecting Appliance Interfaces

You can connect the P1 interface or both the P1 and P2 interfaces to a network switch using an Ethernet cable. You do not need special hardware, such as a particular switch or router. For more information about how to connect the data interfaces (P1 and P2), see Data Interfaces, page 3-4.

Testing an Explicit Forward Configuration

If you want to test an explicit forward proxy configuration, you can separate and forward traffic from a subset of your network infrastructure. To individually test this configuration, clients can forward traffic to the appliance from one web browser and connect to the Internet using another web browser. This method also ensures an alternate path to the Internet while testing.

Deploying the Web Proxy in Transparent Mode

When the appliance is configured as a transparent proxy, client applications are not aware that their traffic gets redirected to the appliance, and they do not need to be configured to point to the appliance. To deploy the appliance in this mode, you need one of the following types of hardware to transparently redirect web traffic to the appliance:
• **WCCP v2 router.** When you specify a WCCP router, you need to configure additional settings on the appliance. For more information about using the appliance with a WCCP router, see Connecting the Appliance to a WCCP Router, page 3-8.

• **Layer 4 switch.** When you specify an L4 switch, you only need to specify that the appliance is connected to an L4 switch when you configure the appliance. You do not need to configure anything else on the appliance.

Typically, you configure the appliance to use an L4 switch or a WCCP v2 router during initial system setup. However, you can configure it to use either an L4 switch or a WCCP v2 router anytime after initial setup on the Network > Transparent Redirection page. For more information about the Network > Transparent Redirection page, see Configuring Transparent Redirection, page 25-17.

### Connecting Appliance Interfaces

When you configure the Web Proxy in transparent mode, you can connect the P1 port or both the P1 and P2 ports to an L4 switch or WCCP router using an Ethernet cable. For more information about how to connect the data interfaces (P1 and P2), see Data Interfaces, page 3-4.

### Connecting the Appliance to a WCCP Router

When you connect the appliance to a WCCP router, you must perform the following tasks:

1. You must create at least one WCCP service on the appliance. For more information, see Configuring the Web Security Appliance, page 3-9.

2. After you create a WCCP service, you must configure the router to work with the Web Security appliance. For more information, see Configuring the WCCP Router, page 3-9.

You can also connect an appliance to multiple WCCP routers. For more information, see Working with Multiple Appliances and Routers, page 3-15.
Configuring the Web Security Appliance

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.

Create WCCP services on the Network > Transparent Redirection page. The WCCP services you create determine how you configure the WCCP routers. For more information about creating WCCP services, see Adding and Editing a WCCP Service, page 25-21.

Note

You can enable the standard service (also known as the “web-cache” service) during system setup, and you can configure different or additional WCCP service groups after you run the System Setup Wizard.

Configuring the WCCP Router

After you create at least one WCCP service in the Web Security appliance, you can configure the WCCP router(s) in the network.

Use the following syntax for enabling WCCP on the router:

```
ip wccp version 2
ip wccp service_group
interface interface_type_number
ip wccp service_group redirect direction
ip wccp service_group password password
```

Enter one of the following values for the `service_group` variable:

- **web-cache**. Enter “web-cache” when the appliance WCCP service uses the standard service.
- **Service ID number**. Enter a number from 0 to 255 when the appliance WCCP service uses a dynamic service ID. The number should match the service ID number used in the appliance.
Table 3-1 describes each part of the WCCP configuration syntax for enabling WCCP on the router.

**Table 3-1 WCCP Router Configuration Syntax for Enabling the Router**

<table>
<thead>
<tr>
<th>WCCP Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip wccp version 2</code></td>
<td>Defines the version of WCCP to use on the router. You must specify version 2 to work with the Web Security appliance. This command is required.</td>
</tr>
<tr>
<td>`ip wccp service_group</td>
<td>Specifies a service group to enable on the router. It also enables the WCCP service on the router. This command is required.</td>
</tr>
<tr>
<td>password password</td>
<td></td>
</tr>
<tr>
<td><code>interface</code></td>
<td>Specifies an interface to configure and enters interface configuration mode. Enter the interface number for the <code>interface_type_number</code> variable. This command is required.</td>
</tr>
<tr>
<td><code>interface_type_number</code></td>
<td></td>
</tr>
<tr>
<td>`ip wccp service_group</td>
<td>Enables WCCP redirection on the specified interface. Enter one of the following values for the <code>direction</code> variable:</td>
</tr>
<tr>
<td>redirect <code>direction</code></td>
<td></td>
</tr>
<tr>
<td><code>in</code></td>
<td>Use <code>in</code> when you want the router to redirect packets as they enter the router.</td>
</tr>
<tr>
<td><code>out</code></td>
<td>Use <code>out</code> when you want the router to redirect packets right before they leave the router.</td>
</tr>
<tr>
<td>`ip wccp service_group</td>
<td>Sets a password on the router for the specified service group. This command is only required when the WCCP service defined on the appliance has password security enabled.</td>
</tr>
<tr>
<td>password password</td>
<td></td>
</tr>
</tbody>
</table>

You can also configure a WCCP router to perform other tasks, such as the following:
Connecting the Appliance to a WCCP Router

- Configure the router from exclude redirecting traffic received on a particular interface.
- If the network uses multiple Web Security appliances, you can configure the router to determine which traffic should be directed to which appliance by using an access list. You might want to redirect only some of the network traffic to the appliance if you are evaluating the Web Security appliance.

**Note**
The Web Security appliance does not support using a multicast address in the WCCP service group. To use multiple routers in a service group, you must specify the IP address of each router in the service group and configure each router separately. You cannot register a router to a multicast address.

**Example WCCP Configurations**

This section shows some sample WCCP services defined in the appliance and the corresponding WCCP configuration you should use to configure the router that connects to the appliance.

**Example 1**

Suppose you have the WCCP service shown in Figure 3-3.
Connecting the Appliance to a WCCP Router

Figure 3-3  Example WCCP Service — Standard Service, No Password Required

Add WCCP v2 Service

<table>
<thead>
<tr>
<th>WCCP v2 Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Profile Name: web_cache</td>
</tr>
<tr>
<td>SERVICE:</td>
</tr>
<tr>
<td>(Standard service ID: 0-web_cache) (destination port 0)</td>
</tr>
<tr>
<td>Dynamic service ID: 0-255</td>
</tr>
<tr>
<td>Port numbers: (up to 8 port numbers, separated by commas)</td>
</tr>
<tr>
<td>Redirect based on destination port</td>
</tr>
<tr>
<td>Redirect based on source port (return path)</td>
</tr>
<tr>
<td>For IP spoofing, define two services, one based on destination port and another based on source port (return path).</td>
</tr>
<tr>
<td>Load balance based on server address</td>
</tr>
<tr>
<td>Applies only if more than one Web Security Appliance is in use</td>
</tr>
<tr>
<td>Router IP Addresses: 1.1.1.1</td>
</tr>
<tr>
<td>Separate multiple entries with line breaks or commas.</td>
</tr>
<tr>
<td>Router Security:</td>
</tr>
<tr>
<td>(Enable Security for Service)</td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>Confirm Password:</td>
</tr>
<tr>
<td>Advanced:</td>
</tr>
<tr>
<td>Load-Balancing Method: Allow Hash or Round</td>
</tr>
<tr>
<td>Forwarding Method: Allow GRE or L2</td>
</tr>
<tr>
<td>Return Method: Allow GRE or L2</td>
</tr>
</tbody>
</table>

In this example, the WCCP service defines the standard service group (also known as a well known service group). The redirection basis is on the destination port by default. Also suppose in this example that you want to configure the ethernet1 interface on the router for this service group.

Use the following WCCP configuration for this example:

```
ip wccp version 2
ip wccp web-cache
interface ethernet1
ip wccp web-cache redirect in
```

Example 2

Figure 3-4 shows a dynamic service you might create when IP spoofing is enabled and the WCCP service shown in Figure 3-3 on page 12 is defined.
Connecting the Appliance to a WCCP Router

Figure 3-4  Example WCCP Service — Dynamic Service for IP Spoofing

Add WCCP v2 Service

In this example, the WCCP service defines a dynamic service group with service ID of 90. The redirection basis is on the source port so it can be used for the return path with IP spoofing enabled. Suppose in this example that you want to configure the ethernet0 interface on the router for this service group.

Use the following WCCP configuration for this example:

```
ip wccp version 2
ip wccp 90
interface ethernet0
ip wccp 90 redirect in
```

For more information about enabling IP spoofing when using a WCCP router, see IP Spoofing when Using WCCP, page 25-20.
Example 3

Suppose you have the WCCP service shown in Figure 3-5.

Figure 3-5  Example WCCP Service — Dynamic Service, Password Required

Add WCCP v2 Service

<table>
<thead>
<tr>
<th>WCCP v2 Service</th>
<th>Service Profile Name: service0_443</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Standard service ID: 0 web-cache (destination port 80)</td>
</tr>
<tr>
<td>Port numbers</td>
<td>80, 443 (up to 10 port numbers, separated by commas)</td>
</tr>
<tr>
<td>Redirect based on destination port</td>
<td>Redirect based on source port (return path)</td>
</tr>
<tr>
<td>Redirect based on source port (return path)</td>
<td>Load balance based on server address</td>
</tr>
<tr>
<td>Load balance based on client address</td>
<td>Applies only if more than one Web Security appliance is in use</td>
</tr>
</tbody>
</table>

Router IP Addresses:

1.1.1.1, 10.5.5.5

Router Security:

- Enable Security for Service
- Password: ********
- Confirm Password: ********

Advanced:

- Load-Balancing Method: Allow Hash or Round Robin
- Forwarding Method: Allow GRE or L2
- Return Method: Allow GRE or L2

In this example, the WCCP service defines a dynamic service group with service ID of 120. The redirection basis is on the destination port, and it has enabled a password for this service group of “admin99” (hidden in the appliance configuration). Also suppose in this example that you want to configure the ethernet0 interface on the router for this service group.

Use the following WCCP configuration for this example:

```
ip wccp version 2
ip wccp 120
interface ethernet0
ip wccp 120 redirect in
ip wccp 120 password admin99
```
Working with Multiple Appliances and Routers

When you connect one or more Web Security appliances to one or more WCCP routers, you have a cluster. You can include up to 32 appliances and up to 32 routers in a cluster. You must configure all appliances and routers in a cluster to communicate with each other.

Using the Web Security Appliance in an Existing Proxy Environment

The Web Security appliance is a proxy-compatible device, and is easily deployed within an existing proxy environment. However, it is recommended that you place the appliance downstream from existing proxy servers, meaning closer to the clients.

You can configure the appliance to work with an existing, upstream proxy in the System Setup Wizard or after the initial setup in the web interface. Use the Network > Upstream Proxies page to enable an upstream proxy or to modify existing settings.

When configuring an upstream proxy, you specify whether the existing proxy is in transparent or explicit forward mode.

Transparent Upstream Proxy

If a transparent upstream proxy uses client IP addresses to manage user authentication and access control, you must enable IP spoofing on the Web Security appliance to send client IP addresses to the upstream proxy. Use the Security Services > Web Proxy page to enable IP spoofing.

When you enable IP spoofing and connect the appliance to a WCCP router, you must create at least two WCCP services. For more information about configuring WCCP services when you enable IP spoofing, see IP Spoofing when Using WCCP, page 25-20.
Explicit Forward Upstream Proxy

If the upstream proxy is in explicit forward mode, consider the following rules and guidelines:

- You must enter the IP address or hostname and port of the upstream proxy.
- Consider whether the hostname of the upstream proxy resolves to multiple IP addresses. The Web Security appliance only queries the DNS server for the IP address at startup. If an IP address is added or removed from that hostname, the proxy must restart to resolve and add the hostname to the new set of IP addresses.
- If the upstream proxy manages user authentication or access control using proxy authentication, you must enable the X-Forwarded-For header to send the client host header to the upstream proxy. Use the Security Services > Web Proxy page to enable the X-Forwarded-For header setting.
- If you want to send authentication credentials to an upstream proxy when the Web Security appliance is deployed in explicit forward mode, you must configure the Web Proxy to forward authorization request headers to a parent proxy server using the `advancedproxyconfig > authentication` CLI command.

Note

By default, the Web Proxy does not forward proxy authorization headers to upstream proxy servers for security reasons.

- If the upstream proxy manages client traffic using a PAC file or a login script, you must update these files to use the IP address or hostname of the Web Security appliance.

Deploying the L4 Traffic Monitor

L4 Traffic Monitor (L4TM) deployment is independent of the Web Proxy deployment. When connecting and deploying the L4 Traffic Monitor, consider the following:

- Physical connection. You can choose how to connect the L4 Traffic Monitor to the network. For more information, see Deploying the L4 Traffic Monitor, page 3-17.
• **Network address translation** (NAT). When configuring the L4 Traffic Monitor, connect it at a point in your network where it can see as much network traffic as possible before getting out of your egress firewall and onto the Internet. It is important that the L4 Traffic Monitor be ‘logically’ connected after the proxy ports and before any device that performs network address translation (NAT) on client IP addresses.

• **L4 Traffic Monitor action setting.** The default setting for the L4 Traffic Monitor is monitor only. After setup, if you configure the L4 Traffic Monitor to monitor and block suspicious traffic, ensure that the L4 Traffic Monitor and the Web Proxy are configured on the same network so that all clients are accessible on routes that are configured for data traffic.

## Connecting the L4 Traffic Monitor

You can connect the L4 Traffic Monitor to the network in any of the following ways:

• **Network tap.** When you use a network tap, you can choose the following communication types:
  - **Simplex.** This communication type uses one cable for all traffic between clients and the appliance, and one cable for all traffic between the appliance and external connections. Connect port T1 to the network tap so it receives all outgoing traffic (from the clients to the Internet), and connect port T2 to the network tap so it receives all incoming traffic (from the Internet to the clients).
  - **Duplex.** This mode uses one cable for all incoming and outgoing traffic. You can use half- or full-duplex Ethernet connections. Connect port T1 to the network tap so it receives all incoming and outgoing traffic.

  **Note**  
  Cisco recommends using simplex when possible because it can increase performance and security.

• **Span/mirror port of an L2 switch.** Connecting is similar to a simplex or duplex tap, depending on whether the connection uses two separate devices or one device.

• **Hub.** Choose duplex when you connect the L4 Traffic Monitor to a hub.
Regardless of how the appliance is connected to the network, you must configure the wiring type. For more information, see Configuring an L4 Traffic Monitor Wiring Type, page 3-18.

For more information about the T1 and T2 ports, see Appliance Interfaces, page 3-3.

**Note**
Use a network tap instead of the span/mirror port of a switch when possible. Network taps use hardware to move packets to the L4 Traffic Monitor and span and mirror ports of a switch use software to move packets. Hardware solutions move packets with better performance than software solutions and are less likely to drop packets in the process.

**Configuring an L4 Traffic Monitor Wiring Type**

Typically, the L4 Traffic Monitor wiring type is configured during system setup. However, you can configure the wiring type after running the System Setup Wizard on the Network > Interfaces page. Click **Edit Settings** and select a wiring type for the T1 and T2 ports.

**Figure 3-6  L4 Traffic Monitor Wiring Types**

<table>
<thead>
<tr>
<th>L4 Traffic Monitor Wiring Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Duplex TAP: T1 (In/Out)</td>
</tr>
<tr>
<td>- Simplex TAP: T1 (In) and T2 (Out)</td>
</tr>
</tbody>
</table>

**Physical Dimensions**

The following physical dimensions apply to the **IronPort S670 and S370** Web Security appliances:

- Height: 8.64 cm (3.40 inches)
- Width: 48.24 cm (18.99 inches) with or without rails
- Depth: 72.06 cm (28.40 inches)
- Weight: maximum 23.59 kg (52 pounds)
The following physical dimensions apply to the **IronPort S160** Web Security appliance:

- Height: 4.2 cm (1.68 inches)
- Width: 48.26 cm (19.0 inches) with rails installed (without rails, 17.5 inches)
- Depth: 57.6 cm (22.7 inches)
- Weight: maximum 9.8 kg (21.6 pounds)
Physical Dimensions
Installation and Configuration

This chapter contains the following topics:

- Before You Begin, page 4-1
- System Setup Wizard, page 4-6

Before You Begin

To use the Web Security appliance, you must run the System Setup Wizard. However, first you must do some steps to prepare the appliance for the System Setup Wizard.

For more information about preparing the appliance for installation, see the Web Security appliance QuickStart Guide. You can find this guide and other useful information about the IronPort Web Security appliance on the Cisco IronPort Customer Support site:


Complete the following tasks before you run the System Setup Wizard:

- **Deployment.** Decide how you are going to configure the appliance within your network. For details, see Deployment, page 3-1.

- **Laptop network connection.** Configure your laptop’s network connection to use an IP address on the same subnet as the Web Security appliance (192.168.42.xx). For details, see Connecting a Laptop to the Appliance, page 4-2.
Before You Begin

- **Appliance physical connections.** Plug the Ethernet cables into the appropriate ports on the back panel of the appliance. For details, see Connecting the Appliance to the Network, page 4-2.

- **Setup information.** Once you know how you will install the appliance in your network, gather all the information, such as IP addresses, necessary for the System Setup Wizard. For details, see Gathering Setup Information, page 4-4.

- **Existing proxy server.** If you plan to use the Web Security appliance in a network that has an existing proxy server, you must locate it downstream from other proxy servers. Also, after you finish the initial setup of the appliance, you must configure it to work with the existing proxy server. For more information about deploying the appliance in a network with an existing proxy, see Using the Web Security Appliance in an Existing Proxy Environment, page 3-15.

### Connecting a Laptop to the Appliance

In order to run the System Setup Wizard the first time, you must connect a computer, such as a laptop, to the appliance. To connect to the appliance, the laptop subnet must be the same as the appliance subnet. The Management ports are labeled M1 and M2. The Web Security appliance only uses the M1 Management port. It does not use M2.

Configure the laptop IP address so it is on the same subnet as the appliance (192.168.42.xx). Then, connect the laptop to the M1 port on the back of the appliance.

### Connecting the Appliance to the Network

You must plug the Ethernet cables into the appropriate ports on the back panel of the appliance. For more information about the Ethernet ports on the appliance, see Appliance Interfaces, page 3-3.

How you deploy the appliance determines which Ethernet cables to plug in where:
Before You Begin

- **Web proxy in transparent mode.** If you want to use one proxy port for all traffic, connect port P1 to an L4 switch or a WCCP router using an Ethernet cable. If you want to use two proxy ports for traffic, connect port P2 to an L4 switch or a WCCP router using an Ethernet cable, and connect port P1 to the internal network.

  For more information about deploying the Web Proxy in transparent mode, see Deploying the Web Proxy in Transparent Mode, page 3-7.

  **Note** When you configure the proxy in transparent mode and connect it to a WCCP router, you must configure the appliance after you run the System Setup Wizard to create at least one WCCP service. For more information about creating WCCP services, see Adding and Editing a WCCP Service, page 25-21.

- **Web proxy in explicit forward mode.** If you want to use one proxy port for all traffic, connect port P1 to a network switch using an Ethernet cable. If you want to use two proxy ports for traffic, connect port P2 to a network switch using an Ethernet cable, and connect port P1 to the internal network.

  For more information about deploying the Web Proxy in explicit forward mode, see Deploying the Web Proxy in Explicit Forward Mode, page 3-6.

- **L4 Traffic Monitor.** Connect the Traffic Monitor ports to the Ethernet tap according to the tap communication type:

  - **Ethernet tap using simplex.** Connect port T1 to the Ethernet tap so it receives all outgoing traffic (from the clients to the Internet), and connect port T2 to the Ethernet tap so it receives all incoming traffic (from the Internet to the clients).

  - **Ethernet tap using duplex.** Connect port T1 to the Ethernet tap so it receives all incoming and outgoing traffic.

  For more information about deploying the L4 Traffic Monitor, see Deploying the L4 Traffic Monitor, page 3-16.
Gathering Setup Information

Once you know how you will install the appliance in your network, you can gather the necessary information, such as IP addresses, to enter in the System Setup Wizard. You can use the worksheet in Table 4-1 to write down the configuration options you decide on. Then, when you run the System Setup Wizard, you can use the information you enter in the worksheet to configure the initial setup.

Table 4-1 System Setup Worksheet

<table>
<thead>
<tr>
<th>Network Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default System Hostname:</td>
</tr>
<tr>
<td>DNS Servers:</td>
</tr>
<tr>
<td>Internet root DNS servers / organization DNS servers</td>
</tr>
<tr>
<td>Organization DNS Servers:</td>
</tr>
<tr>
<td>(maximum 3)</td>
</tr>
<tr>
<td>1.</td>
</tr>
<tr>
<td>2.</td>
</tr>
<tr>
<td>3.</td>
</tr>
<tr>
<td>Network Time Protocol Server:</td>
</tr>
<tr>
<td>Time Zone Region:</td>
</tr>
<tr>
<td>Time Zone Country:</td>
</tr>
<tr>
<td>Time Zone / GMT Offset:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there another proxy on the network: Yes / No</td>
</tr>
<tr>
<td>Other Proxy IP Address:</td>
</tr>
<tr>
<td>Other Proxy Port:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Port</td>
</tr>
<tr>
<td>IP Address:</td>
</tr>
<tr>
<td>Network Mask:</td>
</tr>
<tr>
<td>Hostname:</td>
</tr>
</tbody>
</table>

| Data Port                                            |

Table 4-1 System Setup Worksheet

<table>
<thead>
<tr>
<th>Network Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default System Hostname:</td>
</tr>
<tr>
<td>DNS Servers:</td>
</tr>
<tr>
<td>Internet root DNS servers / organization DNS servers</td>
</tr>
<tr>
<td>Organization DNS Servers:</td>
</tr>
<tr>
<td>(maximum 3)</td>
</tr>
<tr>
<td>1.</td>
</tr>
<tr>
<td>2.</td>
</tr>
<tr>
<td>3.</td>
</tr>
<tr>
<td>Network Time Protocol Server:</td>
</tr>
<tr>
<td>Time Zone Region:</td>
</tr>
<tr>
<td>Time Zone Country:</td>
</tr>
<tr>
<td>Time Zone / GMT Offset:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there another proxy on the network: Yes / No</td>
</tr>
<tr>
<td>Other Proxy IP Address:</td>
</tr>
<tr>
<td>Other Proxy Port:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Port</td>
</tr>
<tr>
<td>IP Address:</td>
</tr>
<tr>
<td>Network Mask:</td>
</tr>
<tr>
<td>Hostname:</td>
</tr>
</tbody>
</table>

| Data Port                                            |

Gathering Setup Information

Once you know how you will install the appliance in your network, you can gather the necessary information, such as IP addresses, to enter in the System Setup Wizard. You can use the worksheet in Table 4-1 to write down the configuration options you decide on. Then, when you run the System Setup Wizard, you can use the information you enter in the worksheet to configure the initial setup.

Table 4-1 System Setup Worksheet

<table>
<thead>
<tr>
<th>Network Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default System Hostname:</td>
</tr>
<tr>
<td>DNS Servers:</td>
</tr>
<tr>
<td>Internet root DNS servers / organization DNS servers</td>
</tr>
<tr>
<td>Organization DNS Servers:</td>
</tr>
<tr>
<td>(maximum 3)</td>
</tr>
<tr>
<td>1.</td>
</tr>
<tr>
<td>2.</td>
</tr>
<tr>
<td>3.</td>
</tr>
<tr>
<td>Network Time Protocol Server:</td>
</tr>
<tr>
<td>Time Zone Region:</td>
</tr>
<tr>
<td>Time Zone Country:</td>
</tr>
<tr>
<td>Time Zone / GMT Offset:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there another proxy on the network: Yes / No</td>
</tr>
<tr>
<td>Other Proxy IP Address:</td>
</tr>
<tr>
<td>Other Proxy Port:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Port</td>
</tr>
<tr>
<td>IP Address:</td>
</tr>
<tr>
<td>Network Mask:</td>
</tr>
<tr>
<td>Hostname:</td>
</tr>
</tbody>
</table>

| Data Port                                            |

Gathering Setup Information

Once you know how you will install the appliance in your network, you can gather the necessary information, such as IP addresses, to enter in the System Setup Wizard. You can use the worksheet in Table 4-1 to write down the configuration options you decide on. Then, when you run the System Setup Wizard, you can use the information you enter in the worksheet to configure the initial setup.

Table 4-1 System Setup Worksheet

<table>
<thead>
<tr>
<th>Network Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default System Hostname:</td>
</tr>
<tr>
<td>DNS Servers:</td>
</tr>
<tr>
<td>Internet root DNS servers / organization DNS servers</td>
</tr>
<tr>
<td>Organization DNS Servers:</td>
</tr>
<tr>
<td>(maximum 3)</td>
</tr>
<tr>
<td>1.</td>
</tr>
<tr>
<td>2.</td>
</tr>
<tr>
<td>3.</td>
</tr>
<tr>
<td>Network Time Protocol Server:</td>
</tr>
<tr>
<td>Time Zone Region:</td>
</tr>
<tr>
<td>Time Zone Country:</td>
</tr>
<tr>
<td>Time Zone / GMT Offset:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there another proxy on the network: Yes / No</td>
</tr>
<tr>
<td>Other Proxy IP Address:</td>
</tr>
<tr>
<td>Other Proxy Port:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Port</td>
</tr>
<tr>
<td>IP Address:</td>
</tr>
<tr>
<td>Network Mask:</td>
</tr>
<tr>
<td>Hostname:</td>
</tr>
</tbody>
</table>

| Data Port                                            |
### Chapter 4  Installation and Configuration

#### Before You Begin

**IP Address:**

**Network Mask:**

**Hostname:**

**Note:** The Web Proxy can share the Management interface. If configured separately, the Data interface IP address and the Management interface IP address cannot share the same subnet.

#### L4 Traffic Monitor

| L4 Traffic Monitor Wiring Type | Simplex network tap / Duplex network tap |

#### Routes

**Management Traffic**

<table>
<thead>
<tr>
<th>Default Gateway</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Route Table Name</td>
<td></td>
</tr>
<tr>
<td>Static Route Table Destination Network</td>
<td></td>
</tr>
<tr>
<td>Static Route Table Gateway</td>
<td></td>
</tr>
</tbody>
</table>

**Data Traffic**

<table>
<thead>
<tr>
<th>Default Gateway</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Route Table Name</td>
<td></td>
</tr>
<tr>
<td>Static Route Table Destination Network</td>
<td></td>
</tr>
<tr>
<td>Static Route Table Gateway</td>
<td></td>
</tr>
</tbody>
</table>

#### Transparent Connection Settings

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Layer 4 switch or No Device / WCCP Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>If WCCP v2 Router, enable standard service</td>
<td>Yes / No</td>
</tr>
<tr>
<td>Standard Service Router Addresses</td>
<td></td>
</tr>
</tbody>
</table>

| Enable Router Security? | No / Yes, password: ______________________________ |

**Note:** When you connect the appliance to a WCCP router, you might need to configure the Web Security appliance to create WCCP services after you run the System Setup Wizard. For more information about creating WCCP services, see Adding and Editing a WCCP Service, page 25-21.

#### Administrative Settings

| Administrator Password |  |
System Setup Wizard

Table 4-1  System Setup Worksheet (continued)

<table>
<thead>
<tr>
<th>Email System Alerts To:</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Relay Host: (optional)</td>
</tr>
<tr>
<td>AutoSupport: Enable / Disable</td>
</tr>
<tr>
<td>SenderBase Network Participation: Enable / Disable</td>
</tr>
<tr>
<td>Participation Level: Limited / Standard</td>
</tr>
</tbody>
</table>

Security Services

<table>
<thead>
<tr>
<th>L4 Traffic Monitor: Monitor only / Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable Use Controls: Enable IronPort URL Filters / Enable Cisco IronPort Web Usage Controls / Disable</td>
</tr>
<tr>
<td>Web Reputation Filters: Enable / Disable</td>
</tr>
<tr>
<td>Malware and Spyware Scanning: Enable Webroot / Enable McAfee / Enable both</td>
</tr>
<tr>
<td>Action for Detected Malware: Monitor only / Block</td>
</tr>
<tr>
<td>IronPort Data Security Filtering: Enable / Disable</td>
</tr>
</tbody>
</table>

DNS Support

To connect to the management interface using a hostname (http://hostname:8080), you must add the appliance hostname and IP address to your DNS server database.

System Setup Wizard

The IronPort AsyncOS for Web operating system provides a browser-based wizard to guide you through initial system configuration. This System Setup Wizard prompts you for basic initial configuration, such as network configuration and security settings. The System Setup Wizard is located on the System Administration tab.

You must run the System Setup Wizard when you first install the Web Security appliance. After you finish the System Setup Wizard, the appliance is ready to monitor web traffic. However, you may want to make more custom configurations...
to the appliance that the System Setup Wizard does not cover. For more information about configuration options, see most of the other chapters in this guide.

Before you run the System Setup Wizard, see Before You Begin, page 4-1 to verify you have all the information you need to configure the appliance. Having this information prepared ahead of time can reduce the amount of time required to complete the initial setup. You should also read the QuickStart Guide for more information about product setup.

---

**Warning**  
Running the System Setup Wizard completely reconfigures the Web Security appliance and resets the administrator password. Only use the System Setup Wizard the first time you install the appliance, or if you want to completely overwrite the existing configuration. Running the System Setup Wizard after the appliance is already configured can also interrupt client access to the web. If you choose to run the System Setup Wizard after performing an initial setup, use the System Administration > Configuration File pages to print a configuration summary and archive the current configuration file.

---

**Warning**  
The IronPort appliance ships with a default IP address of 192.168.42.42 on the Management interface (port). Before connecting the appliance to the network, ensure that no other device on the network has the same IP address.

---

If you are connecting multiple factory-configured IronPort appliances to your network, add them one at a time, reconfiguring each IronPort appliance’s default IP address as you go.

The System Setup Wizard includes the following tabs where you enter configuration information:

- **Start.** For details, see Step 1. Start, page 4-8.
- **Network.** For details, see Step 2. Network, page 4-9.
Accessing the System Setup Wizard

To access the System Setup Wizard, 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.

The appliance login screen appears. Enter the username and password to access the appliance. By default, the appliance ships with the following username and password:

- Username: admin
- Password: ironport

Note
Your session will time out if it is idle for over 30 minutes or if you close your browser without logging out. If this happens, you must re-enter the username and password.

Step 1. Start

When you first start the System Setup Wizard, it displays an end user license agreement.

Step 1
Accept the terms of the agreement by clicking the check box at the bottom of the page.
Chapter 4 Installation and Configuration

System Setup Wizard

Figure 4-1 System Setup Wizard — Start Tab

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

Welcome to your IronPort Web Security Appliance. Please review and accept the license agreement, then click Begin Setup.

IronPort License Agreement

1. Click Begin Setup to continue.

The Network tab appears.

Step 2 Network

On the Network tab, you configure appliance system properties, such as the appliance hostname and time zone. The first page of the Network tab is the System Settings page.

Step 1 Verify that you are viewing the System Configuration page.
**Chapter 4      Installation and Configuration**

**System Setup Wizard**

**Figure 4-2   System Setup Wizard — Network Tab, System Settings**

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

<table>
<thead>
<tr>
<th>System Settings</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default System Hostname:</strong></td>
<td>tiva1Empresa</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DNS Server(s):</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NTP Server:</strong></td>
<td>time.ironport.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Time Zone:</strong></td>
<td>Region</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Country</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time Zone / GMT Offset</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2** Configure the System Setting options.
Table 4-2 describes the System Setting options.

Table 4-2  System Setting Options in System Setup Wizard

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default System Hostname</td>
<td>The fully-qualified hostname for the Web Security appliance. This name should be assigned by your network administrator. This hostname is used to identify the appliance in system alerts.</td>
</tr>
<tr>
<td>DNS Server(s): Use the Internet’s Root DNS Servers</td>
<td>Configures the appliance to use the Internet root DNS servers for domain name service lookups. You might choose this option when the appliance does not have access to DNS servers on your network. The appliance requires access to a working DNS server in order to perform DNS lookups for incoming connections. If you cannot specify a working DNS server that the appliance can reach while you set up the appliance, you can configure it to use the Internet root DNS servers or temporarily assign the IP address of the Management interface so that you can complete the System Setup Wizard. For more information about configuring DNS settings, see Configuring DNS Server(s), page 25-28.</td>
</tr>
<tr>
<td>DNS Server(s): Use these DNS Servers</td>
<td>Specifies local DNS servers for domain name service lookups. You must enter at least one DNS server, and up to three total. You can choose to use the Internet root DNS servers or specify your own DNS servers. For more information about configuring DNS settings, see Configuring DNS Server(s), page 25-28.</td>
</tr>
</tbody>
</table>
Step 3  Click Next.

The Network Context page appears.

**Figure 4-3  System Setup Wizard — Network Tab, Network Context Page**

<table>
<thead>
<tr>
<th>Network Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there another web proxy in your network?</td>
</tr>
<tr>
<td>After completing the System Setup Wizard, you will have the option to define additional upstream proxies.</td>
</tr>
<tr>
<td>Proxy Group Name:</td>
</tr>
<tr>
<td>Address:</td>
</tr>
<tr>
<td>Port:</td>
</tr>
</tbody>
</table>

If another web proxy is present, the IronPort Web Security Appliance is recommended to be placed downstream of the existing proxy (closer to the client), as illustrated below:

Step 4  Configure the Network Context options by indicating whether or not there exists another proxy server on the network.
You can configure the Web Security appliance to interact with multiple proxy servers on the network after you run the System Setup Wizard. For more information about configuring external proxy servers, see Working with External Proxies Overview, page 9-1.

**Step 5** If there is an external proxy server on the network, configure the proxy settings. Table 4-3 describes the proxy settings.

**Table 4-3** Network Context Options in System Setup Wizard

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy group name</td>
<td>Choose a name for the proxy group.</td>
</tr>
<tr>
<td>Address</td>
<td>Enter the address of the proxy server in your organization network.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number of the proxy server in your organization network.</td>
</tr>
</tbody>
</table>

The System Setup Wizard creates a proxy group with the information you provide in Table 4-3. You can edit the proxy group later to include additional proxy servers and to configure load balancing options. You can also create additional proxy groups after system setup.

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

**Step 6** Click Next.

The Network Interfaces and Wiring page appears.

The Web Security appliance has network interfaces that are associated with the physical ports on the machine.
Step 7 Configure the Network Interfaces and Wiring options.
The appliance has network interfaces that are associated with the physical ports on the machine. Table 4-4 describes the Network Interfaces and Wiring options.
### Table 4-4  Network Interfaces and Wiring Options in System Setup Wizard

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Enter the IP address, network mask, and hostname to use to manage the Web Security appliance. Enter an IP address that exists on your management network. By default, the appliance uses the M1 interface for both management and proxy (data) traffic (the “Use M1 port for management only” check box is disabled). However, optionally, you can use the M1 interface for only management traffic by enabling the “Use M1 port for management only” check box. You might want to do this if your organization uses a separate management network. This can increase security by ensuring no proxy traffic can reach the appliance on management interface. When you use M1 for management traffic only, you must configure at least one data interface for proxy traffic. Also, you must define different routes for management and data traffic.</td>
</tr>
</tbody>
</table>
Step 8  Click Next.

The Routes for Management and Data Traffic page appears.
Step 9 Configure the Routes for Management and Data Traffic options.

The number of sections on this page depend on how you configured the “Use M1 port for management only” check box on the previous wizard page:

- **Enabled.** When you use the Management interface for management traffic only, then this page includes two sections to enter gateway and static route table information, one for management traffic and one for data traffic.

- **Disabled.** When you use the Management interface for both management and data traffic only, then this page includes one section to enter gateway and static route table information. AsyncOS uses the route information for both management and data traffic.
Table 4-5 describes the Routes for Management and Data Traffic options.

### Table 4-5 Routes for Management and Data Traffic Options in System Setup Wizard

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway</td>
<td>Enter the default gateway IP address to use for the traffic through the Management and/or Data interface.</td>
</tr>
<tr>
<td>Static Routes Table</td>
<td>Optionally, you can add one or more static routes for management or data traffic. To add a static route, enter a name for the route, its destination network, and gateway IP address, and then click Add Route. A route gateway must reside on the same subnet as the Management or Data interface on which it is configured. To delete a static route you entered, click the Delete button next to the static route entry in the table. For more information about static routes, see Configuring TCP/IP Traffic Routes, page 25-7.</td>
</tr>
</tbody>
</table>

**Step 10** Click **Next**.

The Transparent Connection Settings page appears. By default, when you run the System Setup Wizard, the Web Proxy is deployed in transparent mode. When the Web Proxy is deployed in transparent mode, you must connect it to a Layer 4 switch or a version 2 WCCP router.
Step 11

Choose one of the following options described in Table 4-6.

**Table 4-6  Transparent Connection Options in System Setup Wizard**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 4 Switch or No Device</td>
<td>Choose this option when the Web Security appliance is connected to a layer 4 switch or if you will deploy the Web Proxy in explicit forward mode after running the System Setup Wizard.</td>
</tr>
<tr>
<td>WCCP v2 Router</td>
<td>Choose this option when the Web Security appliance is connected to a version 2 WCCP capable router.</td>
</tr>
<tr>
<td></td>
<td>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 (also known as the “web-cache” service) during system setup, and you can configure different or additional WCCP service groups after you run the System Setup Wizard.</td>
</tr>
<tr>
<td></td>
<td>When you enable the standard service, choose whether or not to require a password for the standard service group. If required, enter the password in the password fields. The password can contain up to seven characters.</td>
</tr>
<tr>
<td></td>
<td>For more information about creating WCCP services, see Adding and Editing a WCCP Service, page 25-21.</td>
</tr>
</tbody>
</table>
Step 12 Click Next.

The Administrative Settings page appears.

*Figure 4-7 System Setup Wizard — Network Tab, Administrative Settings Page*

Step 13 Configure the Administrative Settings options.

*Table 4-7 describes the Administrative Settings.*

*Table 4-7 Administrative Settings in System Setup Wizard*

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Password</td>
<td>Enter a password to access the Web Security appliance. The password must be six characters or more.</td>
</tr>
<tr>
<td>Email System Alerts To</td>
<td>Enter an email address for the account to which the appliance sends alerts. For more information about alerts, see Managing Alerts, page 26-22.</td>
</tr>
</tbody>
</table>
Step 14  Click Next.

The Security tab appears.

Step 3. Security

On the Security tab, you can configure which security services to enable, such as whether to block or monitor certain components. The Security tab contains one page.

Table 4-7  Administrative Settings in System Setup Wizard (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Email via SMTP Relay Host</td>
<td>You can enter a hostname or address for an SMTP relay host that AsyncOS uses for sending system generated email messages. Optionally, you can enter the port number, too. If no port number is defined, AsyncOS uses port 25. If no SMTP relay host is defined, AsyncOS uses the mail servers listed in the MX record. For more information about configuring the SMTP relay hosts, see Configuring SMTP Relay Hosts, page 25-26.</td>
</tr>
<tr>
<td>AutoSupport</td>
<td>Choose whether or not the appliance sends system alerts and weekly status report to IronPort Customer Support.</td>
</tr>
<tr>
<td>SenderBase Network Participation</td>
<td>Choose whether or not to participate in the SenderBase Network. If you participate, you can configure limited or full participation. The SenderBase 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 SenderBase Network Participation, the Web Security appliance sends anonymous statistics about HTTP requests to IronPort to increase the value of SenderBase Network data. For more information about the SenderBase Network, see The SenderBase Network, page 2-5.</td>
</tr>
</tbody>
</table>
Step 1
Verify that you are viewing the Security tab.

**Figure 4-8  System Setup Wizard — Security Tab**

<table>
<thead>
<tr>
<th>Security Settings</th>
<th>Action for Suspicious Malware Addresses</th>
<th>Acceptable Use Controls:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>() Monitor only</td>
<td>(F) Enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Global Access Policy will be initially configured to monitor all pre-defined categories.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acceptable Use Controls Services:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(T) IronPort URL Filters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(R) Cisco IronPort Web Usage Controls</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web Reputation Filters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(F) Enable</td>
</tr>
<tr>
<td>The Global Access Policy will be initially configured to use Web Reputation Filtering.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Malware and Spyware Scanning:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(F) Enable Kaspersky</td>
</tr>
<tr>
<td>(F) Enable McAfee</td>
</tr>
<tr>
<td>(F) Enable Sophos</td>
</tr>
<tr>
<td>The Global Access Policy and Outbound Malware Scanning Policy will be initially configured to apply the actions configured below.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action for Detected Malware:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(F) Monitor only</td>
</tr>
<tr>
<td>(F) Block</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IronPort Data Security Filtering:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(F) Enable</td>
</tr>
<tr>
<td>The Global IronPort Data Security Policy will be initially configured to block uploads based on Web Reputation (if enabled) and monitor all other uploads.</td>
</tr>
</tbody>
</table>

Step 2
Choose the Security Services options.
Table 4-8 describes the Security options.

**Table 4-8 Security Options in System Setup Wizard**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L4 Traffic Monitor</td>
<td>Choose whether the Layer-4 Traffic Monitor should monitor or block layer 4 traffic. The L4 Traffic Monitor detects rogue traffic across all network ports and stops malware attempts to bypass port 80. You might choose to monitor traffic when you evaluate the Web Security appliance, and block traffic when you purchase and use the appliance. For more information, see Configuring the L4 Traffic Monitor, page 21-3.</td>
</tr>
<tr>
<td>Acceptable Use Controls</td>
<td>Choose whether or not to enable Acceptable Use Controls so you can choose a URL filtering engine, either Cisco IronPort Web Usage Controls or IronPort URL Filters. URL filtering engines allow you to control user access based on the category of a URL in a request. Enable this option when you want to restrict users from accessing particular types of websites. <strong>Note:</strong> If you enable Cisco IronPort Web Usage Controls, the Dynamic Content Analysis engine is enabled by default. You can edit this setting after system setup. For more information, see URL Filters, page 16-1.</td>
</tr>
</tbody>
</table>
Table 4-8  Security Options in System Setup Wizard (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Reputation Filters</td>
<td>Choose whether or not to enable Web Reputation filtering for the Global Policy Group. When you create custom Access Policy groups, you can choose whether or not to enable Web Reputation filtering. IronPort Web Reputation Filters is a security feature that analyzes web server behavior and assigns a reputation score to a URL to determine the likelihood that it contains URL-based malware. Enable this option when you want to identify suspicious activity and stop malware attacks before they occur. For more information, see Web Reputation Filters, page 18-1.</td>
</tr>
<tr>
<td>Malware and Spyware Scanning</td>
<td>Choose whether or not to enable malware and spyware scanning using Webroot, McAfee, or Sophos. If enabled, also choose whether to monitor or block detected malware. You might choose to monitor malware when you evaluate the Web Security appliance, and block malware when you purchase and use the appliance. You can further configure malware scanning after you finish the System Setup Wizard. For details, see Configuring Anti-Malware Scanning, page 19-10.</td>
</tr>
<tr>
<td>IronPort Data Security Filtering</td>
<td>Choose whether or not to enable IronPort Data Security Filters. The IronPort Data Security Filters evaluate data leaving the network over HTTP, HTTPS, and FTP to control what data goes where and how and by whom. Enable this option when you want to create IronPort Data Security Policies to block particular types of upload requests. For more information, see Data Security and External DLP Policies Overview, page 12-1.</td>
</tr>
</tbody>
</table>

Step 3  Click Next.
The Review tab appears.

**Step 4. Review**

The last tab of the System Setup Wizard displays a summary of the configuration information you chose. You can edit any of the configuration options by clicking the **Edit** button for each section.

**Step 1** Verify that you are viewing the Review tab.
**Figure 4-9  System Setup Wizard — Review Tab**

**Review Your Configuration**

Please review your configuration. If you need to make changes, click the Previous button to return to the previous page.

<table>
<thead>
<tr>
<th>Network Settings</th>
</tr>
</thead>
</table>
| Default System Hostname: | visasilpa  
| DNS Servers: | 152.160.1.10  
| Network Time Protocol (NTP): | time.ispport.com  
| Time Zone: | UTC  

<table>
<thead>
<tr>
<th>Network Contacts</th>
</tr>
</thead>
</table>
| Upstream proxy: | No upstream proxy  

<table>
<thead>
<tr>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management (M1)</td>
</tr>
</tbody>
</table>
| IP Address: | 152.160.1.115  
| Network Mask: | 255.255.255.0  
| Hostname: | visasilpa  
| Use M port for management only: | Yes  

<table>
<thead>
<tr>
<th>Data (P1)</th>
</tr>
</thead>
</table>
| IP Address: | 152.160.2.115  
| Network Mask: | 255.255.255.0  
| Hostname: | visasilpa  

<table>
<thead>
<tr>
<th>L4 Traffic Monitor:</th>
</tr>
</thead>
</table>
| Wire Type: | Dulsan TAP: T1 (In/Out)  

<table>
<thead>
<tr>
<th>Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management (M1)</td>
</tr>
</tbody>
</table>
| Default Gateway: | 152.160.1.1  
| Static Routes: | No static routes have been defined.  

<table>
<thead>
<tr>
<th>Data (P1)</th>
</tr>
</thead>
</table>
| Default Gateway: | 152.160.2.1  
| Static Routes: | No static routes have been defined.  

<table>
<thead>
<tr>
<th>Management Communication Settings</th>
</tr>
</thead>
</table>
| Transitec Redirection Device Type: | Layer 4 Switch or No Device  

<table>
<thead>
<tr>
<th>Administrative Settings</th>
</tr>
</thead>
</table>
| Administrator Password: | (Not Set)  
| Email System Alerts To: | sample@example.com  
| Internal SMTP Relay Host: | No internal relay host is defined  
| AutoSupport: | Yes  
| SendHone Network Participant: | Yes  

<table>
<thead>
<tr>
<th>Security Settings</th>
</tr>
</thead>
</table>
| L4 Traffic Monitor: | Monitoring  
| Acceptable Use Controls: | Enabled  
| Active Acceptable Use Controls Engine: | Cisco IronPort Web Usage Controls  
| Web Reputation Filters: | Enabled  
| IronPort DVS™ Engine: | Websort: Enabled  
| NGQDM: Enabled  
| SoPhen: Enabled  
| IronPort Data Security Filtering: | Enabled  

**Step 2** Review the configuration information. If you need to change an option, click the Edit button for that section.
Step 3 Click **Install This Configuration** after you confirm the configuration is correct. The Web Security appliance applies the configuration options you selected.

If you changed the Management interface IP address from the current value, then clicking **Install This Configuration** will cause the connection to the current URL to be lost. However, your browser will redirect itself to the new IP address. If you did not change the IP address from the current value, the System Administration > System Setup > Next Steps page appears.

### System Setup Next Steps

Welcome to your IronPort appliance! System setup is complete. Your IronPort appliance should now be configured to work within your network infrastructure. See below for additional tasks and information:

<table>
<thead>
<tr>
<th>Access Policies</th>
<th>Enter Feature Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Web Security Manager to set up access policies.</td>
<td>You enabled several features during System Setup. In order to continue to enjoy these features beyond the initial trial period, you must enter valid feature keys.</td>
</tr>
<tr>
<td>Configure Access Policies</td>
<td>Enter Feature Keys</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reports</th>
<th>Send Configuration File</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IronPort appliance generates, delivers, and archives periodic reports on web security for your organization.</td>
<td>Click the link below to send a copy of the current configuration file to <a href="mailto:admin@example.com">admin@example.com</a>. This file can be used to restore your initial System Setup Wizard defaults if necessary.</td>
</tr>
<tr>
<td>Schedule Reports</td>
<td>Send Configuration File</td>
</tr>
</tbody>
</table>
Web Proxy Services

This chapter contains the following information:

- About Web Proxy Services, page 5-1
- Configuring the Web Proxy, page 5-3
- Working with FTP Connections, page 5-8
- Bypassing the Web Proxy, page 5-15
- Bypassing Application Scanning, page 5-18
- Proxy Usage Agreement, page 5-18
- Configuring Client Applications to Use the Web Proxy, page 5-19
- Working with PAC Files, page 5-19
- Adding PAC Files to the Web Security Appliance, page 5-24
- Advanced Proxy Configuration, page 5-30

About Web Proxy Services

A web proxy is a computer system or software that handles World Wide Web requests of clients by making requests of other servers on the web. The Web Security appliance can act as a web proxy if you enable the Web Proxy feature.

The Web Proxy service monitors and controls traffic that originates from clients on the internal network. Typically, the Web Proxy-enabled Web Security appliance is deployed between clients and the firewall where it intercepts requests for content from clients to servers.
You can configure the Web Proxy as one of the following types:

- **Transparent Proxy.** When the appliance is configured as a transparent proxy, clients are unaware of the Web Proxy. Client applications, such as web browsers, do not have to be configured to accommodate the appliance. You might want to configure the appliance as a transparent proxy because it eliminates the possibility of users reconfiguring their web browsers to bypass the appliance without knowledge of the administrator. To configure the appliance as a transparent proxy, you must connect it to an L4 switch or a WCCP router.

  For information about how to configure the appliance when you configure the proxy in transparent mode, see Configuring Transparent Redirection, page 25-17.

- **Explicit Forward Proxy.** In an explicit forward proxy configuration, the appliance acts on behalf of client web browsers to handle requests for servers on the web. Users must configure their web browsers to point to a single Web Security appliance. You might want to configure the appliance as an explicit forward proxy if you do not have an L4 switch or a WCCP router.

  You can use the Web Security appliance in a network that includes another proxy server. For more information about how to deploy and configure the appliance when the network contains another proxy, see Using the Web Security Appliance in an Existing Proxy Environment, page 3-15.

  The Web Proxy handles both HTTP and native FTP transactions. For more information about working with FTP, see Working with FTP Connections, page 5-8.

### Web Proxy Cache

By default, AsyncOS uses a web proxy cache to increase performance for users accessing the web in some cases.

You can edit the web proxy and proxy cache in the following ways:

- **Remove a URL from the cache.** Use the `evict` subcommand of the `webcache` CLI command to remove one or more URLs from the cache.

- **Specify a domain or URL to never cache.** Use the `ignore` subcommand of the `webcache` CLI command to specify one or more domains or URLs that the web proxy should never store in the proxy cache. You can include embedded regular expression (regex) characters in the URL you specify to never cache.
Each access log file entry includes transaction result codes that describe how the appliance resolved client requests. Transaction result codes indicate whether the transaction was served from the proxy cache or from the destination server. For more information about transaction result codes, see Transaction Result Codes, page 24-23.

Configuring the Web Proxy

Web Proxy settings are configured as part of an initial setup using the System Setup Wizard. To enable Web Proxy services or modify proxy settings after an initial configuration, use the Security Services > Web Proxy page. This page allows you to configure basic and advanced settings to customize proxy services.

The Web Proxy settings apply to all connections that go over HTTP or HTTPS. To configure proxy settings for native FTP connections, see Working with FTP Connections, page 5-8.

To edit the Web Proxy settings:

**Step 1** Navigate to the Security Services > Web Proxy page.

**Step 2** Click Edit Settings.
Figure 5-1  Editing Web Proxy Settings

Edit Web Proxy Settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| HTTP Ports to Proxy | Enter which ports the Web Proxy monitors for HTTP requests.  
 Default is 80 and 3128. |
| Caching          | Choose whether or not the Web Proxy should cache requests and responses.  
 Default is enabled. |
Chapter 5  Web Proxy Services

Configuring the Web Proxy

Chapter 5      Web Proxy Services

Configuring the Web Proxy

Proxy Mode Choose how to deploy the Web Proxy:

- **Transparent mode.** Clients applications are unaware of the Web Proxy and do not have to be configured to connect to the proxy. In transparent mode, the Web Proxy can accept both transparently redirected and explicitly forwarded connections. For more information, see Deploying the Web Proxy in Transparent Mode, page 3-7.

- **Explicit forward mode.** Client applications, such as web browsers, are aware of the Web Proxy and must be configured to point to a single Web Security appliance. In explicit forward mode, the Web Proxy can only accept explicitly forwarded connections. For more information, see Deploying the Web Proxy in Explicit Forward Mode, page 3-6.

IP Spoofing Choose whether or not the Web Proxy should spoof IP addresses when sending requests to upstream proxies and servers.

When the Web Proxy is deployed in transparent mode, you can enable IP spoofing for transparently redirected connections only or all connections (transparently redirected and explicitly forwarded).

When IP spoofing is enabled, requests originating from a client retain the client’s source address and appear to originate from the client rather than from the Web Security appliance.

**Note:** When IP spoofing is enabled and the appliance is connected to a WCCP router, configure a WCCP service to redirect the return path.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Mode</td>
<td>Choose how to deploy the Web Proxy:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Transparent mode.</strong> Clients applications are unaware of the Web Proxy and do not have to be configured to connect to the proxy. In transparent mode, the Web Proxy can accept both transparently redirected and explicitly forwarded connections. For more information, see Deploying the Web Proxy in Transparent Mode, page 3-7.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Explicit forward mode.</strong> Client applications, such as web browsers, are aware of the Web Proxy and must be configured to point to a single Web Security appliance. In explicit forward mode, the Web Proxy can only accept explicitly forwarded connections. For more information, see Deploying the Web Proxy in Explicit Forward Mode, page 3-6.</td>
</tr>
<tr>
<td>IP Spoofing</td>
<td>Choose whether or not the Web Proxy should spoof IP addresses when sending requests to upstream proxies and servers.</td>
</tr>
<tr>
<td></td>
<td>When the Web Proxy is deployed in transparent mode, you can enable IP spoofing for transparently redirected connections only or all connections (transparently redirected and explicitly forwarded).</td>
</tr>
<tr>
<td></td>
<td>When IP spoofing is enabled, requests originating from a client retain the client’s source address and appear to originate from the client rather than from the Web Security appliance.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When IP spoofing is enabled and the appliance is connected to a WCCP router, configure a WCCP service to redirect the return path.</td>
</tr>
</tbody>
</table>
Table 5-1  Web Proxy Settings (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistent Connection Timeout</td>
<td>Enter how long the Web Proxy keeps open a connection to a client or server after a transaction has been completed. Keeping a connection open allows the Web Proxy to use it again for another request. For example, after a client finishes a transaction with google.com, the Web Proxy keeps the connection to the server google.com open for the amount of time specified in the server side persistent timeout if no other client makes a request for google.com.</td>
</tr>
</tbody>
</table>
|                                    | • **Client side**. The maximum number of seconds the Web Proxy keeps a connection open with a client on the network with no activity from the client.  
|                                    | • **Server side**. The maximum number of seconds the Web Proxy keeps a connection open with a destination server with no activity from any client on the network to that server.  
|                                    | Default is 300 seconds for both client and server side persistent timeouts. You might want to increase the server side persistent timeout if clients on the network frequently connect to the same server, or if the network has a relatively slow connection to outside servers. Cisco recommends keeping the default values. However, you might want to increase or decrease these values to keep connections open longer to reduce overhead used to open and close connections repeatedly. Consider that if you increase the persistent timeout values, you also reduce the ability of the Web Proxy to open new connections if the maximum number of simultaneous persistent connections has been reached. |
Configuring the Web Proxy

In-Use Connection Timeout

Enter how long the Web Proxy waits for more data from an idle client or server when the current transaction has not been completed.

For example, if a client opens a connection and sends only half of the request, the Web Proxy waits for the amount of time specified for the client side reserve timeout for the rest of the request before closing the open connection.

- **Client side.** The maximum number of seconds the Web Proxy keeps a connection open with an idle client.
- **Server side.** The maximum number of seconds the Web Proxy keeps a connection open with an idle destination server.

Default is 300 seconds for both client and server side reserve timeouts.

Simultaneous Persistent Connections (Server Maximum Number)

Enter the maximum number of connections (sockets) the Web Proxy keeps open with servers.

**Headers**

- **X-Forwarded-For.** Choose whether or not to forward HTTP “X-Forwarded-For” headers. Default is Do Not Send.

  Note: If the network contains an explicit forward upstream proxy that manages user authentication or access control using proxy authentication, you must enable the X-Forwarded-For header to send the client host header to the upstream proxy.

- **VIA.** Choose whether or not to forward HTTP “VIA” headers in HTTP requests from clients and HTTP responses from servers. Default is Send.

*Table 5-1 Web Proxy Settings (continued)*

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-Use Connection Timeout</td>
<td>Enter how long the Web Proxy waits for more data from an idle client or server when the current transaction has not been completed. For example, if a client opens a connection and sends only half of the request, the Web Proxy waits for the amount of time specified for the client side reserve timeout for the rest of the request before closing the open connection.  - <strong>Client side.</strong> The maximum number of seconds the Web Proxy keeps a connection open with an idle client.  - <strong>Server side.</strong> The maximum number of seconds the Web Proxy keeps a connection open with an idle destination server. Default is 300 seconds for both client and server side reserve timeouts.</td>
</tr>
<tr>
<td>Simultaneous Persistent Connections (Server Maximum Number)</td>
<td>Enter the maximum number of connections (sockets) the Web Proxy keeps open with servers.</td>
</tr>
</tbody>
</table>
| Headers |  - **X-Forwarded-For.** Choose whether or not to forward HTTP “X-Forwarded-For” headers. Default is Do Not Send.  
  Note: If the network contains an explicit forward upstream proxy that manages user authentication or access control using proxy authentication, you must enable the X-Forwarded-For header to send the client host header to the upstream proxy.  
  - **VIA.** Choose whether or not to forward HTTP “VIA” headers in HTTP requests from clients and HTTP responses from servers. Default is Send. |
Working with FTP Connections

The Web Security appliance Web Proxy provides proxy services for the File Transfer Protocol (FTP) as well as HTTP. FTP is a protocol used to transfer data between computers over a network. The Web Proxy can handle the following FTP transactions:

- **FTP over HTTP.** Most web browsers support FTP transactions, but sometimes the transactions are encoded inside an HTTP transaction. All policies and configuration options that apply to HTTP transactions also apply to FTP over HTTP transactions.

- **Native FTP.** FTP clients use FTP to transfer data without invoking an HTTP connection. Native FTP connections are treated and handled differently than HTTP connections.

The component of the Web Proxy that handles native FTP transactions is referred to as the FTP Proxy.

Native FTP connections can be served when the Web Proxy is deployed in either transparent or explicit forward mode.

Computers that transfer data using FTP create two connections between them. The control connection is used to send and receive FTP commands, such as RETR and STOR, and to communicate other information, such as the connection mode and file properties. The data connection is used to transfer the data itself. Typically, computers use port 21 for the control connection, and use a randomly assigned port (usually greater than 1023) for the data connection.

The FTP Proxy supports the following connection modes:

- **Passive.** In passive mode, the FTP server chooses the port used for the data connection and communicates this assignment to the FTP client. Passive mode is typically favored in most network environments where the FTP client is located behind a firewall and inbound connections (such as from an FTP server) are blocked. The default for the FTP Proxy is passive mode.

- **Active.** In active mode, the FTP client chooses the port used for the data connection and communicates this assignment to the FTP server.

Consider the following rules and guidelines when working with native FTP connections:

- You can define which Identity groups apply to native FTP transactions.
You configure FTP Proxy settings that apply to native FTP connections. For more information, see Configuring FTP Proxy Settings, page 5-11.

You can configure which welcome message users see in the FTP client when they connect to an FTP server. Configure the welcome banner when you configure the FTP Proxy settings.

You can define a custom message the FTP Proxy displays in IronPort FTP notification messages when there is an error with FTP Proxy authentication. For more information, see Working with IronPort FTP Notification Messages, page 15-23.

When the FTP Proxy is configured to cache native FTP transactions, it only caches content accessed by anonymous users.

You can configure the FTP Proxy to spoof the IP address of the FTP server. You might want to do this when FTP clients do not allow passive data connections when the source IP address of the data connection (FTP server) is different than the source IP address of the control connection (FTP Proxy).

If the connection between the FTP Proxy and the FTP server is slow, uploading a large file may take a long time when IronPort Data Security Filters are enabled. If the FTP client times out before the FTP Proxy uploads the entire file, users may notice a failed transaction.

### Using Authentication with Native FTP

The FTP Proxy performs user authentication to control which users can make native FTP requests. This user authentication determines which policy groups apply to the native FTP transaction.

However, due to the nature of FTP and FTP clients, only explicit forward connections can authenticate users for native FTP transactions. Due to this limitation, you must configure at least one Identity and Access Policy for native FTP transactions that do not require authentication when the Web Proxy is deployed in transparent mode. This allows FTP connections that are transparently redirected to the Web Security appliance to work. If authentication is required for all policy groups, transparently redirected native FTP transaction will fail.

You can configure the authentication format the FTP Proxy uses when communicating with FTP clients. The FTP Proxy supports the following formats for proxy authentication:

- **Check Point.** Uses the following formats:
Working with FTP Connections

- User: ftp_user@proxy_user@remote_host
- Password: ftp_password@proxy_password

- **Raptor.** Uses the following formats:
  - User: ftp_user@remote_host proxy_user
  - Password: ftp_password
  - Account: proxy_password

When using authentication with native FTP, ensure that the FTP client uses the same authentication settings configured for the FTP Proxy.

---

**Note**

Be careful when requiring authentication for native FTP transactions. FTP is inherently insecure because data (including the authentication credentials) is transmitted directly over the wire without encryption.

---

**Working with Native FTP in Transparent Mode**

When the Web Security appliance is deployed in transparent mode, FTP clients typically are not explicitly configured to use the FTP Proxy. Native FTP connections are transparently redirected to the FTP Proxy and then processed.

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, the FTP Proxy only matches native FTP transactions with IP addresses configured in the Access Policies.

The predefined URL categories and Web Reputation Filters block by hostname and IP address, but for some servers, they may only have hostname information and not the server’s IP address. For example, if the “News” predefined URL category contains the cnn.com, but not the corresponding IP address for that server, and if that URL category is configured to block, then native FTP connections to cnn.com will successfully connect instead of being blocked. Therefore, to make sure the FTP Proxy blocks native FTP connections to certain sites, you must create custom URL categories and enter the IP addresses in the list of sites to block or in the regular expression field.
Configuring FTP Proxy Settings

The FTP Proxy settings apply to native FTP connections. To configure proxy settings that apply to FTP over HTTP connections, configure the Web Proxy. For more information, see Configuring the Web Proxy, page 5-3.

To configure the FTP Proxy settings:

**Step 1** Navigate to the Security Services > FTP Proxy page, and click **Edit Settings**.

![Configuring FTP Proxy Settings](image)

**Figure 5-2 Configuring FTP Proxy Settings**

**Edit FTP Proxy Settings**

<table>
<thead>
<tr>
<th>FTP Proxy Settings</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proxy Listening Port:</td>
<td>8021</td>
<td></td>
</tr>
<tr>
<td>Caching:</td>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>Server Side IP Sourcing:</td>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>Authentication Format:</td>
<td>Check Point</td>
<td></td>
</tr>
<tr>
<td>Passive Mode Data Port Range:</td>
<td>1000-11009</td>
<td></td>
</tr>
<tr>
<td>Active Mode Data Port Range:</td>
<td>1000-12009</td>
<td></td>
</tr>
<tr>
<td>Active Mode Failover:</td>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>Welcome Banner:</td>
<td>Use FTP Server message</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This option will not be available when the proxy is configured in exploit forward mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use Custom message</td>
<td></td>
</tr>
</tbody>
</table>

**Advanced Settings**

- **Central Connection Timeouts**
  - Client Side: 000 seconds
  - Server Side: 000 seconds

- **Data Connection Timeouts**
  - Client Side: 000 seconds
  - Server Side: 000 seconds

**Step 2** Verify the Enable FTP Proxy field is selected.
### Step 3
Configure the basic and advanced FTP Proxy settings defined in Table 5-2.

**Table 5-2 FTP Proxy Settings**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Listening Port</td>
<td>Specify the port FTP clients should use to establish a control connection with the FTP Proxy.</td>
</tr>
<tr>
<td>Caching</td>
<td>Choose whether or not to cache contents of data connections from anonymous users.</td>
</tr>
<tr>
<td>Server Side IP Spoofing</td>
<td>Choose whether or not the FTP Proxy should spoof the FTP server IP address. You might want to do this for FTP clients that do not allow transactions when the IP address is different for the control and data connections.</td>
</tr>
<tr>
<td>Authentication Format</td>
<td>Choose the authentication format the FTP Proxy uses when communicating with FTP clients. For more information, see Using Authentication with Native FTP, page 5-9.</td>
</tr>
<tr>
<td>Passive Mode Data Port Range</td>
<td>Specify a range of TCP ports FTP clients should use to establish a data connection with the FTP Proxy for passive mode connections. Default is 11000-11009.</td>
</tr>
<tr>
<td>Active Mode Data Port Range</td>
<td>Specify a range of TCP ports FTP servers should use to establish a data connection with the FTP Proxy for active mode connections. Default is 12000-12009. You might want to increase the port range in this field to accommodate more requests from the same FTP server. Because of the TCP session TIME-WAIT delay (usually a few minutes), a port does not become available again for the same FTP server immediately after being used. As a result, any given FTP server cannot connect to the FTP Proxy in active mode more than ( n ) times in a short period of time, where ( n ) is the number of ports specified in this field.</td>
</tr>
</tbody>
</table>
Table 5-2  FTP Proxy Settings (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Mode Failover</td>
<td>When this option is enabled, the FTP Proxy will attempt an active mode connection with the FTP server when passive mode fails. This option affects the connection between the FTP Proxy and the FTP server. It does not affect the connection between the FTP client and the FTP Proxy.</td>
</tr>
<tr>
<td>Welcome Banner</td>
<td>Choose which welcome message should appear in FTP clients:</td>
</tr>
<tr>
<td></td>
<td>• FTP server message. The FTP server message only displays for transparently redirected connections. When a native FTP connection is explicitly sent to the FTP Proxy, the FTP client displays a message predefined by the FTP Proxy.</td>
</tr>
<tr>
<td></td>
<td>• Custom message. Enter a message to display for all native FTP connections.</td>
</tr>
</tbody>
</table>
## Control Connection Timeouts

Enter how long the FTP Proxy waits for more communication in the control connection from an idle FTP client or FTP server when the current transaction has not been completed.

For example, if an FTP client opens a control connection and sends some requests, the FTP Proxy waits for the amount of time specified for the client side control connection timeout for the next request before closing the open connection.

- **Client side.** The maximum number of seconds the FTP Proxy keeps a control connection open with an idle client.
- **Server side.** The maximum number of seconds the FTP Proxy keeps a control connection open with an idle FTP server.

Default is 300 seconds for both client and server side control connection timeouts.

### Table 5-2  FTP Proxy Settings (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Connection Timeouts</td>
<td>Enter how long the FTP Proxy waits for more communication in the control connection from an idle FTP client or FTP server when the current transaction has not been completed. For example, if an FTP client opens a control connection and sends some requests, the FTP Proxy waits for the amount of time specified for the client side control connection timeout for the next request before closing the open connection. - <strong>Client side.</strong> The maximum number of seconds the FTP Proxy keeps a control connection open with an idle client. - <strong>Server side.</strong> The maximum number of seconds the FTP Proxy keeps a control connection open with an idle FTP server. Default is 300 seconds for both client and server side control connection timeouts.</td>
</tr>
</tbody>
</table>
Bypassing the Web Proxy

You can configure the Web Security appliance so client requests to or from particular addresses bypass all processing by the Web Proxy. The proxy bypass list only works for requests that are transparently redirected to the Web Proxy using an L4 switch or a WCCP v2 router. When the appliance is deployed in explicit forward mode, or when a client makes an explicit request to the Web Proxy, the request is processed by the Web Proxy.

You might want to create a proxy bypass list to accomplish any of the following:

- Prevent the Web Proxy from interfering with non-HTTP-compliant (or proprietary) protocols using HTTP ports that do not work properly when they connect to a proxy server.

Step 4 Submit and commit your changes.

---

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Connection Timeouts</td>
<td>Enter how long the FTP Proxy waits for more communication in the data connection from an idle FTP client or FTP server when the current transaction has not been completed. For example, if an FTP client opens a data connection and sends only half of the request, the FTP Proxy waits for the amount of time specified for the client side data connection timeout for the rest of the request before closing the open connection.</td>
</tr>
<tr>
<td>Client side</td>
<td>The maximum number of seconds the FTP Proxy keeps a data connection open with an idle client.</td>
</tr>
<tr>
<td>Server side</td>
<td>The maximum number of seconds the FTP Proxy keeps a data connection open with an idle FTP server. Default is 300 seconds for both client and server side data connection timeouts.</td>
</tr>
</tbody>
</table>
Bypassing the Web Proxy

- 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.

Define the proxy bypass list on the Web Security Manager > Bypass Settings page.

Figure 5-3 shows a sample proxy bypass list.

**Figure 5-3 Proxy Bypass List**

To include an address in the proxy bypass list, click **Edit Proxy Bypass Settings**. You can enter multiple addresses separated by line breaks or commas. You can enter addresses using any of the following formats:

- IP address, such as 10.1.1.0
- CIDR address, such as 10.1.1.0/24
- Hostname, such as crm.example.com
- domain names, such as example.com

**Note**
For the proxy bypass list to work with domain names, you need to connect the T1 and T2 network interfaces to the network **even if you do not enable the L4 Traffic Monitor**. For more information, see **How the Proxy Bypass List Works, page 5-17**.

When transactions bypass the Web Proxy, AsyncOS for Web records them in the proxy bypass logs. For more information about logging, see **Working with Log Subscriptions, page 24-9**.

**Note**
If the proxy bypass list contains an address that is a known malware address according to the L4 Traffic Monitor and the L4 Traffic Monitor sees a request for that address, then the request will still be blocked by the L4 Traffic Monitor. If
you want to ensure traffic to that address is always allowed, you must also bypass
the address from the L4 Traffic Monitor. For more information, see How the L4

**How the Proxy Bypass List Works**

When the Web Proxy receives an HTTP or HTTPS request, it checks both the
source and destination IP address to see if it is in the proxy bypass list. If it is, the
packet is sent to the next hop on the network. (In some cases, the packet is sent
back to the transparent redirection device that redirected the packet, if the packet
arrived on a WCCP service using GRE.)

The proxy bypass list works by matching the IP addresses of the request to an IP
address in the proxy bypass list. When names are entered in the bypass list, the
Web Proxy must resolve them to an IP address using DNS. The Web Proxy DNS
resolves hostnames differently than domain names:

- **Hostnames.** Hostnames are resolved to IP addresses using DNS queries
  immediately after they are entered into the proxy bypass list. (An example
  hostname is www.example.com.)

- **Domain names.** Domain names cannot be resolved to IP addresses using
  DNS queries, so the Web Proxy uses DNS snooping using the T1 and T2
  network interfaces. (An example domain name is example.com, and it
  matches both www.example.com and webmail.example.com.)

Because of these differences, if the proxy bypass list contains only IP addresses
and hostnames, then the Web Proxy can easily match the IP address in the request
header to the IP addresses in the proxy bypass list.

However, for the proxy bypass list to work with domain names, you must connect
both the T1 and T2 network interfaces (if using simplex mode) or just connect the
T1 network interface (if using duplex mode) to the network even if you do not
enable the L4 Traffic Monitor. However, the proxy bypass list only bypasses the
Web Proxy scanning. It does not bypass the L4 Traffic Monitor.

**Note**

If the transparent redirection device is a WCCP router, some are intelligent
enough to not forward any other packets to the Web Proxy for the same session.
In this case, the packets are not physically sent to the Web Proxy for the rest of
the session and are truly bypassing it for the rest of the session.
Using WCCP with the Proxy Bypass List

When the Web Security appliance is configured to use a WCCP v2 router, you must ensure that all WCCP services defined in the Web Security appliance use the same forwarding and return method (either L2 or GRE) to work properly with the proxy bypass list. If the forwarding and return methods do not match, some WCCP enabled routers will act inconsistently.

For more information, see Working with the Forwarding and Return Method, page 25-19.

Bypassing Application Scanning

To bypass an application from Web Proxy scanning:

Step 1 Navigate to the Web Security Manager > Bypass Settings page.
Step 2 Click Edit Application Bypass Settings.
The Edit Application Scanning Bypass Settings page appears.

Step 3 Enable Bypass Scanning for the application to bypass.
Step 4 Submit and commit your changes.

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 acknowledgement page when a user first accesses a browser after a certain period of time. When the end-user acknowledgement page appears, users
Configuring Client Applications to Use the Web Proxy

Web browsers and other user agents sometimes need to know how to connect to the Web Proxy in order to access the World Wide Web. When you deploy the Web Security appliance in explicit forward mode, you must configure client applications so they use the Web Proxy. If you deploy the appliance in transparent mode, you can choose whether or not to configure client applications to explicitly use the Web Proxy.

You can configure client applications to explicitly use the Web Proxy by using any of the following configuration methods:

- **Manual.** Manual configuration involves typing the Web Security appliance hostname and port number, such as 3128, in each client application. If the appliance changes, you must edit each application individually. You might want to manually configure an application when you are testing proxy access on a single client machine. IronPort does not recommend manually configuring each client application to use the appliance Web Proxy.

- **Proxy auto-config (PAC) file.** For web browsers, you can configure each browser to use a PAC file to find the Web Proxy. Then you can edit the PAC file to specify the appliance Web Proxy information. For more information, see Working with PAC Files, page 5-19.

For more information about how to configure client applications to use a proxy, see the client application documentation.

Working with PAC Files

A proxy auto-config (PAC) file is a text file that defines how web browsers can automatically choose the appropriate proxy server for fetching a given URL.
When you use a PAC file, you only need to configure each browser once with the PAC file information. Then, you can edit the PAC file multiple times to add, delete, or change Web Proxy connection information without editing each browser. This way you can configure the proxy information about your network in a centralized location and update it easily.

**Note**

Once a browser has read a PAC file, it stores it in memory for the remainder of the browser session.

You might want to use a PAC file for the following reasons:

- **Centralized management.** You can manage the PAC file in a single, central location.
- **Complex network environment.** If the network of proxy servers is complicated, you can create a PAC file to accommodate different server and client needs.
- **Changing network environment.** If your network environment is likely to change in the future, you can easily add, edit, or delete proxy servers in the PAC and have the changes automatically affect all browsers.
- **Failover.** If you have multiple proxy servers, you can provide redundancy in case of failure. You can either program the PAC file to be redundant, or if a failure occurs, change the PAC file to use a different proxy server.

**Note**

Different browsers take different amounts of time to fail over to a secondary proxy. For example, Internet Explorer takes about 25 seconds, and Firefox takes about 50 seconds.

- **Load balancing.** If you have multiple proxy servers, you can use the PAC file to specify which requests go to which proxy server. For example, you might want users on one subnet to use a particular proxy and users on a different subnet to use a different proxy.
**PAC File Format**

The PAC file must include at least one JavaScript function, `FindProxyForURL(url, host)`. The JavaScript function determines the appropriate proxy to use for each URL.

For example, if the Web Security appliance hostname is WSA.example.com, you could create a PAC file that includes the following text:

```javascript
function FindProxyForURL(url, host) { return "PROXY WSA.example.com:3128; DIRECT"; }
```

**Note**
The port you specify in the `FindProxyForURL()` function should be a proxy port for the Web Security appliance configured on the Security Services > Web Proxy page.

However, you can make PAC files more complex. For example, you can create a PAC file that instructs the browser to connect directly to the website under certain conditions, such as matching on a particular hostname or IP address, and to use the proxy server in all other cases. You can create a PAC file that instructs applications to go directly to the website for servers on your intranet.

For more information about creating and using PAC files, see the following locations:

- [http://wp.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html](http://wp.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html)

**Note**
Common convention is to use the .pac file extension for PAC file names.
Creating a PAC File for Remote Users

Some laptop users connect to the Internet both from inside your organization’s network and outside the network. For these users, you can create a PAC file that informs the browser to connect to the Web Proxy when they are on the network, and to connect directly to web servers when they are not on the network.

To do this, make sure the PAC file is hosted on a web server that is DNS resolvable inside the network, but not DNS resolvable outside the network. This works because when you enter a URL for the PAC file location, the browser will always try to use the PAC file in the configured location. If the browser cannot resolve the URL, such as when it is outside the network, it tries to access all web sites directly instead. Then when the laptop connects to the network again, the browser can access the PAC file and will use the Web Proxy to access web sites.

Specifying the PAC File in Browsers

To use a PAC file, you must publish the PAC file in a location that can be accessed by each browser that needs to access it. When you configure a browser to use a PAC file, you can use either of the following methods:

- Enter the PAC file location. See Entering the PAC File Location, page 5-22.
- Detect the PAC file location automatically. See Detecting the PAC File Location Automatically, page 5-23.

Entering the PAC File Location

You can configure a browser to use a PAC file by specifying the exact location of the file. You might want to enter the exact PAC file location for laptop users who might need to use different proxy servers depending on their current location.

You can place the PAC file in the following locations:

- Local machine. You can place the PAC file on each client machine and configure the browsers to use it. You might want to use a local PAC file to test a PAC file before deploying it to the entire organization. Enter the path in the browser configuration. The path you enter depends on the browser type.
Working with PAC Files

- **Web server.** You can place the PAC file on a web server that each client machine can access. For example, you can place the PAC file on an Apache or Microsoft IIS web server. Enter the URL in the browser configuration.

- **Web Security appliance.** You can place the PAC file on the Web Security appliance. You might want to put the PAC file on the Web Security appliance to verify every client machine can access it within the network. Enter the URL in the browser configuration.

  For more information about uploading PAC files to the Web Security appliance, see Adding PAC Files to the Web Security Appliance, page 5-24.

Detecting the PAC File Location Automatically

If a browser supports the Web Proxy Autodiscovery Protocol (WPAD), you can configure it to automatically detect the PAC file location. WPAD is a protocol that allows the browser determine the location of the PAC file using DHCP and DNS lookups.

Before fetching its first page, a web browser configured to automatically detect the PAC file location tries to find the PAC file using DHCP or DNS. Therefore, to use WPAD, you must set up either a DHCP server or a DNS server to direct web browser requests to the PAC file on a network server. However, not all browsers support DHCP to find the PAC file using WPAD.

This section includes some general guidelines for using WPAD with DNS “A” records. For more detailed information, or for information about using WPAD with DHCP, see the following locations:


When you use WPAD with DNS, each domain on the network can only use one PAC file for all users on a domain because only domain name can uniquely identify a PAC file using DNS. For example, users on host1.accounting.example.com and host2.finance.example.com can use different PAC files.

To use WPAD with DNS:

**Step 1** Rename the PAC file to wpad.dat.
Adding PAC Files to the Web Security Appliance

Step 2 
Create an internally resolvable DNS name that starts with “wpad,” such as wpad.example.com.

Step 3 
Place wpad.dat in the root directory of the website that will host the file, such as wpad.example.com. For information about placing the file on the Web Security appliance, see Uploading PAC Files to the Appliance, page 5-28.

Note 
Due to a bug in Internet Explorer 6, create a copy of wpad.dat and change the file name to wpad.da to work with Internet Explorer 6 users. For more information, see http://www.microsoft.com/technet/isa/2004/ts_wpad.mspx.

Step 4 
Configure the web server to set up .dat files with the following MIME type:

application/x-ns-proxy-autoconfig

Note 
If you place wpad.dat on the Web Security appliance, the appliance does this for you already.

Adding PAC Files to the Web Security Appliance

You can configure browsers to explicitly use the Web Proxy by using proxy auto-config (PAC) files. You can place PAC files on the Web Security appliance, and then configure the browsers in one of two ways: enter the URL of a PAC file on the appliance, or set the browsers to automatically detect the PAC file by using the Web Proxy Autodiscovery Protocol (WPAD).

You can add multiple PAC files to the appliance. You might want to add multiple PAC files if the appliance is used by multiple domains on the network. You can use one PAC file for all browsers on a domain.

When you add a PAC file to the appliance, you can specify one or more ports the appliance uses to listen for PAC file requests. For information on specifying the PAC file URL when it is hosted on the Web Security appliance, see Specifying the PAC File URL, page 5-25.

When a browser asks for a PAC file, the appliance sends the file using HTTP. The PAC file is returned using MIME type application/x-ns-proxy-autoconfig.
Note

When browsers are configured to use a PAC file on the appliance, the URL should include the PAC file name. If the URL does not specify the PAC file name, by default, the appliance uses default.pac if it exists and returns an error if it does not. Or, you can configure the default PAC file to use for different hostnames or domains on the network.

For more information about PAC files, see Working with PAC Files, page 5-19.

Specifying the PAC File URL

When you configure a browser to use a PAC file, you can specify the exact location of the file using a URL. When the PAC file is hosted on the Web Security appliance, you can specify the URL using any of the formats in Table 5-3.

Table 5-3  PAC File URL Formats

<table>
<thead>
<tr>
<th>PAC File URL Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://hostname.domain:port/filename">http://hostname.domain:port/filename</a></td>
<td>The PAC file filename is served if it exists; otherwise an error is returned. This assumes port is a configured port on the appliance, and that hostname is the hostname of the appliance network interface configured for PAC file hosting.</td>
</tr>
<tr>
<td><a href="http://hostname.domain:port/">http://hostname.domain:port/</a></td>
<td>The PAC file default.pac is served if it exists; otherwise an error is returned. This assumes port is a configured port on the appliance, and that hostname is the hostname of the appliance network interface configured for PAC file hosting.</td>
</tr>
</tbody>
</table>
Table 5-3  PAC File URL Formats

<table>
<thead>
<tr>
<th>PAC File URL Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://hostname:port/filename">http://hostname:port/filename</a></td>
<td>The PAC file <code>filename</code> is served if it exists; otherwise an error is returned. This assumes <code>port</code> is a configured port on the appliance, and that <code>hostname</code> is the hostname of the appliance network interface configured for PAC file hosting.</td>
</tr>
<tr>
<td><a href="http://hostname:port/">http://hostname:port/</a></td>
<td>The PAC file “default.pac” is served if it exists; otherwise an error is returned. This assumes <code>port</code> is a configured port on the appliance, and that <code>hostname</code> is the hostname of the appliance network interface configured for PAC file hosting.</td>
</tr>
<tr>
<td><a href="http://IPAddress:port/filename">http://IPAddress:port/filename</a></td>
<td>The PAC file <code>filename</code> is served if it exists; otherwise an error is returned. This assumes <code>port</code> is a configured port on the appliance, and that <code>IPAddress</code> is the IP address of the appliance network interface configured for PAC file hosting.</td>
</tr>
<tr>
<td><a href="http://IPAddress:port/">http://IPAddress:port/</a></td>
<td>The PAC file “default.pac” is served if it exists; otherwise an error is returned. This assumes <code>port</code> is a configured port on the appliance, and that <code>IPAddress</code> is the IP address of the appliance network interface configured for PAC file hosting.</td>
</tr>
</tbody>
</table>
Adding PAC Files to the Web Security Appliance

**Table 5-3 PAC File URL Formats**

<table>
<thead>
<tr>
<th>PAC File URL Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://ConfiguredHostname/filename">http://ConfiguredHostname/filename</a></td>
<td>The PAC file <em>filename</em> is served if it is configured on the appliance and exists; otherwise an error is returned. This assumes that <em>ConfiguredHostname</em> is a hostname entered in the Hostname field on the Security Services &gt; Proxy Auto-Configuration File Hosting page.</td>
</tr>
<tr>
<td><a href="http://ConfiguredHostname/">http://ConfiguredHostname/</a></td>
<td>The configured default PAC file name for <em>ConfiguredHostname</em> is served if the hostname is configured on the Security Services &gt; Proxy Auto-Configuration File Hosting page. If the hostname is not configured, an error is returned.</td>
</tr>
<tr>
<td><a href="http://IPAddress/filename">http://IPAddress/filename</a></td>
<td>The PAC file <em>filename</em> is served if it is configured on the appliance and exists; otherwise an error is returned. This assumes that <em>IPAddress</em> is an IP address entered in the Hostname field on the Security Services &gt; Proxy Auto-Configuration File Hosting page. If the IP address is not configured, an error is returned.</td>
</tr>
<tr>
<td><a href="http://IPAddress/">http://IPAddress/</a></td>
<td>The configured default PAC file name for <em>IPAddress</em> is served if the IP address is a configured hostname on the Security Services &gt; Proxy Auto-Configuration File Hosting page. If the IP address is not configured, an error is returned.</td>
</tr>
</tbody>
</table>
Uploading PAC Files to the Appliance

To store PAC files on the Web Security appliance:

Step 1 Navigate to Security Services > Proxy Auto-Configuration File Hosting, and click Enable and Edit Settings.

The Edit Proxy Auto-Configuration File Hosting Settings page appears.

Figure 5-5 Editing the PAC File Host Settings

Step 2 In the PAC Server Ports field, enter one or more port numbers the Web Security appliance should use to listen for PAC file requests.

Step 3 In the Interface field, select the interface the Web Proxy uses to listen for PAC file requests. You can choose any interface that is configured for data traffic. This field only appears when multiple interfaces are configured for data traffic.

Step 4 In the PAC File Expiration section, choose whether to allow the PAC file to expire after a specified number of minutes in the browser’s cache.

Step 5 Click Browse to upload a PAC file from your local machine to the appliance.

Step 6 Navigate to the PAC file location, select it, and click Open.

Step 7 To add another PAC file, click Add Row, and repeat steps 5 and 6.
Optionally, PAC files can be served through HTTP proxy ports, such as port 80. To allow this, you must explicitly configure the hostnames that should serve PAC files and choose a default PAC file for each hostname. The specified default PAC file name is served when browsers do not include the PAC file name when requesting the PAC file URL (“GET/” requests). Otherwise, the PAC file name specified in the URL is served. If a PAC file URL uses an IP address, you can enter the IP address as a configured hostname.

**Step 8** To configure a default PAC file name for different hostnames, in the Hostnames field enter the Web Security appliance hostname or IP address, or any hostname that resolves to the appliance hostname. Then choose the default PAC file name in the Default PAC File for “Get/” Request through Proxy Port field.

For example, if you enter `wsa.example.com` in the Hostnames field and `pacfile1.pac` in the Default PAC File for “Get/” Request through Proxy Port field, then requests for `http://wsa.example.com/` fetch `pacfile1.pac` and requests for `http://wsa.example.com/default.pac` fetch `default.pac`.

**Step 9** Optionally, repeat step 8 to configure a default PAC file name for all hostnames that resolve to the Web Security appliance.

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

**Understanding WPAD Compatibility with Netscape and Firefox**

Netscape and Firefox browsers only use DNS to automatically detect PAC files using WPAD. Therefore, if you want Netscape and Firefox browsers to automatically detect a PAC file stored on the Web Security appliance, you must complete the following steps:

1. Name the PAC file `wpad.dat`.
2. Navigate to the Security Services > Web Proxy page, and delete port 80 from the HTTP Ports to Proxy field.
3. Use port 80 as the PAC Server Port when you upload the file to the appliance.

For more information about using WPAD, see Detecting the PAC File Location Automatically, page 5-23.
Chapter 5  Web Proxy Services

Advanced Proxy Configuration

AsyncOS includes the `advancedproxyconfig` CLI command so you can configure more advanced Web Proxy configurations, such as authentication and DNS parameters.

The `advancedproxyconfig` command includes the following subcommands:

- **Authentication.** Configure authentication parameters, such as the number of outstanding concurrent Basic or NTLMSSP authentication requests to be authenticated by the authentication server and whether or not to log the username that appears in the request URI. You can also use the `authentication` subcommand to enable the user acknowledgment page. For more information about the user acknowledgment page, see Proxy Usage Agreement, page 5-18.

  For more information, see Authentication Options, page 5-32.

- **Caching.** Configure advanced Web Proxy caching options, such as:
  - Whether or not to ignore client requests to not retrieve content from the proxy cache
  - Whether or not to cache content from an untrusted server

  You can configure the parameters separately by selecting “Customized Mode,” or you can choose a predefined set of parameter values. You can choose the following modes:
  - **Safe mode.** This mode uses less caching.
  - **Optimized mode.** This mode uses moderate caching.
  - **Aggressive mode.** This mode uses aggressive caching.

  For more information, see Caching Options, page 5-39.

- **DNS.** Configure DNS-related options, such as the time to cache results of DNS errors and whether or not the Web Proxy should issue an HTTP 302 redirection on DNS lookup failure.
Chapter 5  Web Proxy Services

Advanced Proxy Configuration

For more information, see DNS Options, page 5-42.

- **EUN.** Configure the end-user notification page settings, such as whether to use the standard IronPort end-user notification pages or use pages you customize. For more information on configuring the end-user notification pages, see Working with IronPort FTP Notification Messages, page 15-23.

For more information, see EUN Options, page 5-44.

- **NATIVEFTP.** Configure the FTP Proxy settings, such as the port ranges to use for active and passive mode and the type of authentication to use for explicit forward connections. Applies to native FTP transactions only. For more information on configuring the FTP Proxy, see Configuring FTP Proxy Settings, page 5-11.

For more information, see NATIVEFTP Options, page 5-44.

- **FTPOVERHTTP.** Configure the login name and password to use for anonymous FTP access and whether or not to allow active mode for FTP transfers. Applies to FTP over HTTP transactions only.

For more information, see FTPOVERHTTP Options, page 5-47.

- **HTTPS.** Configure the logging style for URIs used in HTTPS transactions. You can choose to record the full URI (“fulluri”) or just a portion of the URI with the query portion removed (“stripquery”).

For more information, see HTTPS Options, page 5-48.

- **Scanning.** Configure how the DVS engine handles anti-malware scanning of web transactions.

For more information, see Scanning Options, page 5-49.

- **WCCP.** Configure the amount of logging detail to use to debug WCCP related issues.

For more information, see WCCP Options, page 5-49.

- **Miscellaneous.** Configure whether or not the Web Proxy should respond to health checks from L4 switches and whether or not the Web Proxy should perform dynamic adjustment of TCP receive window sizes.

For more information, see Miscellaneous Options, page 5-50.

Each submenu command is discussed in the detail tables below. For the Default Value column, a string means a name or list of characters such as “hello world.”
## Authentication Options

Table 5-4 describes the authentication options for the `advancedproxyconfig` CLI command.

**Table 5-4**  
*advancedproxyconfig CLI Command—Authentication Options*

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When would you like to forward authorization request headers to a parent proxy?</td>
<td>Never, Always, Only if not used by the WSA</td>
<td>Never</td>
<td>Yes</td>
<td>This setting determines whether the Web Proxy includes the “Proxy-Authorization” header to upstream servers, including proxies.</td>
</tr>
<tr>
<td>Enter the Proxy Authorization Realm to be displayed in the end user authentication dialog</td>
<td>String</td>
<td>“IronPort Web Security Appliance”</td>
<td>No</td>
<td>Proxy Authorization Realm displayed in the End User Authentication dialog.</td>
</tr>
<tr>
<td>Would you like to log the username that appears in the request URI?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>No</td>
<td>If enabled, ‘&lt;username&gt;:xxxxx’ is logged i.e the username is displayed and the password is represented as a string, ‘xxxxx’. If disabled, both username and password are stripped. Note that the actual password is never displayed regardless of the value of this variable.</td>
</tr>
<tr>
<td>Would you like to turn on presentation of the User Acknowledgement page?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>No</td>
<td>Enable or disable Acknowledgement page.</td>
</tr>
<tr>
<td>Enter maximum time to remember User Acknowledgement (in seconds):</td>
<td>30 - 2678400</td>
<td>86400</td>
<td>No</td>
<td>Maximum time to remember User Acknowledgement. From 30 seconds to one month (2678400).</td>
</tr>
</tbody>
</table>
### Table 5-4  advancedproxyconfig CLI Command—Authentication Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter maximum idle timeout for User Acknowledgement based on IP Address (in seconds):</td>
<td>30 - 2678400</td>
<td>14400</td>
<td>No</td>
<td>Maximum idle timeout for User Acknowledgement based on IP Address. From 30 seconds to one month (2678400).</td>
</tr>
<tr>
<td>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)?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>No</td>
<td>Choose whether or not AsyncOS should use the group membership attribute when doing a directory lookup. If you do not want to display empty authentication groups and fetch groups whose group membership attribute is different, choose Yes.</td>
</tr>
<tr>
<td>Would you like to allow case insensitive username matching in policies?</td>
<td>Yes, No (Boolean)</td>
<td>Yes</td>
<td>Yes</td>
<td>Choose whether or not the Web Proxy should ignore case when matching user names against the policy groups.</td>
</tr>
<tr>
<td>Would you like to allow wild card matching with the character * for LDAP group names?</td>
<td>Yes, No (Boolean)</td>
<td>Yes</td>
<td>Yes</td>
<td>Choose whether or not to match an asterisk as a wildcard in LDAP group filters. When this option is disabled, using an asterisk (*) in the group filters for LDAP servers works as a literal string.</td>
</tr>
</tbody>
</table>
Enter the charset to be used for basic authentication [ISO-8859-1/UTF-8].

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the charset to be used for basic</td>
<td>ISO-8859-1, UTF-8</td>
<td>ISO-8859-1</td>
<td>No</td>
<td>Choose the character encoding that the Web Proxy should use when reading the Basic authentication credentials in the HTTP request. The setting configured here does not affect the request content, only the Basic authentication credentials. You might want to use ISO-8859-1 if most web browsers used on your network are Internet Explorer, Firefox, and Safari, and UTF-8 if most web browsers on your network are Opera and Chrome. <strong>Note:</strong> The Web Proxy always uses UTF-8 when sending the Basic authentication credentials to the authentication server.</td>
</tr>
<tr>
<td>Would you like to enable referrals for LDAP?</td>
<td>Yes, No</td>
<td>No</td>
<td>Yes</td>
<td>Choose whether or not the Web Proxy should perform LDAP queries on a referred LDAP server. You might want to disable this option if a referred LDAP server is unavailable to the Web Security appliance.</td>
</tr>
</tbody>
</table>
Would you like to enable secure authentication?

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Would you like to enable secure</td>
<td>Yes, No</td>
<td>No</td>
<td>Yes/No</td>
<td>Choose whether or not the Web Proxy redirects clients to securely pass</td>
</tr>
<tr>
<td>authentication?</td>
<td>(Boolean)</td>
<td></td>
<td>(Web Proxy restarts</td>
<td>authentication credentials to the Web Proxy using HTTPS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>when it needs to</td>
<td>For more information on this feature, see Sending Authentication Credentials</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>listens on fewer or</td>
<td>Securely, page 20-37.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>additional ports)</td>
<td></td>
</tr>
<tr>
<td>Enter the redirect port for</td>
<td>1 to 65535</td>
<td>443</td>
<td>Yes/No</td>
<td>Enter the port to use for redirecting requests using HTTPS. Cisco</td>
</tr>
<tr>
<td>secure authentication.</td>
<td></td>
<td></td>
<td>(Web Proxy restarts</td>
<td>recommends using a port greater than 1023.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>when it needs to</td>
<td>For more information on configuring this option, see Configuring Global</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>listens on fewer or</td>
<td>Authentication Settings, page 20-23.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>additional ports)</td>
<td></td>
</tr>
</tbody>
</table>

Note: This option only appears when you enable secure authentication.
### Table 5-4  
**advancedproxyconfig CLI Command—Authentication Options (continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enter the hostname to redirect clients for authentication. | String       | Appliance hostname | No                     | Enter the short hostname of the network interface on which the Web Proxy listens for incoming connections.  
When you enable secure authentication, the Web Proxy uses this hostname in the redirection URL sent to clients for authenticating users.  
For more information on configuring this option, see [Configuring Global Authentication Settings, page 20-23](#). |
| Enter the surrogate timeout.                | Time in seconds | 3600               | No                     | This setting specifies how long the surrogate (IP address or cookie) can be used before requiring authentication credentials again.  
For more information on configuring this option, see [Configuring Global Authentication Settings, page 20-23](#). |
Enter re-auth on request denied option [disabled / embedlinkinblockpage]?

Table 5-4 advancedproxyconfig CLI Command—Authentication Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter re-auth on request denied option [disabled / embedlinkinblockpage]?</td>
<td>disabled/ embedlink inblockpage</td>
<td>disabled</td>
<td>No</td>
<td>This setting allows users to authenticate again if the user is blocked from a website due to a restrictive URL filtering policy. 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. Note: This setting only applies to authenticated users who are blocked due to restrictive URL filtering policies. It does not apply to blocked transactions by subnet with no authentication. For more information, see Allowing Users to Re-Authenticate, page 20-39.</td>
</tr>
<tr>
<td>Would you like to send Negotiate header along with NTLM header for NTLMSSP authentication?</td>
<td>1, 2</td>
<td>1</td>
<td>No</td>
<td>Choose whether or not the Web Proxy sends “Negotiate” as an acceptable authentication protocol when establishing the NTLM handshake with the Active Directory server. Choose one of the following values: 1. Do not send Negotiate header 2. Send Negotiate header</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 5-4  advancedproxyconfig CLI Command—Authentication Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the IP address to user name mapping update interval for transparent user identification in seconds.</td>
<td>Time in seconds</td>
<td>600</td>
<td>No</td>
<td>The amount of time that passes before contacting the Novell eDirectory server to obtain an updated IP address to user name mapping for transparent user identification.</td>
</tr>
</tbody>
</table>
The Caching submenu provides four options to set the advanced caching mode.

---

**Table 5-4 advancedproxyconfig CLI Command—Authentication Options (continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the maximum wait time for transparent user identification in seconds. (Note: Setting this value to 0 will disable on-demand query to the directory server if the given IP address is not found in the mapping. WSA will still query the directory server at fixed intervals).</td>
<td>Time in seconds</td>
<td>5</td>
<td>No</td>
<td>Maximum time the Web Proxy takes to query the directory server again if the IP address to user name mapping is not readily available. When the query takes more than the timeout value, transparent user identification is considered to have failed. This limits the authentication delay experienced by the end user.</td>
</tr>
<tr>
<td>Configure username and IP address masking in logs and reports:</td>
<td>1, 2, 3</td>
<td>3</td>
<td>No</td>
<td>Choose whether or not to mask user names and/or IP addresses in logs and reports. Masked user names appear as “AUTHENTICATED_USER” in the logs, but guest user names are not masked. Choose one of the following options: 1. Mask both user names and IP addresses in logs and reports 2. Mask only usernames and replace them with IP addresses in logs and reports 3. Show usernames and IP addresses in logs and reports</td>
</tr>
</tbody>
</table>
Table 5-5 describes the caching options for the Customized Mode option in the `advancedproxyconfig` CLI command.

**Table 5-5** advancedproxyconfig CLI Command—Caching Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Would you like to allow objects with a heuristic expiration time to be served as not-modified If-Modified-Since hits from cache?</td>
<td>Yes, No (Boolean)</td>
<td>Yes</td>
<td>No</td>
<td>0 = favor freshness on IMS to objects with heuristic expiration time 1 = favor bandwidth conservation</td>
</tr>
<tr>
<td>Would you like to allow ETAG mismatch on client revalidations?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>No</td>
<td>In some cases, the server might report different ETags for the same version of the same file. This can be seen, for example, with clustered IIS servers. In these cases, requiring both a last modified time (LMT) match and an ETag match on client revalidations would lead to a lot of misses, so it should be sufficient just to match the LMT if it is given. <strong>Note:</strong> Setting this to 1 is not HTTP-compliant.</td>
</tr>
<tr>
<td>Would you like to allow caching when requests are authenticated by the origin server?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>Yes</td>
<td>Allow caching for requests authenticated by origin server.</td>
</tr>
<tr>
<td>Would you like to allow caching from servers whose DNS results do not match the TCP destination IP (not trust-worthy and applicable only in transparent modes)?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>Yes</td>
<td>Allow caching from servers whose DNS results do not match the TCP destination IP.</td>
</tr>
</tbody>
</table>
### Table 5-5 advancedproxyconfig CLI Command—Caching Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the Heuristic maximum age to cache the document with Last-Modified Time but no actual caching value (in seconds):</td>
<td>Time in seconds</td>
<td>86400</td>
<td>No</td>
<td>Heuristic maximum age to cache the document with LMT but no actual caching value.</td>
</tr>
<tr>
<td>Enter the Heuristic maximum age to cache the document without Last-Modified Time and no actual caching value (in seconds):</td>
<td>Time in seconds</td>
<td>0</td>
<td>No</td>
<td>Heuristic maximum age to cache the document without LMT and no actual caching value.</td>
</tr>
<tr>
<td>Enter the Heuristic age to cache errors (HTTP_SERVICE_UNAVAILABLE, HTTP_GATEWAY_TIMEOUT etc) (in seconds):</td>
<td>Time in seconds</td>
<td>300</td>
<td>No</td>
<td>Heuristic age to cache errors (HTTP_SERVICE_UNAVAILABLE, HTTP_GATEWAY_TIMEOUT etc).</td>
</tr>
<tr>
<td>Would you like proxy to ignore client directive to not fetch content from the cache?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>No</td>
<td>Disable/Enable ignoring of the client directive to not fetch content from the cache. Enabling this is not HTTP compliant.</td>
</tr>
<tr>
<td>Enter the time interval during which reload requests must be ignored by the proxy (in seconds):</td>
<td>Time in seconds</td>
<td>0</td>
<td>No</td>
<td>Disable/Enable reload requests to be ignored for the specified time interval. This allows reload requests to be ignored for a certain amount of time, even though it is not HTTP-compliant. You might want to enter a value greater than zero to improve bandwidth usage.</td>
</tr>
</tbody>
</table>
**Table 5-5** advancedproxyconfig CLI Command—Caching Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Would you like to allow proxy to convert reload requests into max-age requests?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>No</td>
<td>Allow reload requests to be converted into max-age requests (not HTTP-compliant, but may improve bandwidth usage). This gets its max-age value from “ignoreReloadTime.”</td>
</tr>
<tr>
<td>Time in seconds after which an explicit IMS Refresh request must be issued:</td>
<td>Time in seconds</td>
<td>300</td>
<td>No</td>
<td>Time in seconds after which an explicit IMS Refresh request must be issued.</td>
</tr>
</tbody>
</table>

### DNS Options

Table 5-6 describes the DNS options for the advancedproxyconfig CLI command.

**Table 5-6** advancedproxyconfig CLI Command—DNS Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the URL format for the HTTP 307 redirection on DNS lookup failure:</td>
<td>String with EUN page variables %P/www.%H.com/%u</td>
<td>%P//www.%H.com/%u</td>
<td>No</td>
<td>URL format for the HTTP 307 redirection on DNS lookup failure. See Table 15-2, ‘Variables for Customized End-User Notification Pages,’ on page 9 for the list of valid variables.</td>
</tr>
<tr>
<td>Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure?</td>
<td>Yes, No (Boolean)</td>
<td>Yes</td>
<td>Yes</td>
<td>Disable/Enable automatic HTTP 307 redirection on DNS lookup failure.</td>
</tr>
</tbody>
</table>
Table 5-6  
advancedproxyconfig CLI Command—DNS Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Would you like proxy not to automatically failover to DNS results when upstream proxy (peer) is unresponsive?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>Yes</td>
<td>Disable/Enable automatic failover to DNS results when upstream proxy (peer) is unresponsive.</td>
</tr>
<tr>
<td>Find web server by: 0 = use DNS answers in order, 1 = use client supplied address then DNS, 2 = use ONLY client supplied address:</td>
<td>0, 1, 2</td>
<td>1</td>
<td>Yes</td>
<td>Specify how the appliance should find the location of the requested web server.</td>
</tr>
</tbody>
</table>
EUN Options

Table 5-7 describes the EUN options for the advancedproxyconfig CLI command.

Table 5-7  advancedproxyconfig CLI Command—EUN Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
</table>
| Choose:              | 1, 2, 3      | 3             | Yes                    | Choose whether to use the IronPort end-user notification pages or uploaded customized end-user notification pages. Choose one of the following options:  
                       |              |               |                        | • 1. Refresh EUN pages  
                       |              |               |                        | • 2. Use Custom EUN pages  
                       |              |               |                        | • 3. Use Standard EUN pages  
                       |              |               |                        | For more information, see Editing IronPort Notification Pages, page 15-8. |

NATIVEFTP Options

Table 5-8 describes the NATIVEFTP options for the advancedproxyconfig CLI command.

Table 5-8  advancedproxyconfig CLI Command—NATIVEFTP Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Would you like to enable FTP proxy?</td>
<td>Yes, No (Boolean)</td>
<td>Yes</td>
<td>Yes</td>
<td>Choose whether or not to enable the FTP Proxy.</td>
</tr>
<tr>
<td>Enter the ports that FTP proxy listens on.</td>
<td>1 to 65535</td>
<td>8021</td>
<td>Yes</td>
<td>Specify the port FTP clients should use to establish a control connection with the FTP Proxy.</td>
</tr>
</tbody>
</table>
### Table 5-8  \textit{advancedproxyconfig} CLI Command—NATIVEFTP Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the range of port numbers for the proxy to listen on for passive FTP connections.</td>
<td>port1-port2 (string) 1024 - 65535</td>
<td>11000-1109</td>
<td>Yes</td>
<td>Specify a range of TCP ports FTP clients should use to establish a data connection with the FTP Proxy for passive mode connections.</td>
</tr>
<tr>
<td>Enter the range of port numbers for the proxy to listen on for active FTP connections.</td>
<td>port1-port2 (string) 1024 - 65535</td>
<td>12000-12009</td>
<td>Yes</td>
<td>Specify a range of TCP ports FTP servers should use to establish a data connection with the FTP Proxy for active mode connections.</td>
</tr>
<tr>
<td>Would you like to use active mode when passive mode fails?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>No</td>
<td>When this option is enabled, the FTP Proxy will attempt an active mode connection with the FTP server when passive mode fails.</td>
</tr>
<tr>
<td>Enter the authentication format:</td>
<td>Check Point, Raptor</td>
<td>Check Point</td>
<td>Yes</td>
<td>Choose the authentication format the FTP Proxy uses when communicating with FTP clients. For more information, see \textit{Using Authentication with Native FTP}, page 5-9.</td>
</tr>
<tr>
<td>Would you like to enable caching?</td>
<td>Yes, No (Boolean)</td>
<td>Yes</td>
<td>Yes</td>
<td>Choose whether or not to cache contents of data connections from anonymous users.</td>
</tr>
<tr>
<td>Would you like to enable server IP spoofing?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>Yes</td>
<td>Choose whether or not the FTP Proxy should spoof the FTP server IP address. You might want to do this for FTP clients that do not allow transactions when the IP address is different for the control and data connections.</td>
</tr>
</tbody>
</table>
Would you like to pass FTP server welcome message to the clients?

- **Yes, No** (Boolean)
  - **Default Value**: Yes
  - **Web Proxy Must Restart**: Yes
  - **Description**: Choose which welcome message should appear in FTP clients:
    - **FTP server message**. Enter “Yes.” The FTP server message only displays for transparently redirected connections. When a native FTP connection is explicitly sent to the FTP Proxy, the FTP client displays a message predefined by the FTP Proxy.
    - **Custom message**. Enter “No.” You can enter a custom message to display for all native FTP connections in the next question.

Enter the customized server welcome message.

- **Valid Values**: String
- **Default Value**: N/A
- **Web Proxy Must Restart**: Yes
- **Description**: This command appears when you enter No for the FTP server welcome message.
  Enter the custom message to display for all native FTP connections.

### Table 5-8: `advancedproxyconfig CLI Command—NATIVEFTP Options (continued)`

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
</table>
| Would you like to pass FTP server welcome message to the clients? | Yes, No (Boolean) | Yes | Yes | Choose which welcome message should appear in FTP clients:
- **FTP server message**. Enter “Yes.” The FTP server message only displays for transparently redirected connections. When a native FTP connection is explicitly sent to the FTP Proxy, the FTP client displays a message predefined by the FTP Proxy.
- **Custom message**. Enter “No.” You can enter a custom message to display for all native FTP connections in the next question. |
| Enter the customized server welcome message. | String | N/A | Yes | This command appears when you enter No for the FTP server welcome message.
Enter the custom message to display for all native FTP connections. |
**FTPOVERHTTP Options**

Table 5-9 describes the FTPOVERHTTP options for the `advancedproxyconfig` CLI command.

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the login name to be used for anonymous FTP access:</td>
<td>String</td>
<td>anonymous</td>
<td>No</td>
<td>Anonymous FTP login name.</td>
</tr>
<tr>
<td>Enter the password to be used for anonymous FTP access:</td>
<td>String</td>
<td>proxy@</td>
<td>No</td>
<td>Anonymous FTP login password.</td>
</tr>
<tr>
<td>Would you like to use active FTP transfer mode when passive mode fails?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>No</td>
<td>Choose whether or not to allow FTP transfers to use active mode if passive mode fails.</td>
</tr>
<tr>
<td>Enter the range of port numbers for the proxy to bind to when making passive FTP connections.</td>
<td>port1-port2 (string)</td>
<td>13000-13001</td>
<td>No</td>
<td>Specify a range of TCP ports the appliance can use for establishing a passive data connection with an FTP server. If a port is being used, the Web Proxy chooses the next port in the range until it finds an available port. This option only appears when active mode is enabled.</td>
</tr>
<tr>
<td>Enter the range of port numbers for the proxy to listen on for active FTP connections.</td>
<td>port1-port2 (string)</td>
<td>10000-10001</td>
<td>No</td>
<td>When you enable active mode for FTP transfers, enter the range of TCP ports the appliance can use for establishing a data connection with an FTP server. If a port is being used, the Web Proxy chooses the next port in the range until it finds an available port. This option only appears when active mode is enabled.</td>
</tr>
</tbody>
</table>
HTTPS Options

Table 5-10 describes the HTTPS options for the `advancedproxyconfig` CLI command.

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS URI Logging Style:</td>
<td>fulluri or stripquery</td>
<td>fulluri</td>
<td>Yes</td>
<td>You can log the entire URI (fulluri), or a partial form of the URI with the query portion removed (stripquery). However, even when you choose to strip the query from the URI, personally identifiable information may still remain.</td>
</tr>
</tbody>
</table>
| Would you like to decrypt unauthenticated transparent HTTPS requests for authentication purpose? | Yes, No (Boolean) | Yes           | No                      | Choose how the Web Proxy handles transparently redirected HTTPS transactions it receives before an HTTP request that was authenticated using an identity with an IP-based surrogate. Select one of the following options:  
  • **Yes.** Decrypt the HTTPS request for authentication purposes.  
  • **No.** Deny the HTTPS request. |
Scanning Options

Table 5-11 describes the scanning options for the `advancedproxyconfig` CLI command.

**Table 5-11 advancedproxyconfig CLI Command—Scanning Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
</table>
| Would you like the proxy to do malware scanning all content regardless of content type? Note that this will have serious performance impact and is not recommended. | Yes, No (Boolean) | No            | No                      | Choose whether or not the DVS engine should scan all response content regardless of the content type.  
**Note:** Enabling this setting results in a significant performance impact for the Web Proxy. |

WCCP Options

Table 5-12 describes the WCCP options for the `advancedproxyconfig` CLI command.

**Table 5-12 advancedproxyconfig CLI Command—WCCP Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the log level for debugging WCCP:</td>
<td>1 - 5</td>
<td>2</td>
<td>Yes</td>
<td>WCCP log level</td>
</tr>
</tbody>
</table>
## Miscellaneous Options

Table 5-13 describes the miscellaneous options for the `advancedproxyconfig` CLI command.

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode)?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>Yes</td>
<td>Disable/Enable support for responding to health checks from L4 switches (always enabled if WSA is in L4 transparent mode). L4 switches issue ‘HEAD / HTTP/1.0’ requests directed at the proxy to ensure that it is responding.</td>
</tr>
<tr>
<td>Would you like proxy to perform dynamic adjustment of TCP receive window size?</td>
<td>Yes, No (Boolean)</td>
<td>Yes</td>
<td>Yes</td>
<td>Disable/Enable dynamic adjustment of TCP receive window size.</td>
</tr>
<tr>
<td>Enable caching of HTTPS responses?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>No</td>
<td>Choose whether or not the Web Security appliance should store HTTPS responses in the web cache.</td>
</tr>
<tr>
<td>Enter minimum idle timeout for checking unresponsive upstream proxy (in seconds).</td>
<td>Time in seconds</td>
<td>10</td>
<td>No</td>
<td>The minimum amount of time the Web Proxy waits before checking if an upstream proxy is still unavailable.</td>
</tr>
<tr>
<td>Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds).</td>
<td>Time in seconds</td>
<td>86400</td>
<td>No</td>
<td>The maximum amount of time the Web Proxy waits before checking if an upstream proxy is still unavailable.</td>
</tr>
</tbody>
</table>
Chapter 5  Web Proxy Services

Advanced Proxy Configuration

Table 5-13  advancedproxyconfig CLI Command—Miscellaneous Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode of the proxy:</td>
<td>1, 2, 3</td>
<td>2</td>
<td>Yes</td>
<td>Choose how to deploy the Web Proxy using one of the following options: 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 For more information, see Deployment Overview, page 3-1.</td>
</tr>
<tr>
<td>Spoofing of the client IP by the proxy:</td>
<td>1, 2, 3</td>
<td>1</td>
<td>No</td>
<td>Choose whether or not the Web Proxy should spoof IP addresses when sending requests to upstream proxies and servers using one of the following options: 1. Disable 2. Enable for all requests 3. Enable for transparent requests only When IP spoofing is enabled, requests originating from a client retain the client’s source address and appear to originate from the client rather than from the Web Security appliance. Note: When IP spoofing is enabled and the appliance is connected to a WCCP router, configure a WCCP service to redirect the return path.</td>
</tr>
</tbody>
</table>
Table 5-13  
**advancedproxyconfig CLI Command—Miscellaneous Options (continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you want to pass HTTP X-Forwarded-For headers?</td>
<td>Yes, No (Boolean)</td>
<td>Yes</td>
<td>No</td>
<td>Choose whether or not the Web Proxy retains any “X-Forwarded-For” header included in the requests it receives. When set to No, the Web Proxy removes any “X-Forwarded-For” header from requests that enter the Web Proxy from a downstream proxy server. You might want to do this if the downstream proxy server includes client IP address in the header and you do not want to expose those IP addresses to servers outside your network.</td>
</tr>
<tr>
<td>Would you like to permit tunneling of non-http requests on http ports?</td>
<td>Yes, No (Boolean)</td>
<td>Yes</td>
<td>No</td>
<td>Choose whether or not to allow non-HTTP traffic on ports the Web Proxy is configured to monitor, such as port 80. This option applies when the Web Proxy is in transparent mode. Enabling this option blocks applications that attempt to tunnel non-HTTP traffic on ports typically used for HTTP traffic. <strong>Note:</strong> When a transaction is blocked due to this setting, the ACL decision tag for the transaction is logged as BLOCK_ADMIN_TUNNELING.</td>
</tr>
<tr>
<td>Would you like to block tunneling of non-SSL transactions on SSL Ports?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>No</td>
<td>Choose whether or not the Web Proxy should block non-SSL traffic on SSL ports.</td>
</tr>
</tbody>
</table>
Table 5-13  advancedproxyconfig CLI Command—Miscellaneous Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Valid Values</th>
<th>Default Value</th>
<th>Web Proxy Must Restart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses?</td>
<td>Yes, No (Boolean)</td>
<td>No</td>
<td>No</td>
<td>Choose whether or not the access logs should include the X-Forwarded-For header value instead of the IP address of the incoming connection.</td>
</tr>
<tr>
<td>Do you want proxy to throttle content served from cache?</td>
<td>Yes, No (Boolean)</td>
<td>Yes</td>
<td>No</td>
<td>Choose whether or not the Web Proxy should apply per user bandwidth controls to content served from the web cache in addition to the content served from web servers. Applies to application types that have bandwidth limits applied.</td>
</tr>
</tbody>
</table>
Working with Policies

This chapter contains the following information:

- Working with Policies Overview, page 6-1
- Policy Types, page 6-3
- Working with Policy Groups, page 6-6
- Policy Group Membership, page 6-10
- Working with Time Based Policies, page 6-13
- Working with User Agent Based Policies, page 6-16
- Tracing Policies, page 6-18

Working with Policies Overview

The Web Security appliance includes an advanced policy framework to intelligently map data policies to business processes for protection on the network and at the endpoint. It allows you to define policies to enforce your organization’s acceptable use policies by controlling access to the Internet. You can create groups of users and apply different levels and types of access control to each group.

For example, you can configure the appliance to enforce the following types of policies:

- Users in the Marketing group can access a competitor’s website, but other users cannot.
- Guest users on customer-facing machines, such as computers in a company store, cannot access banking sites, but employees can.
- No users can access gambling sites. Instead, when they try to view a gambling site, they see a web page that explains the organization’s policies.
- All users trying to access a particular site that no longer exists are redirected to a different site.
- All users except those in IT are blocked from accessing potential malware sites, but users in IT can access them for testing purposes, and the downloaded content is scanned for harmful objects.
- All requests for streaming media are blocked during business hours, but allowed outside of business hours.
- All requests from a particular user agent, such as a software update program, are allowed without requiring authentication.
- Block uploads of all Excel spreadsheet files greater than 2 MB.
- Block uploads of data to sites with a bad web reputation.
- Block uploads of data infected with malware.

To enforce organizational policies, you define different policies in the Web Security appliance. The appliance uses different types of policies for different functions. For more information about the types of policies, see Policy Types, page 6-3.

When you work with policies, you create policy groups. After you create policy groups, you can define the control settings for each group. For more information about working with policy groups, see Working with Policy Groups, page 6-6.

After you have created policies, you can figure out which policy groups apply to a particular client transaction for troubleshooting purposes. For example, you can find out if user jsmith tries to open a Firefox browser to the URL http://www.google.com, then which policy groups apply to the transaction. For more information about tracing policies, see Tracing Policies, page 6-18.

**Note**

The Web Security appliance is permissive by default. That is, requests are allowed unless specifically blocked in a policy group.
Policy Types

The Web Security appliance uses multiple types of policies to enforce organizational policies and requirements.

- **Identities.** “Who are you?”
- **Decryption Policies.** “To decrypt or not to decrypt?”
- **Routing Policies.** “From where to fetch content?”
- **Access Policies.** “To allow or block the transaction?”
- **IronPort Data Security Policies.** “To block the upload of data?” IronPort Data Security Policies actions are defined on the Web Security appliance.
- **External DLP (data loss prevention) Policies.** “To block the upload of data?” External DLP Policies actions are defined on an external DLP appliance.
- **Outbound Malware Scanning Policies.** “To block the upload of malicious data?”
- **SaaS Application Authentication Policies.** “To allow this user access to the SaaS application?”

You use the policies together to create the behavior you need or expect when clients access the web.

To define policies, you create policy groups. After you create policy groups, you can define the control settings for each group. For more information about working with policy groups, see Working with Policy Groups, page 6-6.

All policy types have a global policy group that maintains default settings and rules that apply to web transactions not covered by another policy. For more information on global policies, see Working with Policy Groups, page 6-6.

Identities

An Identity is a policy that identifies the user making a request. This is the only policy where you can define whether or not authentication is required. An Identity addresses the question, “who are you?” However, Identities do not specify a list of users who are authorized to access the web. You specify authorized users in the other policy types after you specify the Identity to use.
All other policies you create must specify an Identity.

Configure Identities on the Web Security Manager > Identities page. For more information about Identities, see Identities, page 7-1.

**Decryption Policies**

Decryption Policies determine whether or not an HTTPS connection should be decrypted, passed through, or dropped. They address the question, “to decrypt or not to decrypt?”

The appliance uses Decryption Policies to evaluate HTTPS requests. The Decryption Policy group that applies to an HTTPS request determines whether the appliance drops the connection, passes it through without decryption, or decrypts the connection and subsequently evaluate the decrypted request and response against the defined Access Policy groups.

Configure Decryption Policy groups on the Web Security Manager > Decryption Policies page. For more information about Decryption Policy groups, see Decryption Policies, page 10-1.

**Routing Policies**

Routing Policies determine to where to pass the client request, either to another proxy or to the destination server. They address the question, “from where to fetch content?”

You can use this policy type to select a group of upstream proxies configured for load balancing or failover.


**Access Policies**

Access Policies determine whether to allow or block HTTP and decrypted HTTPS transactions. They address the question, “to allow or block the transaction?”
Access Policies determine how the appliance controls access to services, applications, and objects on the web for HTTP and decrypted HTTPS requests. The appliance uses Access Policies to evaluate and scan HTTP requests and HTTPS requests designated for decryption.


IronPort Data Security Policies

IronPort Data Security Policies determine whether or not to block a request to upload data using logic defined on the Web Security appliance. They address the question, “to block the upload of data?”

The Web Proxy uses IronPort Data Security Policies to evaluate and scan HTTP requests and decrypted HTTPS requests that have any data in the request body.


External DLP Policies

External DLP (data loss prevention) policies determine whether or not to block a request to upload data using logic stored on an external DLP server. They address the question, “to block the upload of data?”

The Web Proxy uses External DLP Policies to evaluate HTTP requests and decrypted HTTPS requests that have any data in the request body and send them to an external DLP server for scanning.

Configure External DLP Policy groups on the Web Security Manager > External Data Loss Prevention page. For more information about External DLP Policy groups, see Data Security and External DLP Policies, page 12-1.
Outbound Malware Scanning Policies

Outbound Malware Scanning Policies determine whether or not to block a request to upload data that contains malicious data. They address the question, “To block the upload of malicious data?”

The Web Proxy uses Outbound Malware Scanning Policies to scan for malware HTTP requests and decrypted HTTPS requests that have any data in the request body.

Configure Outbound Malware Scanning Policy groups on the Web Security Manager > Outbound Malware Scanning page. For more information about Outbound Malware Scanning Policy groups, see Outbound Malware Scanning, page 11-1.

SaaS Application Authentication Policies

SaaS Application Authentication Policies determine whether or not a user is allowed access to a Software as a Service (SaaS) application. They address the question, “To allow this user access to a SaaS application?”

SaaS Application Authentication Policies determine how the appliance controls user access to configured SaaS applications, such as WebEx. When you enable Cisco SaaS Access Control, users log into the configured SaaS applications using their network authentication user credentials. That means they use the same user name and password for all SaaS applications as well as network access.


Working with Policy Groups

A policy group is an administrator defined configuration that allows you to apply acceptable use policies to specific categories of users. After you create policy groups, you can define the control settings for each group.
You can create as many user defined policy groups as required to enforce the proper access control. The Web Security appliance displays policy groups together in a policies table.

All policies have a default, global policy group that applies to a transaction if none of the user defined policy groups apply. A global policy group maintains default settings and rules that apply to web transactions not covered by another policy. This group appears in the last row of a policies table, and the Web Proxy applies its rules last if no other matching occurs.

Creating Policy Groups

You can create policy groups based on combinations of several criteria, such as client subnet or the URL category of the destination site. You must define at least one criterion for policy group membership. When you define multiple criteria, the client request must meet all criteria to match the policy group.

Options used to configure policy groups allow you to specify exceptions to global policy settings and control access to services for groups of users.

For more information about creating policy groups for the different policy types, see the following locations:

- Creating Identities, page 7-20
- Creating Access Policies, page 8-7
- Creating Decryption Policies, page 10-30
- Creating Routing Policies, page 9-8
- Creating Data Security and External DLP Policies, page 12-10

Using the Policies Tables

The policies table is an ordered list of policy groups and the settings you configure for each filtering component. It displays policy groups by row and control settings by column. The control settings you can define vary by policy type.

Figure 6-1 on page 8 shows the Access Policies table.
Chapter 6   Working with Policies

Working with Policy Groups

Figure 6-1   Access Policies Table

Access Policies

<table>
<thead>
<tr>
<th>Order</th>
<th>Group</th>
<th>Protocols and User Agents</th>
<th>URL Filters</th>
<th>Applications</th>
<th>Objects</th>
<th>Web Reputation and Anti-Malware Filters</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ExampleAP1 (Clients: TnLab)</td>
<td>(global policy)</td>
<td>(global policy)</td>
<td>(global policy)</td>
<td>(global policy)</td>
<td>(global policy)</td>
<td>Delete</td>
</tr>
<tr>
<td>2</td>
<td>ExampleAP2 (Clients: UTLS, SAP)</td>
<td>(global policy)</td>
<td>(global policy)</td>
<td>(global policy)</td>
<td>(global policy)</td>
<td>(global policy)</td>
<td>Delete</td>
</tr>
</tbody>
</table>


Click to edit user defined policy group membership. Global policy group (not editable). Click to customize policy control settings.

Figure 6-2 shows the Decryption Policies table.

Figure 6-2   Decryption Policies Table

Decryption Policies

<table>
<thead>
<tr>
<th>Order</th>
<th>Group F</th>
<th>URI Categories</th>
<th>Web Reputation</th>
<th>Default Action</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ExampleAF1 (Clients: ITMS)</td>
<td>(global policy)</td>
<td>(global policy)</td>
<td>(global policy)</td>
<td>Delete</td>
</tr>
<tr>
<td></td>
<td>Global Policy (Identity: null)</td>
<td>Monitor: 66</td>
<td>Enabled</td>
<td>Decrypt</td>
<td>Delete</td>
</tr>
</tbody>
</table>

(When enabled, authentication is applicable to forward connections and pre-established transparent IP-based credentials only.)

Click to edit user defined policy group membership. Global policy group (not editable). Click to customize policy control settings.

Any policy group that you create is added as a new row in the policies table. New policy groups inherit global policy settings for each control setting until you override them. To edit policy groups, click the links in each row.

When you create or configure a policy group, you define the following components:
• **Policy group membership.** Define how to group users that belong to the policy group. For user defined policy groups, you can group by different properties, such as client IP address, authentication group or user name, or URL category. The properties you can define for a policy depends on the policy type.

Click the policy group name to edit the group membership requirements, such as client IP address and authentication requirements. A page is displayed where you can configure membership requirements.

---

**Note**

For global policies, you can only define the membership requirements for the global Identity group and not for the global Access, Decryption, or Routing groups. Global Access, Decryption, and Routing groups always match all Identities.

For more information about policy group membership, see [Policy Group Membership, page 6-10](#).

• **Policy group control settings.** Define how users in the group can use the Internet. The control settings you can define depend on the policy type. For example, for Routing Policies, you define from which proxy group to fetch the content, and for Access Policies, you can use the Web Security appliance features, such as Web Reputation, anti-malware scanning, and more to determine whether or not to allow the client request.

Click the link in the policy group row under the control setting you want to configure, such as URL Categories or Routing Destination. When you click a link in the table, a page is displayed where you can configure settings for that policy group.

For more information on configuring control settings for each policy type, see the following sections:

- Controlling HTTP and Native FTP Traffic, page 8-11
- Controlling HTTPS Traffic, page 10-34
- Creating Routing Policies, page 9-8
- Controlling Upload Requests Using External DLP Policies, page 12-25
Policy Group Membership

All policy groups define which transactions apply to them. When a client sends a request to a server, the Web Proxy receives the request, evaluates it, and determines to which policy group it belongs. The Web Proxy applies the configured policy control settings to a client request based on the client request’s policy group membership.

Transactions belong to a policy group for each type of policy that is enabled. If a policy type has no user defined policy groups, then each transaction belongs to the global policy group for that policy type.

Policy group membership for a Routing, Decryption, Access, Data Security, and External DLP Policies is based on an Identity and optional additional criteria. That means that the Web Proxy evaluates Identity groups before the other policy types. The Web Security appliance allows you to define some membership criteria at either the Identity level or the non-Identity policy level. For more information, see Policy Group Membership Rules and Guidelines, page 6-12.

Suppose you define an Identity by subnet 10.1.1.0/24 and then create an Access Policy using that Identity. The Access Policy membership applies to all IP addresses specified in the Identity by default. You can then choose to configure the Access Policy membership so that it applies to a subset of the addresses defined in the Identity, such as addresses 10.1.1.0-15.

For more information defining membership for each policy type, see the following sections:

- Evaluating Identity Group Membership, page 7-2
- Evaluating Access Policy Group Membership, page 8-4
- Evaluating Decryption Policy Group Membership, page 10-27
- Evaluating Routing Policy Group Membership, page 9-5
- Evaluating Data Security and External DLP Policy Group Membership, page 12-7

Authenticating Users versus Authorizing Users

The Web Security appliance separates where it authenticates users from where it authorizes users.
Authentication is the mechanism by which the Web Proxy securely identifies a user. It answers the following questions:

- Who is the user?
- Is the user really whom he/she claims to be?

Authorization is the mechanism by which the Web Proxy determines the level of access the user has to the World Wide Web. It answers the following questions:

- Is this user allowed to view this website?
- Is this user allowed to connect to this HTTPS server without the connection being decrypted?
- Is this user allowed to directly connect to the web server, or must it connect to another proxy server first?
- Is this user allowed to upload this data?

The Web Proxy can only authorize a user to access an Internet resource after it authenticates who the user is. The Web Proxy authenticates users when it evaluates Identity groups, and it authorizes users when it evaluates all other policy group types. What that means is the Identity group indicates who is making the request, but does not indicate whether that client is allowed to make the request.

By separating authentication from authorization, you can create a single Identity group that identifies a group of users and then you can create multiple policy groups that allow different levels of access to subsets of users in the group in the Identity.

For example, you can create one Identity group that covers all users in an authentication sequence. Then you can create an Access Policy group for each authentication realm in the sequence. You can also use this Identity to create one Decryption Policy with the same level of access for all users in the Identity.

**Working with Failed Authentication and Authorization**

You can allow users another opportunity to access the web if they fail authentication or authorization. How you configure the Web Security appliance depends on what fails:

- **Authentication.** When authentication fails, you can grant guest access to the user. Authentication might fail under the following circumstances:
  - A new hire has been provided credentials in an email but they are not yet populated in the authentication server.
A visitor comes to the office and needs to be granted restrictive Internet access, but is not in the corporate user directory.

For more information on configuring guest access, see Allowing Guest Access to Users Who Fail Authentication, page 7-13.

- **Authorization.** A user might authenticate correctly, but not be granted access to the web due to the applicable Access Policy. In this case, you can allow the user to re-authenticate with more privileged credentials. To do this, enable the “Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction” global authentication setting. For more information, see Allowing Users to Re-Authenticate, page 20-39.

**Working with All Identities**

You can create a policy group that specifies “All Identities” as the configured Identity group. “All Identities” applies to every valid client request because by definition, every request either succeeds and has a user defined or global Identity assigned to it or is terminated because it fails authentication (and no guest access was provided for users failing authentication).

When you create a policy group that uses All Identities, you must configure at least one advanced option to distinguish the policy group from the global policy group.

Typically, you use All Identities in a policy while also configuring an advanced option, such as a particular user agent or destination (using a custom URL category). This allows you to create a single rule that makes an exception for a specific case instead of creating multiple rules to make the exception for the specific case. For example, you can create an Access Policy group whose membership applies to All Identities and a custom URL category for all intranet pages. Then you can configure the Access Policy control settings to disable anti-malware filtering and Web Reputation scoring.

**Policy Group Membership Rules and Guidelines**

Consider the following rules and guidelines when defining policy group membership:

- The Web Proxy evaluates Identity groups before the other policy types.
Subnet membership criteria defined in the Identity group can be further narrowed down in the policy group using the Identity group.

Advanced membership criteria (proxy ports, URL categories, and user agents) defined in the Identity group cannot be defined in the policy group using the Identity group.

Define Identity groups as broadly as possible. Then you can use the Identity groups in other policy types and further narrow down membership as necessary.

Define fewer, more generic Decryption and Routing Policies as much as possible.

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. For other purposes, define membership by URL category in the Access, Decryption, Routing, Data Security, or External DLP Policy group. This can increase performance in most cases.

Working with Time Based Policies

The Web Security appliance provides the means to create time based policies by specifying time ranges, such as business hours, and using those time ranges to define access to the web. You can define policy group membership based on time ranges, and you can specify actions for URL filtering based on time ranges.

You might want to use time ranges to accomplish the following tasks:

- You can block access to high bandwidth sites, such as streaming media, or distracting sites, such as games, during business hours.
- You can route transactions to a particular external proxy after midnight when the other proxies are being serviced.
- You can allow larger files to be downloaded on the weekends.

Define time ranges on the Web Security Manager > Defined Time Ranges page. You can create time ranges to define concepts such as “business hours” or “weekend shift.” Then you can use the time ranges in the following locations:

- Policy group membership for a Routing, Access, or Decryption Policy.
- URL filtering settings for Access Policies.
When you define a time range, you can specify the day(s) of the week and the time of day. A transaction matches the time range when it occurs on one of the days specified and during the time specified. You can also define multiple combinations of day and time in a single time range. For example, you can define a time range that applies to transactions that occur on Monday through Friday from 08:00 to 17:00 or on Saturday from 09:00 to 13:00.

Policies and URL filtering actions can be defined inside or outside the defined time ranges.

**Note**  
Because you can define time based policy group membership only for Routing, Access, and Decryption Policies, but not Identities, you cannot create time based policies that define when users must authenticate. Authentication requirements are defined in Identity groups, but time based policies are defined in other policy group types. (bug #41723)

## Creating Time Ranges

To create a time range:

**Step 1**  
Go to Web Security Manager > Defined Time Ranges.

**Step 2**  
Click **Add Time Range**.

The Add Time Range page appears.
Step 3  In the Time Range Name field, enter a name to use for the time range. Each time range name must be unique.

Step 4  In the Time Zone section, choose whether to use the time zone setting on the Web Security appliance or a different time zone setting you configure.

Step 5  In the Time Values section, define at least one row that specifies the days of the week and time of day to include in this time range.

a. In the Day of the Week section, select at least one day.

b. In the Time of Day section, choose All Day or enter a time range in the day using the From and To fields.

Each time range includes the start time and excludes the end time. For example, entering 8:00 through 17:00 matches 8:00:00 through 16:59:59, but not 17:00:00.

Midnight must be specified as 00:00 for a start time, and as 24:00 for an end time.

Note  A transaction must occur on the day and in the time specified to match a row in the Time Values section. That means the Day of Week and Time of Day values have an “AND” relationship with each other within a single row.

Step 6  Optionally, you can create additional time value rows by clicking Add Row.
Working with User Agent Based Policies

The Web Security appliance provides the means to create policies to define access to the web by the client application (user agent), such as a web browser, making the client request. You can define policy group membership based on user agents, and you can specify control settings based on user agents.

You might want to specify user agents to accomplish the following tasks:

- You can exempt certain user agents from authentication. You might want to do this for client applications that cannot handle prompting users for authentication credentials. For more information about how to do this, see Exempting User Agents from Authentication, page 6-18.
- You can block access from particular user agents that you define.

You can configure user agents in the following locations:

- Policy group membership for all policy types, including Identities.
- Application control settings for Access Policies.

**Note**

When the appliance is deployed in transparent mode, user agent information is not available for Decryption Policies.

Configuring User Agents for Policy Group Membership

When you define policy group membership for any policy type, you can expand the Advanced section to define membership by additional criteria, such as user agent. When you click the User Agents link, the Membership by User Agent page appears allowing you to define membership by user agent.
Figure 6-3 on page 17 shows the Membership by User Agent page for an Identity policy group.

**Figure 6-3  Defining Policy Group Membership by User Agent**

On this page, you can select as many user agents as desired. The web interface includes some of the more common user agents that you can select using a check box. You can also type a regular expression to define any user agent necessary.

For each user agent you select in the Common User Agents section, AsyncOS for Web creates a regular expression to define the user agent. However, if you select the Any Versions option for each browser type, AsyncOS for Web creates a single regular expression that represents all versions of that browser instead an expression for each version. Creating one regular expression instead of multiple increases performance.

For example, when you select “Version 2.X” and “Version 1.X or earlier” for Firefox, AsyncOS for Web uses the following regular expressions:
Tracing Policies

Firefox/2
Firefox/1

However, when you select “Firefox Any Versions,” AsyncOS uses the following regular expression:

Firefox

Also, you can configure the policy group membership to either match the user agents you define, or matching all other user agents than the ones defined.

Exempting User Agents from Authentication

To exempt a user agent from authentication:

Step 1 Create an Identity policy group with membership that is based on the user agent to exempt.

For more information about creating Identities, see Creating Identities, page 7-20.

Step 2 Do not require authentication for the Identity policy group.

Step 3 Place the Identity policy group above all other Identity policy groups that require authentication.

Step 4 Submit and commit your changes.

Tracing Policies

The Web Security appliance web interface includes a tool that traces a particular client request and details how the Web Proxy processes the request. The Web Proxy evaluates the request against all committed Access, Decryption, IronPort Data Security, Outbound Malware Scanning, and Routing Policies and calculates other attributes, such as the web reputation score.

The policy trace tool allows administrators to troubleshoot when end users ask questions about Web Proxy behavior. It simulates client requests as if they were made by the end users and describes Web Proxy behavior. It can be a powerful troubleshooting or debugging tool, especially if you have combined many of the advanced features available on the Web Security appliance.
When you use the policy trace tool, the Web Proxy does not record the requests in the access log or reporting database.

By default, the Web Proxy simulates an HTTP GET request. However, when you specify a file to upload in the Request Details section, the Web Proxy simulates an HTTP POST request.

**Note**
The policy trace tool explicitly makes requests even if the Web Security appliance is deployed in transparent mode.

You can trace policies on the System Administration > Policy Trace page.

To trace policies:

**Step 1** Navigate to the System Administration > Policy Trace page.

**Step 2** In the URL field, enter the URL in the client request to simulate.

**Step 3** Optionally, in the Client IP Address field, enter the IP address of the machine to simulate.
Note If no IP address is specified, AsyncOS uses localhost.

Step 4 Optionally, you can simulate an authentication user by entering the following authentication requirements in the User area:

- **User Name.** Enter the user name of the authentication user.
- **Authentication Realm.** Choose an authentication realm.

Note For authentication to work for the user you enter here, the user must have already successfully authenticated through the Web Security appliance.

Step 5 Optionally, by expanding the Advanced section, you can configure additional settings to simulate a more specific user request that you want to trace. Figure 6-4 shows the expanded Advanced section.
Figure 6-4  Policy Trace Feature Advanced Section

The Advanced settings are divided into details of the transaction request to simulate and transaction response details to override.

Step 6  Configure the transaction request information to simulate as desired. Table 6-1 describes the request side advanced settings you can configure.

Table 6-1  Policy Trace Advanced Settings for Requests

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Port</td>
<td>Select a specific proxy port to use for the trace request to test policy group membership based on proxy port.</td>
</tr>
<tr>
<td>User Agent</td>
<td>Specify the user agent to simulate in the request.</td>
</tr>
<tr>
<td>Time of Request</td>
<td>Specify the day of week and time of day to simulate in the request.</td>
</tr>
</tbody>
</table>
Step 7

Configure the transaction response details to override as desired.

You might want to override a transaction response detail to simulate how a different response value, such as a lower web reputation score, would affect the policies assigned to the transaction. Table 6-2 describes the response side advanced settings you can configure.

### Table 6-2  Policy Trace Advanced Settings for Response Overrides

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Category</td>
<td>Choose whether or not to override the URL category of the transaction response.</td>
</tr>
<tr>
<td>Application</td>
<td>Choose an application that the Application Visibility and Control engine can detect.</td>
</tr>
<tr>
<td>Object Size</td>
<td>Enter the size of the response object in bytes. You can enter K, M, or G to represent Kilobytes, Megabytes, or Gigabytes.</td>
</tr>
<tr>
<td>MIME Type</td>
<td>Enter the MIME type.</td>
</tr>
<tr>
<td>Web Reputation Score</td>
<td>Enter the web reputation score from -10.0 to 10.0.</td>
</tr>
<tr>
<td>Anti-malware Scanning Verdicts</td>
<td>Choose whether or not to override the Webroot, McAfee, or Sophos scanning verdicts.</td>
</tr>
</tbody>
</table>
Step 8  Click **Find Policy Match**.

The policy trace tool displays the results in the Results area.

**Note**  The **Find Policy Match** button turns into a **Cancel** button while the policy trace processes the parameters you enter. You can cancel the trace at any time.

Figure 6-5 on page 23 shows the Policy Trace page with some results from a policy trace.

**Figure 6-5  Policy Trace Results**

<table>
<thead>
<tr>
<th>Policy Trace</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td><strong>Transaction</strong></td>
</tr>
<tr>
<td><strong>User</strong></td>
</tr>
<tr>
<td><strong>Authentication Realm</strong></td>
</tr>
<tr>
<td><strong>Authorized Groups</strong></td>
</tr>
</tbody>
</table>

Advanced Find Policy Match

**Results**

<table>
<thead>
<tr>
<th>URL Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Category: News</td>
</tr>
<tr>
<td>IMBS Score: 6.0</td>
</tr>
<tr>
<td>Object Size: 93891 bytes</td>
</tr>
<tr>
<td>MIME Type: text/html</td>
</tr>
</tbody>
</table>

**Policy Match**

<table>
<thead>
<tr>
<th>Description policy: None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing policy: Global Routing Policy</td>
</tr>
<tr>
<td>Access policy: Global Access Policy</td>
</tr>
</tbody>
</table>

Final Result

<table>
<thead>
<tr>
<th>Request completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details: Request allowed by Web Reputation score</td>
</tr>
<tr>
<td>Trace session complete</td>
</tr>
</tbody>
</table>
Identities Overview

To control web traffic on the network and protect your network from web based threats, the Web Proxy needs to identify who is trying to access the web. Users can be identified by different criteria, such as their machine address or authenticated user name. The Web Proxy can apply different actions to transactions based on who is submitting the request.

To identify who is accessing the web, you create Identities in the Web Security appliance. An Identity is a policy that identifies and groups users. An Identity addresses the question, “who are you?”
Identities are the only policy where you define whether or not authentication is required to access the web. However, Identities do not specify a list of users who are authorized (allowed) to access the web. You specify authorized users in the other (non-Identity) policy types.

All other policy types use an Identity as the basis to determine which policy group applies to the transaction. That means you can create a single Identity and use it multiple times in the non-Identity policy groups.

You might want to group the following types of users or machines:

- **A group of machine addresses in a test lab.** You can create a Routing Policy with this Identity so requests from these machines are fetched directly from the destination server.

- **All authenticated users based on the All Realms authentication sequence.** You can create a single Access Policy using this Identity, or you can create a different Access Policy for each authentication realm and configure different control settings for users in each realm.

- **Users accessing the Web Security appliance on a particular proxy port.** You can create a Routing Policy using this Identity that fetches content from a particular external proxy for requests that explicitly connect to the appliance on a particular proxy port.

- **All subnets trying to access a website in a user defined URL category do not require authentication.** You can create an Access Policy using this Identity to exempt requests to particular destinations from authentication. You might want to do this for Windows update servers.

Define Identities on the Web Security Manager > Identities page. For more information about creating Identities, see Creating Identities, page 7-20.

### Evaluating Identity Group Membership

When a client sends a request to a server, the Web Proxy receives the request, evaluates it, and determines to which Identity group it belongs.

To determine the Identity group that a client request matches, the Web Proxy follows a very specific process for matching the Identity group membership criteria. During this process, it considers the following factors for group membership:

- **Subnet.** The client subnet must match the list of subnets in a policy group.
Chapter 7 Identities

Evaluating Identity Group Membership

- **Protocol.** The protocol used in the transaction, either HTTP/HTTPS or native FTP.

- **Port.** The proxy port of the request must be in the Identity group’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.

  You might want to define Identity group membership on the proxy port if you have one set of clients configured to explicitly forward requests on one port, and another set of clients configured to explicitly forward requests on a different port.

  **Note** Cisco recommends only defining Identity group membership by the proxy port when the appliance is deployed in explicit forward mode, or when clients explicitly forward requests to the appliance. When you define Identity group membership by the proxy port when clients requests get transparently redirected to the appliance, some requests might be erroneously denied.

- **User agent.** The user agent making the request must be in the Identity group’s list of user agents, if any are listed. You might want to group by user agent for user agents that cannot handle authentication and you want to create an Identity that does not require authentication.

- **URL category.** The URL category of the request URL must be in the Identity group’s list of URL categories, if any are listed. You might want to group by URL destination category if you create different authentication groups based on URL categories and want to apply them to users depending on the website categorization.

- **Authentication requirements.** If the Identity group requires authentication, the client authentication credentials must match the Identity group’s authentication requirements. For more information about how authentication works with Identity groups, see Understanding How Authentication Affects Identity Groups, page 7-4.

The information in this section gives an overview of how the appliance matches client requests to Identity groups. For more details on exactly how the appliance matches client requests, see Matching Client Requests to Identity Groups, page 7-10.
The Web Proxy sequentially reads through each Identity group in the Identity policies table. It compares the client request status to the membership criteria of the first Identity group. If they match, the Web Proxy assigns the Identity group to the transaction.

If they do not match, the Web Proxy compares the client request to the next Identity group. It continues this process until it matches the client request to a user defined Identity group, or if it does not match a user defined Identity group, it matches the global Identity policy. When the Web Proxy matches the client request to an Identity group or the global Identity policy, it assigns the Identity group to the transaction.

If at any time during the comparison process the user fails authentication, the Web Proxy terminates the request. For more information about how authentication works with Identity groups, see Understanding How Authentication Affects Identity Groups, page 7-4.

After the Web Proxy assigns an Identity to a client request, it evaluates the request against the other policy group types. For more information, see the following locations:

- Evaluating Access Policy Group Membership, page 8-4
- Evaluating Decryption Policy Group Membership, page 10-27
- Evaluating Routing Policy Group Membership, page 9-5
- Evaluating Data Security and External DLP Policy Group Member, page 12-7

**Understanding How Authentication Affects Identity Groups**

Requiring authentication for users can help your organization control access to the web for groups of users. AsyncOS allows you to create multiple Identity groups and define the membership criteria based on authentication requirements.

When authentication is required for an Identity group, a gold key icon appears next to the Identity group name in the Policies table, as shown in Figure 7-1.
To define authentication requirements for an Identity group, you can choose an authentication realm or sequence that applies to the Identity group.

You can specify the authorized users when you use the Identity in a non-Identity policy group.

Consider the following rules and guidelines when creating and ordering Identity groups:

- **Identity group order.** All Identity groups that do not require authentication must be above Identity groups that require authentication.

- **Cookie-based authentication.** 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. How HTTPS and FTP over HTTP requests are matched against the Identity groups varies based on other factors. For more information, see Understanding How Authentication Affects HTTPS and FTP over HTTP Requests, page 7-6.

- **Identity uniqueness.** Verify the Identity group membership requirements are unique for each Identity group. If two Identity groups require the exact same membership, then client requests never match the lower Identity group. If any non-Identity policy uses the lower Identity group, client requests never match that policy.
• **Global Identity policy.** The global Identity policy does not require authentication by default when you create an authentication realm. If you want the global Identity policy to require authentication, you must assign an authentication realm, authentication sequence, or the All Realms sequence to the global Identity policy.

For some examples of how the Web Proxy matches client requests to an Identity group for different Identity policies tables, see Example Identity Policies Tables, page 7-31.

**Understanding How Authentication Affects HTTPS and FTP over HTTP Requests**

How the Web Proxy matches HTTPS and FTP over HTTP requests with Identities depends on the type of request (either explicitly forwarded or transparently redirected to the Web Proxy) and the authentication surrogate type:

• **No authentication surrogates.** The Web Proxy matches HTTPS and FTP over HTTP requests with Identity groups the same way it matches HTTP requests. For a diagram of how this occurs, see Figure 7-2 on page 11.

• **IP-based authentication surrogates and explicit requests.** The Web Proxy matches HTTPS and FTP over HTTP requests with Identity groups the same way it matches HTTP requests. For a diagram of how this occurs, see Figure 7-2 on page 11.

• **IP-based authentication surrogates and transparent requests.** The Web Proxy matches FTP over HTTP requests with Identity groups the same way it matches HTTP requests. But for HTTPS requests, the behavior is different, depending on whether or not the HTTPS request comes from a client that has authentication information available from an earlier HTTP request:
  – **Information available from a previous HTTP request.** The Web Proxy matches HTTPS requests with Identity groups the same way it matches HTTP requests. HTTPS requests are treated with the Identity associated with the IP address.
  – **No information available from a previous HTTP request.** When the Web Proxy has no credential information for the client, then it 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.

For a diagram of how this occurs, see Figure 7-2 on page 11.

- **Cookie-based authentication surrogates and transparent 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. In this situation, HTTPS and FTP over HTTP requests still match the Identity group according to the other membership criteria, but the Web Proxy does not prompt clients for authentication even if the Identity group 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 the non-Identity policy groups, it matches only non-Identity groups that specify “All Identities” and apply to “All Users.” Typically, this is the global policy, such as the global Access Policy. For a diagram of how this occurs, see Figure 7-3 on page 12.

- **Cookie-based authentication surrogates and explicit requests.** The behavior is different, depending on whether or not credential encryption is enabled:
  - **Credential encryption enabled.** The behavior is the same as cookie-based authentication with transparent requests, as described previously.
  - **Credential encryption disabled.** The Web Proxy uses no surrogates. HTTPS and FTP over HTTP requests are authenticated and matched to Identity groups like HTTP requests. For a diagram of how this occurs, see Figure 7-2 on page 11.
Table 7-1 summarizes the previous information.

Table 7-1  *Matching HTTPS and FTP over HTTP Requests to Identities*

<table>
<thead>
<tr>
<th>Surrogate Types</th>
<th>Explicit Requests</th>
<th>Transparent Requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Surrogate</td>
<td>HTTPS and FTP over HTTP requests are matched like HTTP requests.</td>
<td>N/A</td>
</tr>
<tr>
<td>IP-based</td>
<td>HTTPS and FTP over HTTP requests are matched like HTTP requests.</td>
<td>FTP over HTTP requests are matched like HTTP requests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTPS requests are matched like HTTP requests under any of the following conditions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A previous HTTP request was authenticated using an identity with an IP-based surrogate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A previous HTTP request was not authenticated, but the HTTPS Proxy is configured to decrypt the first HTTPS request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Otherwise, if a previous HTTP request was not authenticated and the HTTPS Proxy is configured to deny the request, the HTTPS request fails.</td>
</tr>
<tr>
<td>Cookie-based</td>
<td>The client is not prompted for authentication.</td>
<td>The client is not prompted for authentication.</td>
</tr>
</tbody>
</table>
Understanding How Authentication Scheme Affects Identity Groups

You define the authentication scheme for each Identity group, not at each realm or sequence. That means you can use the same NTLM realm or a sequence that contains an NTLM realm and use it in Identity groups that use either the NTLMSSP, Basic, or “Basic or NTLMSSP” authentication schemes.

The Web Proxy communicates which scheme(s) it supports to the client application at the beginning of a transaction. The Identity group currently in use determines which scheme(s) it supports. When the Web Proxy informs the client application that it supports both Basic and NTLMSSP, the client application chooses which scheme to use in the transaction.

Some client applications, such as Internet Explorer, always choose NTLMSSP when given a choice between NTLMSSP and Basic. This might cause a user to not pass authentication when all of the following conditions are true:

- The Identity group uses a sequence that contains both LDAP and NTLM realms.
- The Identity group uses the “Basic or NTLMSSP” authentication scheme.
- A user sends a request from an application that chooses NTLMSSP over Basic.
- The user only exists in the LDAP realm.

When this happens, the Web Proxy uses the NTLMSSP scheme to authenticate users in this Identity group because the client requests it. However, LDAP servers do not support NTLMSSP, so no user that exists only in the specified LDAP server(s) can pass authentication in this Identity group.

Therefore, when you need to use an authentication sequence that contains both LDAP and NTLM realms, consider the client applications that might try to access a URL when you configure the authentication scheme for an Identity group. For example, you might want to choose Basic as the only authentication scheme for an Identity group in some cases.
Matching Client Requests to Identity Groups

Figure 7-2 on page 11 shows how the Web Proxy evaluates a client request against the Identity groups when the Identity is configured to use:

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

Figure 7-3 on page 12 shows how the Web Proxy evaluates a client request against the Identity groups when the Identity is configured to use cookies as the authentication surrogates, credential encryption is enabled, and the request is explicitly forwarded.
Figure 7-2  Policy Group Flow Diagram for Identities - No Surrogates and IP-Based Surrogates

Receive request from client.

- Compare the client request against the next (or first) identity group in the policies table.

  - Is the client subnet in the identity group's list of subnet(s)?
    - Yes, or none defined
  
  - Is the proxy port in the identity group's list of ports in the Advanced section?
    - Yes, or none defined
  
  - Is the user agent in the policy group's list of user agents in the Advanced section?
    - Yes, or none defined
  
  - Is the URL category of the request URL in the Identity group's list of URL categories in the Advanced section?
    - Yes, or none defined

- Does the identity group require authentication?
  - Yes
  
  - Does the client successfully authenticate as a member of the applicable realm or sequence?
    - No
    
  - Does the Identity support guest privileges for users failing authentication?
    - No
    
  - Assign the Identity and then evaluate the request against the other policy types.
  
- Terminate the request. Reply to client with authentication required.
Figure 7-3  Policy Group Flow Diagram for Identities - Cookie-Based Surrogates

Receive request from client.

No
Is this a transparently redirected encrypted HTTPS transaction received before an HTTP transaction?

Yes
Is the HTTPS Proxy configured to decrypt the request for authentication purposes?

No
Compare the client request against the next (or first) Identity group in the policies table.

Yes
No
Is the client subnet in the Identity group's list of subnet(s)?

Yes, or none defined
No
Is the proxy port in the Identity group's list of ports in the Advanced section?

Yes, or none defined
No
Is the user agent in the policy group's list of user agents in the Advanced section?

Yes, or none defined
No
Is the URL category of the request URL in the Identity group's list of URL categories in the Advanced section?

Yes, or none defined
No
Does the Identity group require authentication?

Yes

No
Does the client successfully authenticate as a member of the applicable realm or sequence?

No

Does the Identity support guest privileges for users failing authentication?

Yes
Assign the Identity and then evaluate the request against the other policy types.

No
Terminate the request. Reply to client with authentication required.
Chapter 7      Identities

Allowing Guest Access to Users Who Fail Authentication

Allowing Guest Access to Users Who Fail Authentication

You can grant limited access to users who fail authentication due to invalid credentials. By default, when a client passes invalid authentication credentials, the Web Proxy continually requests valid credentials, essentially blocking access to all Internet resources. However, when you allow guest access, the first time the client passes invalid authentication credentials, the user is treated as a guest and the Web Proxy does not request authentication again.

You might want to grant guest access to users in the following situations:

- A visitor comes to the office and needs to be granted restrictive Internet access, but is not in the corporate user directory.
- An employee from another branch location (or from an acquired company) comes to the corporate headquarters, and needs Internet access. The user directories of the branch location (or acquired company) and corporate headquarters are separate, so the employee's credentials do not work in the corporate headquarters.
- A new hire has been provided credentials in an email but they are not yet populated in the authentication server.
- A user logs into a Windows workstation using a local account instead of a Windows domain account and the user needs access to the Internet.

The authentication server administrator in your organization can create a guest user account in the user directory. However, allowing guest access through the Web Security appliance has the benefit that the administrator does not have to communicate the guest credentials to every visitor.

To grant guest access to users who fail authentication, you create an Identity that requires authentication, but also allows guest privileges. Then you create another policy using that Identity and apply that policy to the guest users. When users who fail authentication have guest access, they can access the resources defined in the policy group that specifies guest access for that Identity.

A user who fails authentication has all transactions blocked if either of the following conditions are true:

- Guest privileges are not provided in any Identity.
- The user does not match any Identity that provides guest privileges.
A user who fails authentication has transactions *allowed* when *all* of the following conditions are true:

- The user matches an Identity with guest privileges.
- A non-Identity policy group uses that Identity and applies to guest users.

For example, you can create an Access or Decryption Policy that is specific to guest users.

**Note**

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

When the Web Proxy grants a user guest access, it identifies and logs the user as a guest in the access logs. You can specify whether the Web Proxy identifies the user by IP address or user name. In the access logs, reports, and end-user acknowledgement page, entries for guest users have one of the following formats:

- (unauthenticated) *IP_address*
- (unauthenticated) *username_entered*

You can enable guest access for an Identity that uses any authentication protocol or scheme.

To grant guest access to a user:

**Step 1** Define an Identity group and enable the Support Guest privileges option.
Chapter 7      Identities

Allowing Guest Access to Users Who Fail Authentication

Step 2 Create an Access, Decryption, Routing, Data Security, or External DLP Policy and select the Identity created in step 1.

Step 3 In the Access, Decryption, Routing, Data Security, or External DLP Policy group membership, select “Guests (users failing authentication)” for the Identity in step 1.

Step 4 Submit and commit your changes.
Identifying Users Transparently

Traditionally, users identified by an authentication user name are explicitly prompted to enter a user name and password. The credentials the user enters are then 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 so that it identifies users by an authenticated user name transparently—that is, without prompting the end user. You might want to do this to:

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

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

To identify users transparently, you must define at least one LDAP authentication realm that supports Novell eDirectory.

You can also transparently identify remote users when using Secure Mobility Solution. For more information, see Transparently Identifying Remote Users, page 13-5.
Understanding Transparent User Identification

Novell eDirectory maintains a mapping that matches authenticated user names to their current IP addresses. AsyncOS for Web communicates with the Novell eDirectory server at regular intervals to maintain the current IP address to user name mapping.

When a client makes a request for a website, the Web Security appliance receives the request and obtains the IP address from the request. AsyncOS for Web then checks the IP address to user name mapping stored on the Web Security appliance to assign a user name to the client request. AsyncOS for Web also fetches the user groups from the Novell eDirectory server at this time. Assuming it matches a user name to the IP address, AsyncOS for Web applies policies to the transaction as appropriate.

If the IP address does not match a user name, you can configure how to handle the transaction. You can grant the end user guest access, or you can force an authentication prompt to appear to the end 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. Figure 7-4 shows where you grant user access when configuring an Identity for transparent user identification.

The current IP address to user name mapping is updated, by default, every 600 seconds. You can change this time interval using the advancedproxyconfig > authentication CLI command.

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 Allowing Users to Re-Authenticate, page 20-39.
Identifying Users Transparently

Rules and Guidelines

Consider the following rules and guidelines when you identify users transparently using Novell eDirectory:

- Novell Client must be installed on each client machine, and end users must use it to authenticate against a Novell eDirectory server.
- The Novell LDAP tree used by the Novell client login must be the same LDAP tree configured in the authentication realm.
- If the Novell clients use multiple Novell LDAP trees, create an authentication realm for each tree, and then create an authentication sequence that uses each Novell LDAP authentication realm.
- When you configure the LDAP authentication realm for Novell eDirectory, you must specify a Bind DN for the query credentials.
- Novell eDirectory must be configured to update the NetworkAddress attribute of the user object when users login. For more information on how to do this, see the following Novell support article:
  http://www.novell.com/support/php/search.do?cmd=displayKC&docType=kc&externalId=7004564&sliceId=1&docTypeID=DT_TID_1_1&dialogID=100407203&stateId=0%200%20100405493?

Note: Novell eDirectory versions 8.6, 8.7, and 8.8 can be configured to update the NetworkAddress attribute.

- When querying Novell eDirectory, AsyncOS for Web only searches for direct parent groups that the user belongs to. It does not search nested groups.
- If your network environment includes both Novell eDirectory and Microsoft Active Directory and users fail to login using Novell eDirectory, they can either log into Active Directory using Basic authentication scheme or be granted guest access. They cannot use NTLMSSP authentication scheme.
- When using DHCP to assign IP addresses to client machines, ensure the IP address to user name mapping is updated on the Web Security appliance more frequently than the DHCP lease. Use the `advancedproxyconfig > authentication` CLI command to update the mapping update interval.
• If an end user logs out of a machine and another user logs in to 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 Identity 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 Identity to transparently authenticate users, the authentication surrogate must be IP address. You cannot select a different surrogate type.

• You can use the “network address” field of the user in Novell eDirectory to obtain the IP address of the workstation from where the user previously logged in.

• You can log which users were identified transparently in the access logs and WC3 logs using the %m and x-auth-mechanism custom fields. A value of SSO_EDIR indicates that the user name was obtained by matching the client IP address to an authenticated user name in Novell eDirectory. (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 the Secure Mobility Solution.)

## Configuring Transparent User Identification

To use transparent user identification:

---

**Step 1**

Create an LDAP authentication realm for a Novell eDirectory server. Configure the realm to use Version 3 and to “Support Novell eDirectory.”

For more information on configuring LDAP options, see LDAP Authentication, page 20-43.

For more information on creating authentication realms, see Creating Authentication Realms, page 20-15.
Creating Identities

You can create Identities based on combinations of several criteria, such as client subnet or the URL category of the destination site. You must define at least one criterion for Identity membership. When you define multiple criteria, the client request must meet all criteria to match the Identity.

For more information about how the Web Proxy matches a client request with an Identity, see Evaluating Identity Group Membership, page 7-2 and Matching Client Requests to Identity Groups, page 7-10.

You define Identity group membership on the Web Security Manager > Identities page.

Note
Deleting an authentication realm or sequence disables Identities that depend on the deleted realm or sequence.

To create an Identity group:

Step 1 Navigate to the Web Security Manager > Identities page.
Step 2 Click Add Identity.

Step 2 Define an Identity group that identifies users transparently using Novell eDirectory:
   b. Select the LDAP authentication realm that supports Novell eDirectory.
   c. Configure all other Identity options as desired.

For more information on creating Identities, see Creating Identities, page 7-20.

Step 3 Create policies that use the Identity for transparent user identification.
Chapter 7      Identities

Creating Identities

Identities: Add Identity

Identity Settings:

- Enable identity
- Name: [Field]

[Optional: Enter a name for the Identity group and an optional description.]

Description: [Field]

Insert Above: [Field]

Membership Definition:

Membership is defined by any combination of the following options. All criteria must be met for the policy to take affect.

Define Members by User Location:
- Local Users Only
- Remote Users Only
- Both

Define Members by Subnet:

[Table: Subnet Configuration]

Define Members by Protocol:
- All protocols
- HTTP/HTTPS Only
- Native FTP Only

Define Members by Authentication:
- No authentication

This option may not be valid if any preceding identity requires authentication on all subnets.

Advanced: Define additional group membership criteria.

Step 3
Enter a name for the Identity group and an optional description.

Note
Each Identity group name must be unique and only contain alphanumeric characters or the space character.

Step 4
In the Insert Above field, choose where in the policies table to place the Identity group.

When configuring multiple Identity groups, specify a logical order for each group. Carefully order your Identity groups to ensure that correct matching occurs.

Position groups that do not require authentication above the first policy group that requires authentication. For more information about how authentication affects Identity groups, see Understanding How Authentication Affects Identity Groups, page 7-4.

Step 5
In the Define Members by User Location section, configure the Identity to apply to local users, remote users, or both local and remote users.
The setting chosen here affects the available authentication settings for this Identity.

This section only appears when the Secure Mobility Solution is enabled. For more information, see Achieving Secure Mobility Overview, page 13-1.

In the Define Members by Subnet field, enter the addresses to which this Identity should apply.

You can enter IP addresses, CIDR blocks, and subnets. Separate multiple addresses with commas.

If you do not enter an address in this field, the Identity group applies to all IP addresses. For example, if you configure the Identity to require authentication, but do not define any other settings, then the Identity acts similarly to the Default Identity Policy with authentication required.

In the Define Members by Protocol section, choose to which protocols this Identity should apply:

- **All protocols.** Applies to all protocols the Web Security appliance supports.
- **HTTP/HTTPS Only.** Applies to all requests that use HTTP or HTTPS as the underlying protocol, including FTP over HTTP and any other protocol tunneled using HTTP CONNECT.
- **Native FTP Only.** Applies to native FTP requests only.

In the Define Members by Authentication section, choose whether or not this Identity requires authentication. You can choose one of the following options:

- **No Authentication.** The user is identified primarily by IP address. Go to Step 15.
- **Require Authentication.** The user is identified by the authentication credentials entered. Go to Step 9.
- **Identify Users Transparently through Novell eDirectory.** The user is identified by the current IP address to user name mapping received from the Novell eDirectory server. Go to Step 10.
Identify Users Transparently through Cisco ASA Integration. The user is identified by the current IP address to user name mapping received from the Cisco adaptive security appliance (ASA). Go to Step 11.

To configure the Identity to require authentication:

In the Select a Realm or Sequence field, choose a defined authentication realm or sequence.

If you choose an NTLM authentication realm or sequence that contains an NTLM authentication realm, then choose an authentication scheme in the Select a Scheme field.

To grant guest access to users who fail authentication due to invalid credentials, select the Support Guest privileges check box.

For more information, see Allowing Guest Access to Users Who Fail Authentication, page 7-13.

You can specify individual authenticated users or groups of users when you use the Identity in a different type of policy group. For more information, see Configuring Identities in Other Policy Groups, page 7-28.

d. Go to Step 12.

Step 10 To configure the Identity to use transparent user identification with Novell eDirectory:

a. In the Select a Realm or Sequence field, choose a defined LDAP authentication realm that supports Novell eDirectory or sequence that contains only LDAP realms that support Novell eDirectory.
Choose how to handle transactions when transparent user identification fails: either grant users guest access, or force an authentication prompt to appear to end users.

Transparent user identification might fail if the Web Proxy cannot determine the user who is currently logged in from the specified IP address. That is, if the IP address is not in the IP address to user mapping.

Choose whether or not to allow the user guest access when a user is shown an authentication prompt due to failed transparent user identification and the user then fails authentication due to invalid credentials.

For more information on transparent user identification, see Identifying Users Transparently, page 7-16.

Go to Step 12.

To configure the Identity to use transparent user identification by integrating with a Cisco adaptive security appliance (ASA):

In the Select a Realm or Sequence field, choose a defined authentication realm or sequence.

If you choose an NTLM authentication realm or sequence that contains an NTLM authentication realm, then choose the authentication scheme in the Select a Scheme field.

You can specify individual authenticated users or groups of users when you use the Identity in a different type of policy group. For more information, see Configuring Identities in Other Policy Groups, page 7-28.
Go to Step 12.

View the settings in the Authentication Surrogate section.

The options vary depending on the Web Proxy deployment mode. Choose how transactions used for authenticating the client are associated with a user (either by IP address or by using a cookie) after the user has authenticated successfully. Choose one of the options in Table 7-2:

<table>
<thead>
<tr>
<th>Surrogate Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The Web Proxy tracks an authenticated user at a particular IP address. To achieve transparent user identification, you must choose IP-based authentication.</td>
</tr>
<tr>
<td>Persistent Cookie</td>
<td>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.</td>
</tr>
<tr>
<td>Session Cookie</td>
<td>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.</td>
</tr>
<tr>
<td>No Surrogate</td>
<td>The Web Proxy does not use a surrogate to cache the credentials, and it tracks an authenticated user for every new TCP connection. When you choose this option, the web interface disables other settings that no longer apply. This option is available only in explicit forward mode and when you disable credential encryption on the Network &gt; Authentication page.</td>
</tr>
</tbody>
</table>
You might want to use IP-based authentication when:

- There is only one user on a client machine and you want users to be able to achieve single sign-on behavior.
- You want to use transparent user identification.
- You want to create an Identity that works with applications that do not work with cookie-based surrogates, such as MSN Messenger.

You might want to choose cookie-based authentication when there are multiple users on one machine, such as a Citrix server or a kiosk shared by many users.

For more information about which authentication surrogates are supported with other configurations and different types of requests, see Tracking Authenticated Users, page 20-42.

You can define a timeout value for the authentication surrogate for all requests. For more information, see Configuring Global Authentication Settings, page 20-23.

In the Explicit Forward Request field, choose whether or not the surrogate used for transparent requests should also be used for explicit requests.

Enabling credential encryption automatically enables this field.

This option appears only when the Web Proxy is deployed in transparent mode.

Optionally, expand the Advanced section to define additional membership requirements.

To define Identity group membership by any of the advanced options, click the link for the advanced option and configure the option on the page that appears.
Table 7-3 describes Identity group advanced options.

**Table 7-3 Identity Group Advanced Options**

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Ports</td>
<td>To define policy group membership by the proxy port used to access the Web Proxy, enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas.</td>
</tr>
<tr>
<td></td>
<td>For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. You might want to define policy group membership on the proxy port if you have one set of clients configured to explicitly forward requests on one port, and another set of clients configured to explicitly forward requests on a different port.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Cisco recommends defining policy group membership by the proxy port only when the appliance is deployed in explicit forward mode, or when clients explicitly forward requests to the appliance. If you define policy group membership by the proxy port when client requests are transparently redirected to the appliance, some requests might be denied.</td>
</tr>
<tr>
<td>URL Categories</td>
<td>Choose the user defined or predefined URL categories. Membership for both user defined and predefined URL categories is excluded by default, meaning the Web Proxy ignores all categories unless they are selected in the Add column.</td>
</tr>
<tr>
<td>User Agents</td>
<td>Choose whether or not to define policy group membership by the user agent used in the client request. You can select some commonly defined browsers, or define your own using regular expressions. Choose whether this policy group should apply to the selected user agents or to any user agent that is not in the list of selected user agents. For more information on creating user agent based policies, see Working with User Agent Based Policies, page 6-16.</td>
</tr>
</tbody>
</table>

**Step 17** Submit and commit your changes.
Configuring Identities in Other Policy Groups

Every non-Identity policy group specifies at least one Identity group as part of its policy group membership. You can configure a non-Identity policy group to use multiple Identity groups, and you can specify which users or groups of users are authorized to access the web using the policy group.

You might want to specify multiple Identity groups in a policy group under the following circumstances:

- You have an Identity group defined for HTTP transactions and another Identity group defined for native FTP transactions. You can create a single non-Identity policy group that applies to both HTTP and native FTP transactions
- Separate Identity groups are defined for each authentication realm. You want to create one Access Policy group that defines the same access control settings for users in multiple authentication realms.

**Note**
You can also specify All Identities and configure the authenticated users.

*Figure 7-5* shows a policy group that uses multiple Identities.
Figure 7-5  Multiple Identities in a Policy Group

<table>
<thead>
<tr>
<th>Policy Member Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Membership is defined by the combination of the following options. All options must be met for the policy to take effect.</td>
</tr>
<tr>
<td>Select One or More Identities</td>
</tr>
<tr>
<td>Identity</td>
</tr>
<tr>
<td>AllAuthenticatedUsers</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>SatelliteOffice</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>JCAUsers</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

The specified user groups in this Identity are authorized for this policy group.
All authenticated users in this Identity are authorized for this policy group.
This Identity uses an authentication sequence and this policy group applies to one realm in the sequence.

Note
If an Identity group becomes disabled, then that Identity group is removed (not disabled) from any non-Identity policy group that used it. If the Identity group becomes enabled again, the non-Identity policy groups that previously used the Identity do not automatically include the enabled Identity. Identity groups become disabled due to a deleted authentication realm or sequence.

To configure Identity group information in a policy group:

Step 1  Create a new policy group or edit the membership of an existing policy group for Access, Decryption, Routing, Data Security, or External DLP Policy.

Step 2  Scroll down to the Identities and Users section.
Chapter 7  Identities

Configuring Identities in Other Policy Groups

Step 3  Choose one of the following options from the dropdown menu:

- **Select One or More Identities.** This option allows you to configure specific Identity groups. Go to step 4.

- **All Identities.** This option specifies all configured Identity groups. Go to step 5.

Step 4  Under the Identity column, choose the Identity group to apply to this policy group.

Step 5  If you choose an Identity that requires authentication, you can specify which users are authorized for this policy group. These users must authenticate. In the Authorized Users and Groups column, choose one of the following options:

- **All authenticated users.** You can configure the Identity in this policy group to apply to all users in the Identity group by default. If the Identity group specifies an authentication sequence, you can configure this policy group to apply to one authentication realm or all realms in the sequence.

- **Selected Groups and Users.** You can configure the Identity in this policy group to apply to specific users. You can define users by group object or user object. Click the link for either Groups or Users, and enter the group or user information on the page that opens.

  When you add groups of users for an Identity using an NTLM authentication realm, the Edit Groups page displays the first 500 matching entries, omitting built-in groups.

- **Guests (users failing authentication).** If the Identity group allows guest access, you can configure this policy group to apply to all users who fail to authenticate in this Identity. For more information, see Allowing Guest Access to Users Who Fail Authentication, page 7-13.
• **All users (authenticated and unauthenticated users).** You can configure this policy group to apply to every user in every Identity group. This option only appears when you choose All Identities. When you apply the policy group to all users, you must specify at least one advanced option to distinguish this policy group from the global policy.

**Step 6** Optionally, if you configured specific Identity groups, you can add another Identity group to this policy group by clicking **Add Identity**.

**Step 7** If you add another Identity group, repeat steps 4 through 5.

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

### Example Identity Policies Tables

This section shows some sample Identity groups defined in an Identity policies table and describes how the Web Proxy evaluates different client requests using each Identity policies table.

#### Example 1

*Table 7-4* shows an Identity policies table with three user defined Identity groups. The first Identity group applies to a particular subnet and does not require authentication. The second Identity group applies to all subnets and requests for URLs in the “Proxies & Translators” category, and requires authentication on RealmA. The third Identity group applies to all subnets, has no advanced options defined, and requires authentication on RealmA. The global Identity policy applies to all subnets (by definition) and does not require authentication.

<table>
<thead>
<tr>
<th>Order</th>
<th>Subnet(s)</th>
<th>Authentication Required?</th>
<th>Realm or Sequence</th>
<th>Advanced Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.1.1.1</td>
<td>No</td>
<td>N/A</td>
<td>none</td>
</tr>
<tr>
<td>2</td>
<td>All</td>
<td>Yes</td>
<td>RealmA</td>
<td>URL Category is “Proxies &amp; Translators”</td>
</tr>
</tbody>
</table>
Chapter 7  Identities

Example Identity Policies Tables

Cisco IronPort AsyncOS 7.1 for Web User Guide

Table 7-4  Policies Table Example 1 (continued)

<table>
<thead>
<tr>
<th></th>
<th>All</th>
<th>Yes</th>
<th>RealmA</th>
<th>none</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>All</td>
<td>Yes</td>
<td>RealmA</td>
<td>none</td>
</tr>
<tr>
<td>Global Identity policy</td>
<td>All (by default)</td>
<td>No</td>
<td>N/A</td>
<td>N/A (none by default)</td>
</tr>
</tbody>
</table>

The Web Proxy matches client requests to Identity groups in this scenario differently, depending on the client’s subnet and the URL category of the request:

**Any client on subnet 10.1.1.1 for any URL.** When a client on subnet 10.1.1.1 sends a request for any URL, the Web Proxy evaluates the first Identity group and determines that the client subnet matches the first Identity group subnet. Then it determines that no authentication is required and no advanced options are configured, so it assigns the first Identity group to the transaction.

**Any client on a subnet other than 10.1.1.1 for URLs in the “Proxies & Translators” URL category.** When a client on a subnet other than 10.1.1.1 sends a request for a URL in the “Proxies & Translators” category, the Web Proxy evaluates the first Identity group and determines that the client subnet is not listed in the first Identity group’s list of subnets. Therefore, it evaluates the second Identity group, and then determines that the client subnet is listed in the second Identity group’s list of subnets. Then it determines that the URL in the request matches the URL category in the second Identity group’s advanced section. Then it determines that the second Identity group requires authentication, so it tries to authenticate the user against the authentication server(s) defined in RealmA. If the user exists in RealmA, the Web Proxy assigns the second Identity group to the transaction. If the user does not exist in RealmA, AsyncOS terminates the client request because the client failed authentication.

**Any client on a subnet other than 10.1.1.1 for any URL not in the “Proxies & Translators” URL category.** When a client on a subnet other than 10.1.1.1 sends a request for a URL, the Web Proxy evaluates the first Identity group and determines that the client subnet is not listed in the first Identity group’s list of subnets. Therefore, it evaluates the second Identity group, and then determines that the client subnet is listed in the second Identity group’s list of subnets. Then it determines that the URL in the request
does not match the URL category in the second Identity group’s advanced section. Therefore, it evaluates the third Identity group, and then determines that the client subnet is listed in the third Identity group’s list of subnets. The third Identity group does not have any advanced options configured, so continues to compare against authentication requirements. Then it determines that the third Identity group requires authentication, so it tries to authenticate the user against the authentication server(s) defined in RealmA. If the user exists in RealmA, the Web Proxy assigns the third Identity group to the transaction. If the user does not exist in RealmA, the Web Proxy terminates the client request because the client failed authentication.

Note that in this scenario, most client requests will never match the global Identity group because of the user defined Identity group (the third group) that applies to all subnets, has no advanced options, and requires authentication. Any client on the network that does not match the first or second Identity group will match the third Identity group. The exception to this is for HTTPS requests when the appliance is in transparent mode with cookie-based authentication. Any client on a subnet other than 10.1.1.1 will match the global Identity group even though it requires authentication.

Table 7-5 shows a policies table with two user defined Identity groups. The first Identity group applies to all subnets, requires authentication, and specifies RealmA for authentication. The second Identity group applies to all subnets, requires authentication, and specifies RealmB for authentication. Neither Identity group has any advanced option configured. The global Identity group applies to all subnets, requires authentication, and specifies the All Realms sequence for authentication.

<table>
<thead>
<tr>
<th></th>
<th>Policies Table Example 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>All</td>
</tr>
<tr>
<td>2</td>
<td>All</td>
</tr>
<tr>
<td>Global Identity policy</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>RealmA</td>
</tr>
<tr>
<td></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>RealmB</td>
</tr>
<tr>
<td></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>All Realms</td>
</tr>
<tr>
<td></td>
<td>N/A (none by default)</td>
</tr>
</tbody>
</table>
In this scenario, when a client sends a request for a URL, the Web Proxy evaluates the first Identity group and determines that the Identity group applies to all subnets and has no advanced options configured. It determines that the Identity group requires authentication and that the only realm specified in the Identity group is RealmA. Therefore, *in order for a client on any subnet to pass authentication, it must exist in RealmA.*

When a client that exists in RealmA sends a request for a URL, the client passes authentication and the Web Proxy assigns the first Identity group to the transaction. When a client that does *not* exist in RealmA sends a request for a URL, the client fails authentication and the Web Proxy terminates the request.

Note that when a client in RealmB sends a request for a URL, the Web Proxy does *not* match the client request with the second Identity group. This is because a previous Identity group already applies to the same subnets (and the exact same advanced options, which in this example is none) in the second Identity group and it requires authentication, but from RealmA instead. Clients in RealmB do not “fall through” to the second Identity group.

If you want users in RealmB to have different Access, Decryption, and Routing Policy settings applied to them than users in RealmA, perform the following steps:

1. Create an authentication sequence that contains both RealmA and RealmB. You can choose the order of the realms in the sequence depending on your business needs.

2. Create one Identity group and configure it for whichever subnets on which users in RealmA and RealmB might exist. In this example, you would configure the Identity group for all subnets.

3. Configure the Identity group to use the sequence you defined in step 1.

4. Create two user defined policy groups of the same type, such as Access Policies, and configure them both to use the Identity group with the authentication sequence you defined in step 3.

5. Configure the first policy group to only apply to users in one realm, such as RealmA. You can do this by specifying a particular realm in the sequence, or by using authentication groups, or entering specific usernames.

6. Configure the second policy group to only apply to users in the other realm, such as RealmB. You can do this by specifying a particular realm in the sequence, or by using authentication groups, or entering specific usernames.
When you configure the appliance in this way, any client that sends a request for a URL must exist in either realm in the sequence (RealmA or RealmB) in order to pass authentication at the Identity level. Once an Identity has been assigned to the client request, the Web Proxy can compare the client request against the other policy types and determine which policy group, such as an Access Policy group, to match and then apply those control settings. In this example, the Web Proxy matches users in RealmA with the policy group configured in step 5, and matches users in RealmB with the policy group configured in step 6.
This chapter contains the following information:

- Access Policies Overview, page 8-1
- Evaluating Access Policy Group Membership, page 8-4
- Creating Access Policies, page 8-7
- Controlling HTTP and Native FTP Traffic, page 8-11
- Blocking Specific Applications and Protocols, page 8-18

AsyncOS for Web uses multiple web security features in conjunction with its Web Proxy and DVS engine to control web traffic, protect networks from web-based threats, and enforce organization acceptable use policies. You can define policies that determine which HTTP connections are allowed and blocked.

To configure the appliance to handle HTTP requests, perform the following tasks:

**Enable the Web Proxy.** To allow or block HTTP traffic, you must first enable the Web Proxy. Usually, the Web Proxy is enabled during the initial setup using the System Setup Wizard. For more information, see Configuring the Web Proxy, page 5-3.
Step 2 Create and configure Access Policy groups. After the Web Proxy is enabled, you create and configure Access Policy groups to determine how to handle each request from each user. For more information, see Access Policy Groups, page 8-2.

Access Policy Groups

Access Policies define how the Web Proxy handles HTTP and FTP requests and decrypted HTTPS connections for network users. You can apply different actions to specified groups of users. You can also specify which ports the Web Proxy monitors for HTTP transactions.

Note

HTTP PUT and POST requests are handled by Outbound Malware Scanning, IronPort Data Security, and External DLP Policies. For more information, see Data Security and External DLP Policies Overview, page 12-1 and Outbound Malware Scanning, page 11-1.

When the Web Proxy receives an HTTP request on a monitored port or a decrypted HTTPS connection, it compares the request to the Access Policy groups to determine which Access Policy group to apply. After it assigns the request to an Access Policy group, it can determine what to do with the request. For more information about evaluating policy group membership, see Policy Group Membership, page 6-10.

The Web Proxy can perform any of the following actions on an HTTP request or decrypted HTTPS connection:

- **Allow.** The Web Proxy permits the connection without interruption. Allowed connections may not have been scanned by the DVS engine.
- **Block.** The Web Proxy does not permit the connection and instead displays an end user notification page explaining the reason for the block.
- **Redirect.** The Web Proxy does not allow the connection to the originally requested destination server and instead connects to a different specified URL. You might want to redirect traffic at the appliance if your organization published the links to an internal site, but the location of the site changed since publication, or if you do not have control over the web server. For more information about redirecting traffic, see Redirecting Traffic, page 16-23.
Chapter 8  Access Policies

Access Policies Overview

The preceding actions are final actions that the Web Proxy takes on a client request. The Monitor action that you can configure for Access Policies is not a final action. For more information, see Understanding the Monitor Action, page 8-3.

After the Web Proxy assigns an Access Policy to an HTTP or decrypted HTTPS request, it compares the request to the policy group’s configured control settings to determine which action to apply. You can configure multiple security components to determine how to handle HTTP and decrypted HTTPS requests for a particular policy group. For more information about the security components that you can configure and how the Web Proxy uses Access Policy groups to control HTTP traffic, see Controlling HTTP and Native FTP Traffic, page 8-11.

Understanding the Monitor Action

When the Web Proxy compares a transaction to the control settings, it evaluates the settings in order. Each control setting can be configured to perform one of the following actions for Access Policies:

- Monitor
- Allow
- Block
- Redirect

All actions except Monitor are final actions that the Web Proxy applies to a transaction. A final action is an action that causes the Web Proxy to stop comparing the transaction to the rest of the control settings.

The Monitor action is an intermediary action. The Web Proxy continues comparing the transaction to the other control settings to determine which final action to apply.

For example, if an Access Policy is configured to monitor a suspect user agent, the Web Proxy does not make a final determination about a request from the user agent. If an Access Policy is configured to block a particular URL category, then any request to that URL category is blocked before fetching the content from the server regardless of the server’s reputation score.
Evaluating Access Policy Group Membership

After the Web Proxy assigns an Identity to a client request, the Web Proxy evaluates the request against the other policy types to determine which policy group it belongs for each type. When the HTTPS Proxy is enabled, it applies HTTP and decrypted HTTPS requests against the Access Policies. When HTTPS Proxy is not enabled, by default, it evaluates HTTP and all HTTPS requests against the Access Policies.

The Web Proxy applies the configured policy control settings to a client request based on the client request's policy group membership.

To determine the policy group that a client request matches, the Web Proxy follows a specific process for matching the group membership criteria. During this process, it considers the following factors for group membership:

- **Identity.** Each client request either matches an Identity, fails authentication and is granted guest access, or fails authentication and gets terminated. For more information about evaluating Identity group membership, see Evaluating Identity Group Membership, page 7-2.

- **Authorized users.** If the assigned Identity requires authentication, the user must be in the list of authorized users in the Access Policy group to match the policy group. The list of authorized users can be any of the specified groups or users or can be guest users if the Identity allows guest access.
Advanced options. You can configure several advanced options for Access Policy group membership. Some options (such as proxy port and URL category) can also be defined within the Identity. When an advanced option is configured in the Identity, it is not configurable in the Access Policy group level.

The information in this section gives an overview of how the Web Proxy matches client requests to Access Policy groups. For more details about exactly how the Web Proxy matches client requests, see Matching Client Requests to Access Policy Groups, page 8-5.

The Web Proxy sequentially reads through each policy group in the policies table. It compares the client request status to the membership criteria of the first policy group. If they match, the Web Proxy applies the policy settings of that policy group.

If they do not match, the Web Proxy compares the client request to the next policy group. It continues this process until it matches the client request to a user defined policy group. If it does not match a user defined policy group, it matches the global policy group. When the Web Proxy matches the client request to a policy group or the global policy group, it applies the policy settings of that policy group.

Matching Client Requests to Access Policy Groups

Figure 8-1 on page 6 shows how the Web Proxy evaluates a client request against the Access Policy groups.
Figure 8-1  Policy Group Flow Diagram for Access Policies

1. Receive request from client.
2. Compare the client request against the next (or first) identity group in the policies table.
3. Is the current policy group the global policy?
   - Yes
   - No
4. Is the transaction assigned to one of the policy group's configured identities, or does the policy group use "All Identities"?
   - Yes
   - No
5. Is the current time in the policy group's configured time range in the Advanced section?
   - Yes, or no time range defined
   - No
6. Is the client subnet in the policy group's list of subnet(s) in the Advanced section?
   - Yes, or none defined
   - No
7. Is the proxy port in the policy group's list of ports in the Advanced section?
   - Yes, or none defined
   - No
8. Is the protocol in the policy group's list of protocol(s) in the Advanced section?
   - Yes, or none defined
   - No
9. Is the user agent in the policy group's list of user agents in the Advanced section?
   - Yes, or none defined
   - No
10. Is the URL category of the request URL in the policy group's list of URL categories in the Advanced section?
    - Yes, or none defined
    - No
11. Is the user one of the authorized users listed in the policy group?
    (List of authorized users can be a list of user names, user groups, all authenticated users, guest users, or All Users. If the policy group only uses identities with no authentication, then all clients are authorized.)
    - Yes
    - No

Apply the Access Policy group settings to the client request.
Creating Access Policies

You can create Access Policy groups based on combinations of several criteria, such as one or more Identities or the URL category of the destination site. You must define at least one criterion for policy group membership. When you define multiple criteria, the client request must meet all criteria to match the policy group. However, the client request needs to match only one of the configured Identities.

For more information about how the Web Proxy matches a client request with a policy group, see Evaluating Access Policy Group Membership, page 8-4 and Matching Client Requests to Access Policy Groups, page 8-5.


To create an Access Policy group:

Step 1 Navigate to the Web Security Manager > Access Policies page.

Step 2 Click Add Policy.

Step 3 In the Policy Name field, enter a name for the policy group, and in the Description field, optionally add a description.

Note Each policy group name must be unique and only contain alphanumeric characters or the space character.

Step 4 In the Insert Above Policy field, choose where in the policies table to place the policy group.

When configuring multiple policy groups you must specify a logical order for each group. Carefully order your policy groups to ensure that correct matching occurs.

Step 5 In the Identities and Users section, choose one or more Identity groups to apply to this policy group.

For more information on how to do this, see Configuring Identities in Other Policy Groups, page 7-28.

Step 6 Optionally, expand the Advanced section to define additional membership requirements.
Step 7  To define policy group membership by any of the advanced options, click the link for the advanced option and configure the option on the page that appears.
Table 8-1 describes the advanced options you can configure for Access Policy groups.

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Protocols**   | Choose whether or not to define policy group membership by the protocol used in the client request. Select the protocols to include.  
“All others” means any protocol not listed above this option.  
**Note:** When the HTTPS Proxy is enabled, only Decryption Policies apply to HTTPS transactions. You cannot define policy membership by the HTTPS protocol for Access, Routing, Outbound Malware Scanning, Data Security, or External DLP Policies. |
| **Proxy Ports** | Choose whether or not to define policy group membership by the proxy port used to access the Web Proxy. Enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas.  
For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. You might want to define policy group membership on the proxy port if you have one set of clients configured to explicitly forward requests on one port, and another set of clients configured to explicitly forward requests on a different port.  
Cisco recommends only defining policy group membership by the proxy port when the appliance is deployed in explicit forward mode, or when clients explicitly forward requests to the appliance. If you define policy group membership by the proxy port when client requests are transparently redirected to the appliance, some requests might be denied.  
**Note:** If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level. |
Creating Access Policies

Table 8-1  Access Policy Group Advanced Options (continued)

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnets</td>
<td>Choose whether or not to define policy group membership by subnet or other addresses. You can choose to use the addresses that may be defined with the associated Identity, or you can enter specific addresses here. <strong>Note:</strong> If the Identity associated with this policy group defines its membership by addresses, then in this policy group you must enter addresses that are a subset of the Identity’s addresses. Adding addresses in the policy group further narrows down the list of transactions that match this policy group.</td>
</tr>
<tr>
<td>Time Range</td>
<td>Choose whether or not to define policy group membership by a defined time range. Choose the time range from the Time Range field and then choose whether this policy group should apply to the times inside or outside the selected time range. For more information on creating time based policies, see Working with Time Based Policies, page 6-13. For more information on creating time ranges, see Creating Time Ranges, page 6-14.</td>
</tr>
<tr>
<td>URL Categories</td>
<td>Choose whether or not to define policy group membership by URL categories. Select the user defined or predefined URL categories. <strong>Note:</strong> If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</td>
</tr>
</tbody>
</table>
Step 8 Submit your changes.

Step 9 Configure Access Policy group control settings to define how the Web Proxy handles transactions.

The new Access Policy group automatically inherits global policy group settings until you configure options for each control setting. For more information, see Controlling HTTP and Native FTP Traffic, page 8-11.

Step 10 Submit and commit your changes.

## Controlling HTTP and Native FTP Traffic

After the Web Proxy assigns an HTTP, native FTP, or decrypted HTTPS request to an Access Policy group, the request inherits the control settings of that policy group. The control settings of the Access Policy group determine whether the appliance allows, blocks, or redirects the connection.

Figure 8-2 shows where you can configure control settings for the Access Policy groups.

You can configure the following settings to determine what action to take on the request:

- **Protocols and User Agents.** For more information, see Protocols and User Agents, page 8-14.
- **URL Categories.** For more information, see URL Categories, page 8-15.
- **Applications.** For more information, see Applications, page 8-15.
- **Objects.** For more information, see Object Blocking, page 8-16.
- **Web Reputation and Anti-Malware Filtering.** For more information, see Web Reputation and Anti-Malware, page 8-17.

After an Access Policy group is assigned to a request, the control settings for the policy group are evaluated to determine whether to allow, block, or redirect the request. For more information about assigning an Access Policy group to a request, see Policy Group Membership, page 6-10.

Figure 8-3 on page 13 shows how the Web Proxy determines which action to take on a request after it has assigned a particular Access Policy to the request.
Figure 8-3 Applying Access Policy Actions

1. Receive request from client.
2. Is the request on a blocked HTTP CONNECT port?
   - Yes, continue to monitor.
   - No, action is Block.
3. Is the request coming from a blocked custom user agent?
   - Yes, continue to monitor.
   - No, action is Block.
4. Is the request coming from a blocked suspect user agent?
   - Yes, continue to monitor.
   - No, action is Block.
5. Is the request using a blocked protocol?
   - Yes, action is Block.
   - No, action is Monitor.
6. Is the URL category of the request URL in the Access Policy group's list of custom URL categories?
   - Yes, action is Block.
   - No, action is Monitor.
7. Did the user accept the warning?
   - Yes, action is Block.
   - No, action is Monitor.
8. What is the configured action for uncategorized URLs?
   - Action is Monitor.
   - Is Safe Search enabled and configured to block unapproved engines, and is the transaction an unsafe request to an unapproved engine?
     - Yes, action is Block.
     - No, continue to monitor.
   - Is Site Content Filtering enabled?
     - Yes, action is Block.
     - No, continue to monitor.
9. Does the reputation score of the destination server indicate to block or scan the connection?
   - Yes, action is Scan.
   - No, continue to monitor.
10. Does the malware scanning verdict based on the URL request indicate to block the connection request?
    - Yes, action is Block.
    - No, continue to monitor.
11. Is the request to an application configured to be blocked?
    - Yes, continue to monitor.
    - Fetch the response from the server or cache.
12. Is the request on a blocked HTTP CONNECT port?
    - Yes, continue to monitor.
    - No, action is Block.
13. Is the response size larger than the maximum allowed?
    - Yes, continue to monitor.
    - Did the response match an application that is configured to be blocked?
      - Yes, action is Block.
      - No, continue to monitor.
14. Does the reputation score of the destination server indicate to allow the connection?
    - Yes, action is Block.
    - No, continue to monitor.
15. Does the malware scanning verdict based on the response indicate to block the response?
    - Yes, action is Block.
    - No, continue to monitor.
Chapter 8      Access Policies

Controlling HTTP and Native FTP Traffic

Figure 8-3 on page 13 shows two different decision points that involve the web reputation score of the destination server. The web reputation score of the server is evaluated only once, but the result is applied at two different points in the decision flow.

Protocols and User Agents

You can use the Protocols and User Agents settings on the Access Policies > Protocols and User Agents page to control policy group access to protocols and configure blocking for particular client applications (also known as user agents), such as instant messaging clients, web browsers, and Internet phone services. You can also configure the appliance to tunnel HTTP CONNECT requests on specific ports. With tunneling enabled, the appliance passes HTTP traffic through specified ports without evaluating it.

For more information about blocking user agents, see Blocking Specific Applications and Protocols, page 8-18.

Figure 8-4    Settings for Controlling Protocols and User Agents

Access Policies: Protocols and User Agents: exampleaccesspolicy

<table>
<thead>
<tr>
<th>Protocol Controls</th>
<th>Block Protocols:</th>
<th>HTTP CONNECT Ports:</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP over HTTP</td>
<td>100, 21, 443, 563, 9443, 1000</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Native FTP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

HTTP CONNECT enables applications to tunnel outbound traffic over HTTP, unless the protocol is blocked above. Enter 2-405555 to allow all ports via HTTP CONNECT; Leave field blank to block all ports.

Custom User Agents

<table>
<thead>
<tr>
<th>Block Custom User Agents:</th>
<th>Example User Agent Patterns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example user agent pattern</td>
<td>(Enter any regular expression, one regular expression per line, to block user agent)</td>
</tr>
</tbody>
</table>
Controlling HTTP and Native FTP Traffic

URL Categories

AsyncOS for Web allows you to configure how the appliance handles a transaction based on the URL category of a particular HTTP or HTTPS request. Using a predefined category list, you can choose to monitor or block content by category. You can also create custom URL categories and choose to allow, monitor, block, warn, or redirect traffic for a website in the custom category. You can use custom URL categories to create block and allow lists based on destination.

For information about enabling a URL filtering engine, see Configuring the URL Filtering Engine, page 16-5. For information on configuring URL categories in Access Policies, see Configuring URL Filters for Access Policy Groups, page 16-7.

You can also use the Access Policies > URL Categories page to filter adult content by enforcing safe searches and site content ratings. For more information, see Filtering Adult Content, page 16-20.

Applications

You can use the Access Policies > Applications Visibility and Control page to configure the Web Proxy block or allow applications by application type or a particular application. You can also apply controls to particular application behaviors within a particular application, such as file transfers.

Cisco IronPort Web Usage Controls includes the Application Visibility and Control engine (AVC engine) which allows you to apply deeper controls to particular application types. The AVC engine is an acceptable use policy component that inspects web traffic to gain deeper understanding and control of web traffic used for applications.
For more information on enabling the AVC engine, see Enabling the AVC Engine, page 17-3. For more information on configuring application settings in Access Policies, see Understanding Application Control Settings, page 17-4.

Object Blocking

You can use the settings on the Access Policies > Objects page to configure the Web Proxy to block file downloads based on file characteristics, such as file size and file type. For more information about blocking a specific object or MIME-type, see Blocking Specific Applications and Protocols, page 8-18.

Note

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 be sure 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.
Figure 8-5  Blocking Object Types

Access Policies: Objects: exampleaccesspolicy

<table>
<thead>
<tr>
<th>Edit Objects Blocking Settings</th>
<th>Define Custom Objects Blocking Settings:</th>
</tr>
</thead>
</table>

Object Blocking Settings

Object Size

HTTP/HTTPS Max. Download Size:
- C (in MB)
- M (Mbyte)
- No Maximum

FTP Max. Download Size:
- C (in MB)
- M (Mbyte)
- No Maximum

Block Object Type

- Archives
- Document Types
- Executable Code
- Installers
- Media
- P2P Metadatas
- Web Page Content
- Miscellaneous

Custom MIME Types

Block: Custom MIME Types:

(Enter multiple entries on separate lines. Example: audio/mpeg3 or audio/* are valid entries.)

Web Reputation and Anti-Malware

The Web Reputation and Anti-Malware Filtering policy inherits global settings respective to each component. To customize filtering and scanning for a particular policy group, you can use the Web Reputation and Anti-Malware Settings pull-down menu to customize monitoring or blocking for malware categories based on malware scanning verdicts and to customize web reputation score thresholds.

For more information about configuring web reputation scores, see Configuring Web Reputation Scores, page 18-5.

For more information about configuring anti-malware settings, see Configuring Anti-Malware Scanning, page 19-10.
Blocking Specific Applications and Protocols

You can configure how the appliance manages some kinds of applications based on the port being used:

- **Port 80.** You can control how the Web Security appliance manages these applications using Access Policies, but only as they are accessed via HTTP tunneling on port 80.
- **Ports other than 80.** You can block these applications on other ports by using the L4 Traffic Monitor.

Use the Web Security Manager > Access Policies page to manage access and monitoring for these types of applications on a more granular (per policy) level. Use the L4 Traffic Monitor to manage access and monitoring on a more global basis.

### Blocking on Port 80

To block access to these types of applications where port 80 is used, you can use the Web Security Manager > Access Policies page. The Access Policies page provides several methods for blocking access. You can block access by clicking on any of the following columns for a particular policy group:

- Protocols and User Agents
- URL Categories
- Objects

You can block access to predefined URL categories such as Chat and Peer-to-Peer, or create your own custom URL categories. You can block specific applications based on their “agent patterns” or signatures.

You can apply some or all of these methods on various Access Policies by creating additional Access Policy groups. For details on how to create additional Access Policy groups, see Creating Access Policies, page 8-7.

### Policy: Protocols and User Agents

You can create a rule that blocks a particular user agent based on its pattern using Regular Expressions.
You block access to applications based on their agent pattern similarly for the different Access Policies:


Once you view the Access Policies: Protocols and User Agents: *Policy_Name* page, add user agent patterns (also called signatures) to the Block Custom User Agents section of the page.

**Figure 8-6  Entering Agent Patterns to Block**

You can click the Example User Agent Patterns link for a list of some example user agent patterns.

**Table 8-2** provides a list of common patterns.

<table>
<thead>
<tr>
<th>Application</th>
<th>Search in Setting</th>
<th>HTTP header</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOL Messenger</td>
<td>Request headers</td>
<td>User-Agent</td>
<td>Gecko/</td>
</tr>
<tr>
<td>BearShare</td>
<td>Response header</td>
<td>Server</td>
<td>Bearshare</td>
</tr>
<tr>
<td>BitTorrent</td>
<td>Request headers</td>
<td>User-Agent</td>
<td>BitTorrent</td>
</tr>
<tr>
<td>eDonkey</td>
<td>Request headers</td>
<td>User-Agent</td>
<td>e2dk</td>
</tr>
<tr>
<td>Gnutella</td>
<td>Request headers</td>
<td>User-Agent</td>
<td>Gnutella</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Gnuclient:</td>
</tr>
<tr>
<td>Kazaa</td>
<td>Request headers</td>
<td>P2P-Agent</td>
<td>Kazaa</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Kazaaclient:</td>
</tr>
</tbody>
</table>
This is not a comprehensive list, as signatures change occasionally, and new applications are developed. You can find additional signatures at various websites, including the following websites:

- http://www.user-agents.org/

Cisco IronPort does not maintain, verify, or support the user agent listings at any of these websites.

### Policy: URL Categories

You can specify categories of URLs to block, including the predefined “Web-based Chat” and “Peer File Transfer” categories. You can also add specific custom URL categories should you want to add a URL that is not already included in the predefined categories. You may then add the custom category to the list of blocked URLs.

For more information about using URL Categories, see URL Categories, page 8-15.
Policy: Objects

You can block some Peer-to-Peer files directly, via the Access Policies: Objects: Global Policy page.

On the Web Security Manager > Access Policies page, click on the value in the Objects column for the desired policy.

In the Block Object Type section, check any boxes in the P2P Metafiles group. You can add custom MIME (Multipurpose Internet Mail Extensions) types by entering them in the Custom MIME Types field. For example, entering the application/x-zip signature blocks ZIP archive files.

Blocking on Ports Other Than 80

If these applications are using ports other than 80, you may want to block access to a specific server or block of IP addresses to which the client must connect. To manage these applications on other ports, use the L4 Traffic Monitor. The L4 Traffic monitor allows you to restrict access on specific ports. However, the restriction is global, so it will apply to all traffic on that port.
Working with External Proxies

This chapter contains the following topics:

- Working with External Proxies Overview, page 9-1
- Routing Traffic to Upstream Proxies, page 9-2
- Adding External Proxy Information, page 9-3
- Evaluating Routing Policy Group Membership, page 9-5
- Creating Routing Policies, page 9-8

Working with External Proxies Overview

The Web Security appliance is a proxy-compatible device, and is easily deployed within an existing proxy environment. However, it is recommended that you place the appliance downstream from existing proxy servers, meaning closer to the clients.

You can configure the appliance to work with multiple existing, upstream proxies. Use the Network > Upstream Proxies page to define upstream proxies or to modify existing settings. You define groups of proxies, and you can configure the appliance to use load balancing and failover features when connecting to multiple proxies.

After defining proxy groups, you can create Routing Policies to determine whether the Web Proxy connects to the server identified by the client or to a member of one the proxy groups.
Routing Traffic to Upstream Proxies

When the Web Proxy does not deliver a response from the cache, it can direct client requests directly to the destination server or to an external proxy on the network. You use Routing Policies to create rules that indicate when and to where to direct transactions. A Routing Policy determines to where to pass the client request, either to another proxy (as defined by the proxy group) or to the destination server. It addresses the question, “from where to fetch content?” You might want to create Routing Policies if you have a highly distributed network.

Figure 9-1 shows Routing Policies on the Web Security Manager > Routing Policies page.

When you define multiple external proxies in a proxy group, the Web Proxy can use load balancing techniques to distribute requests to different proxies defined in the group. You can choose the following load balancing techniques:

- **None (failover).** The Web Proxy directs transactions to one external proxy in the group. It tries to connect to the proxies in the order they are listed. If one proxy cannot be reached, the Web Proxy attempts to connect to the next one in the list.

- **Fewest connections.** The Web Proxy keeps track of how many active requests are with the different proxies in the group and it directs a transaction to the proxy currently servicing the fewest number of connections.
Chapter 9    Working with External Proxies

Adding External Proxy Information

- **Hash based.** The Web Proxy uses a hash function to distribute requests to the proxies in the group. The hash function uses the proxy ID and URL as inputs so that requests for the same URL are always directed to the same external proxy.

- **Least recently used.** The Web Proxy directs a transaction to the proxy that least recently received a transaction if all proxies are currently active. This setting is similar to round robin except the Web Proxy also takes into account transactions a proxy has received by being a member in a different proxy group. That is, if a proxy is listed in multiple proxy groups, the “least recently used” option is less likely to overburden that proxy.

- **Round robin.** The Web Proxy cycles transactions equally among all proxies in the group in the listed order.

For information about creating Routing Policies, see Creating Routing Policies, page 9-8.

---

**Note**

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.

---

### Adding External Proxy Information

To define external proxy information, you create a proxy group. A proxy group is an object that defines a list of proxies and their connection information and the load balancing technique to use when distributing requests to proxies in the group. You can create multiple proxy groups and can define multiple proxies within a group.

AsyncOS for Web allows you to enter the same proxy server information multiple times into the same proxy group. You might want to include the same proxy server multiple times to allow unequal load distribution among the proxies in the proxy group.
Adding External Proxy Information

### Note
You can only specify one existing proxy during the System Setup Wizard. AsyncOS creates a proxy group with one proxy using the information you enter in the System Setup Wizard. You can specify additional proxies in the web interface after initial setup.

To create a proxy group:

#### Step 1
Navigate to Network > Upstream Proxies, and click **Add Group**.

The Add Upstream Proxy Group page appears.

#### Add Upstream Proxy Group

<table>
<thead>
<tr>
<th>Proxy Group</th>
<th>Name:</th>
<th>Proxy Address</th>
<th>Port</th>
<th>Reconnection Attempts</th>
<th>Add Row</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Servers</td>
<td></td>
<td>hostname or IP address</td>
<td></td>
<td>Any number greater than 0</td>
<td></td>
</tr>
<tr>
<td>Load Balancing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure Handling</td>
<td></td>
<td>Specify how to handle requests if all proxies in this group fail.</td>
<td></td>
<td>Connect directly to destination host</td>
<td>Drop requests</td>
</tr>
</tbody>
</table>

#### Step 2
Enter a name for the proxy group in the Name field.

#### Step 3
In the Proxy Servers section, define at least one external proxy.

a. In the Proxy Address field, enter the hostname or IP address of the proxy server.

b. In the Port field, enter the port number used to access the proxy.

c. In the Reconnection Attempts field, enter the number of times the Web Proxy should try to connect to the proxy server before ignoring it.

d. Optionally, you can define another proxy server by clicking Add Row.

#### Step 4
In the Load Balancing field, choose the method the Web Proxy should use to distribute transactions to the proxies when the group contains multiple proxies.

For more information about the load balancing options, see **Routing Traffic to Upstream Proxies**, page 9-2.

#### Step 5
In the Failure Handling field, choose how the Web Proxy should handle transactions when all proxies in the group fail.
Evaluating Routing Policy Group Membership

After the Web Proxy assigns an Identity to a client request, it evaluates the request against the other policy types to determine which policy group it belongs for each type. Any request that does not get terminated due to failed authentication gets evaluated against the Routing Policies to determine from where to fetch the data.

Once the Web Proxy assigns a Routing Policy group to a request, it fetches the content from the location configured for the policy group, either from a configured proxy group or directly from the server.

To determine the policy group that a client request matches, the Web Proxy follows a specific process for matching the group membership criteria. During this process, it considers the following factors for group membership:

- **Identity.** Each client request either matches an Identity, fails authentication and is granted guest access, or fails authentication and gets terminated. For more information about evaluating Identity group membership, see Evaluating Identity Group Membership, page 7-2.

- **Authorized users.** If the assigned Identity requires authentication, the user must be in the list of authorized users in the Routing Policy group to match the policy group.

- **Advanced options.** You can configure several advanced options for Routing Policy group membership. Some options (such as proxy port and URL category) can also be defined within the Identity. When an advanced option is configured in the Identity, it is not configurable in the Routing Policy group level.

The information in this section gives an overview of how the appliance matches client requests to Routing Policy groups. For more details about exactly how the appliance matches client requests, see Matching Client Requests to Routing Policy Groups, page 9-6.

The Web Proxy sequentially reads through each policy group in the policies table. It compares the client request status to the membership criteria of the first policy group. If they match, the Web Proxy applies the policy settings of that policy group.
If they do not match, the Web Proxy compares the client request to the next policy group. It continues this process until it matches the client request to a user defined policy group. If it does not match a user defined policy group, it matches the global policy group. When the Web Proxy matches the client request to a policy group or the global policy group, it applies the policy settings of that policy group.

**Matching Client Requests to Routing Policy Groups**

Figure 9-2 on page 7 shows how the Web Proxy evaluates a client request against the Routing Policy groups.
Figure 9-2   Policy Group Flow Diagram for Routing Policies

1. Receive request from client.
2. Compare the client request against the next (or first) identity group in the policies table.
3. Is the current policy group the global policy?
   - No
   - Is the transaction assigned to one of the policy group's configured identities, or does the policy group use "All Identities"?
     - Yes
     - Is the current time in the policy group's configured time range in the Advanced section?
       - Yes, or no time range defined
       - Is the client subnet in the policy group's list of subnet(s) in the Advanced section?
         - Yes, or none defined
         - Is the proxy port in the policy group's list of ports in the Advanced section?
           - Yes, or none defined
           - Is the protocol in the policy group's list of protocol(s) in the Advanced section?
             - Yes, or none defined
             - Is the user agent in the policy group's list of user agents in the Advanced section?
               - Yes, or none defined
               - Is the URL category of the request URL in the policy group's list of URL categories in the Advanced section?
                 - Yes, or none defined
                 - Is the user one of the authorized users listed in the policy group?
                   - List of authorized users can be a list of user names, user groups, all authenticated users, guest users, or All Users. If the policy group only uses identities with no authentication, then all clients are authorized.
                   - Yes
                   - Fetch the content from the location specified in the policy group settings.
Creating Routing Policies

You can create Routing Policy groups based on combinations of several criteria, such as Identity or the port used to access the Web Proxy. You must define at least one criterion for policy group membership. When you define multiple criteria, the client request must meet all criteria to match the policy group.

For more information about how the appliance matches a client request with a policy group, see Evaluating Routing Policy Group Membership, page 9-5 and Matching Client Requests to Routing Policy Groups, page 9-6.


To create a Routing Policy group:

Step 1 Navigate to the Web Security Manager > Routing Policies page.

Step 2 Click Add Group.

Step 3 In the Policy Name field, enter a name for the policy group, and in the Description field, optionally add a description.

Note Each policy group name must be unique and only contain alphanumeric characters or the space character.

Step 4 In the Insert Above Policy field, choose where in the policies table to place the policy group.

When configuring multiple policy groups you must specify a logical order for each group. Carefully order your policy groups to ensure that correct matching occurs.

Step 5 In the Identities and Users section, choose one or more Identity groups to apply to this policy group.

For more information on how to do this, see Configuring Identities in Other Policy Groups, page 7-28.

Step 6 Optionally, expand the Advanced section to define additional membership requirements.
Step 7 To define policy group membership by any of the advanced options, click the link for the advanced option and configure the option on the page that appears.
Table 9-1 describes the advanced options you can configure for policy groups.

**Table 9-1 Policy Group Advanced Options**

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Protocols       | Choose whether or not to define policy group membership by the protocol used in the client request. Select the protocols to include.  

“All others” means any protocol not listed above this option.  

**Note:** When the HTTPS Proxy is enabled, only Decryption Policies apply to HTTPS transactions. You cannot define policy membership by the HTTPS protocol for Access, Routing, Outbound Malware Scanning, Data Security, or External DLP Policies.

| Proxy Ports     | Choose whether or not to define policy group membership by the proxy port used to access the Web Proxy. Enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas.  

For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. You might want to define policy group membership on the proxy port if you have one set of clients configured to explicitly forward requests on one port, and another set of clients configured to explicitly forward requests on a different port.  

Cisco recommends only defining policy group membership by the proxy port when the appliance is deployed in explicit forward mode, or when clients explicitly forward requests to the appliance. If you define policy group membership by the proxy port when client requests are transparently redirected to the appliance, some requests might be denied.  

**Note:** If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.
Creating Routing Policies

Table 9-1  Policy Group Advanced Options (continued)

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Subnets         | Choose whether or not to define policy group membership by subnet or other addresses. You can choose to use the addresses that may be defined with the associated Identity, or you can enter specific addresses here.  
Note: If the Identity associated with this policy group defines its membership by addresses, then in this policy group you must enter addresses that are a subset of the Identity’s addresses. Adding addresses in the policy group further narrows down the list of transactions that match this policy group. |
| Time Range      | Choose whether or not to define policy group membership by a defined time range. Choose the time range from the Time Range field and then choose whether this policy group should apply to the times inside or outside the selected time range.  
For more information on creating time based policies, see Working with Time Based Policies, page 6-13.  
For more information on creating time ranges, see Creating Time Ranges, page 6-14. |
| URL Categories  | Choose whether or not to define policy group membership by URL categories. Select the user defined or predefined URL categories.  
Note: If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level. |
Creating Routing Policies

9-12

Cisco IronPort AsyncOS 7.1 for Web User Guide

OL-23207-01

Chapter 9  Working with External Proxies

Table 9-1  Policy Group Advanced Options (continued)

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Agents</td>
<td>Choose whether or not to define policy group membership by the user agent used in the client request. You can select some commonly defined browsers, or define your own using regular expressions. Choose whether this policy group should apply to the selected user agents or to any user agent that is not in the list of selected user agents. For more information on creating user agent based policies, see Working with User Agent Based Policies, page 6-16. <strong>Note:</strong> If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</td>
</tr>
<tr>
<td>User Location</td>
<td>Choose whether or not to define policy group membership by user location, either remote or local. This option only appears when the Secure Mobility Solution is enabled. For more information, see Achieving Secure Mobility Overview, page 13-1.</td>
</tr>
</tbody>
</table>

Step 8  Submit your changes.

Step 9  Configure Routing Policy group control settings to define how the Web Proxy handles transactions.

The new policy group automatically inherits global policy group settings until you configure options for each control setting. For more information, see Routing Traffic to Upstream Proxies, page 9-2.

Step 10  Submit and commit your changes.
CHAPTER 10

Decryption Policies

This chapter contains the following information:

- Decryption Policies Overview, page 10-1
- Digital Cryptography Terms, page 10-6
- HTTPS Basics, page 10-8
- Digital Certificates, page 10-9
- Decrypting HTTPS Traffic, page 10-13
- Enabling the HTTPS Proxy, page 10-21
- Evaluating Decryption Policy Group Membership, page 10-27
- Creating Decryption Policies, page 10-30
- Controlling HTTPS Traffic, page 10-34
- Importing a Trusted Root Certificate, page 10-37

Decryption Policies Overview

HTTPS is a web protocol that acts as a secure form of HTTP. HTTPS encrypts HTTP requests and responses before they are sent across the network. Common thinking is that any connection to a site using HTTPS is “safe.” HTTPS connections are secure, not safe, and they do not discriminate against malicious or compromised servers. HTTPS is a secure way to complete legitimate transactions, but more dangerously, it is a secure way to download malware which can infect your network.
Not being able to inspect HTTPS traffic makes the network vulnerable to the following risks:

- **Secure site hosting malware.** Spammers and phishers can create legitimate looking websites that are only reachable through an HTTPS connection. Some users may mistakenly trust the web server because it requires an HTTPS connection, resulting in intentional and unintentional downloaded malware.

- **Malware from HTTPS web applications.** Some malware can infect the network from legitimate web applications, such as secure email clients, by downloading attachments.

- **Secure anonymizing proxy.** Some web servers offer a proxy service over an HTTPS connection that allows users to circumvent acceptable use policies. When users on the network use a secure proxy server outside the network, they can access any website, regardless of its web reputation or malware content.

The appliance uses both a URL filtering engine and IronPort Web Reputation Filters to make intelligent decisions about when to decrypt HTTPS connections. With this combination, administrators and end users are not forced to make a trade-off between privacy and security.

You can define HTTPS policies that determine if an HTTPS connection can proceed without examination or whether the appliance should act as an intermediary, decrypting the data passing each way and applying Access Policies to the data as if it were a plaintext HTTP transaction.

To configure the appliance to handle HTTPS requests, you must perform the following tasks:

1. **Enable the HTTPS Proxy.** To monitor and decrypt HTTPS traffic, you must first enable the HTTPS Proxy. For more information, see Enabling the HTTPS Proxy, page 10-21.

2. **Create and configure Decryption Policy groups.** Once the HTTPS Proxy is enabled, you can create and configure Decryption Policy groups to determine how to handle each request from each user. For more information, see Decryption Policy Groups, page 10-3.

3. **Import custom root certificates (optional).** Optionally, you can import one or more custom root certificates so the Web Proxy can recognize additional trusted root certificate authorities used by HTTPS servers. For more information, see Importing a Trusted Root Certificate, page 10-37.
Decryption Policies Overview

This book uses many terms from digital cryptography. This book also includes sections with background information about HTTPS and digital cryptography for reference only. For a list of the terms and definitions used in this book, see Digital Cryptography Terms, page 10-6. For an overview of HTTPS the protocol, see HTTPS Basics, page 10-8.

Note

Sections in this chapter that refer to a “certificate and key” imply a certificate and private key.

Decryption Policy Groups

Decryption Policies define how the appliance should handle HTTPS connection requests for users on the network. You can apply different actions to specified groups of users. You can also specify which ports the appliance should monitor for HTTPS transactions.

When a client makes an HTTPS request on a monitored secure port, the appliance compares the request to the Decryption Policy groups to determine in which Decryption Policy group the request belongs. Once it assigns the request to a Decryption Policy group, it can determine what to do with the connection request. For more information about evaluating policy group membership, see Policy Group Membership, page 6-10.

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

- **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. You might want to drop connections to third party proxies that allow users on the network bypass the organization’s acceptable use policies.

- **Pass through.** The appliance passes through the connection between the client and the server without inspecting the traffic content. You might want to pass through connections to trusted secure sites, such as well known banking and financial institutions.

- **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. You might want to decrypt connections to third party email
providers, such as gmail or hotmail. For more information about how the appliance decrypts HTTPS traffic, see Decrypting HTTPS Traffic, page 10-13.

**Note**
The actions above are final actions the Web Proxy takes on an HTTPS request. The “Monitor” action you can configure for Decryption Policies is not a final action. For more information, see Understanding the Monitor Action, page 10-5.

Once the appliance assigns a Decryption Policy to an HTTPS connection request, it evaluates the request against the policy group's configured control settings to determine which action to take. You can configure URL filter and web reputation settings to determine how to handle HTTPS requests for a particular policy group. For more information about how the appliance uses Decryption Policy groups to control HTTPS traffic, see Controlling HTTPS Traffic, page 10-34.

**Note**
Cisco recommends creating 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. For more information about Access Policy groups, see Access Policies, page 8-1.

For information about creating and using policy groups, see Working with Policies, page 6-1.

**Note**
The next two sections contain information about digital cryptography and HTTPS for reference only.

### Personally Identifiable Information Disclosure

If you choose to decrypt an end-user’s HTTPS session, then the Web Security appliance access logs and reports may contain personally identifiable information. Cisco recommends that Web Security appliance administrators take care when handling this sensitive information.
You also have the option to 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.

**Understanding the Monitor Action**

When the Web Proxy evaluates the control settings against a transaction, it evaluates the settings in a particular order. Each control setting can be configured to one of the following actions for Decryption Policies:

- Monitor
- Drop
- Pass through
- Decrypt

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.

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.

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.

Figure 10-9 on page 36 shows the order the Web Proxy uses when evaluating control settings for Decryption Policies. Looking at the flow diagram, you can see that the only actions applied to a transaction are the final actions listed above: Drop, Pass Through, and Decrypt.

**Note**

Figure 8-3 on page 13 shows the order the Web Proxy uses when evaluating control settings for Access Policies.
Digital Cryptography Terms

To understand how encryption and decryption works, you need to understand a little bit about cryptographic encoding techniques. Figure 10-1 describes some terms used in cryptography that are discussed in this chapter.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate authority</td>
<td>An entity which issues digital certificates for use by other parties. Certificate authorities are sometimes referred to as trusted third parties. Certificate authorities are typically commercial companies that charge for their services. However, some institutions and governments have their own certificate authorities, and some offer their services for free.</td>
</tr>
<tr>
<td>Cipher</td>
<td>An algorithm used for encoding and decoding text to make it unreadable to any system without the appropriate key. Ciphers work with keys to encode or decode text.</td>
</tr>
<tr>
<td>Ciphertext</td>
<td>Encoded text after a cipher has been applied to it.</td>
</tr>
<tr>
<td>Digital certificate</td>
<td>An electronic document that identifies and describes an organization that has been verified and signed by a trusted organization called a certificate authority. A digital certificate is similar in concept to an “identification card.” SSL uses certificates to authenticate servers. For more information about digital certificates, see Digital Certificates, page 10-9.</td>
</tr>
<tr>
<td>Digital signature</td>
<td>A checksum that verifies that a message was created by the stated author and was not altered since its creation.</td>
</tr>
<tr>
<td>Key</td>
<td>A numeric parameter used by a cipher to encode or decode text.</td>
</tr>
</tbody>
</table>
### Digital Cryptography Terms

**Plaintext or cleartext**

Message text in its original form, before it gets encoded by a cipher.

**Public key cryptography**

A system that uses two different keys for encoding and decoding text where one key is publicly known and available and the other key is private.

With public key cryptography, anyone can send an encoded message to a server that has publicized its public key, but only the recipient server can decode the message with its private key.

This is also known as asymmetric key cryptography.

**Public key infrastructure (PKI)**

An arrangement that binds public keys with respective user identities by means of a certificate authority.

X.509 is a standard that is an example PKI. X.509 specifies standards for public key certificates and an algorithm for validating certification paths.

**Private key cryptography**

A system that uses the same key for encoding and decoding text.

Because both sides of the transaction need the same key, they need a secure way to communicate which key to use in a particular communication session. Usually, they set up secure communication using public key cryptography and then generate a temporary symmetric key to use for the rest of the session.

This is also known as symmetric key cryptography.

**Root certificate**

A certificate that is the topmost certificate in a certificate tree structure.

All certificates below the root certificate inherit the trustworthiness of the root certificate.

Root certificates can be unsigned public key certificates or self-signed certificates.

**Self-signed certificate**

A digital certificate where the certificate authority is the same as the certificate creator.

---

**Table 10-1  Cryptography Terms and Definitions (continued)**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plaintext or cleartext</td>
<td>Message text in its original form, before it gets encoded by a cipher.</td>
</tr>
<tr>
<td>Public key cryptography</td>
<td>A system that uses two different keys for encoding and decoding text where one key is publicly known and available and the other key is private. With public key cryptography, anyone can send an encoded message to a server that has publicized its public key, but only the recipient server can decode the message with its private key. This is also known as asymmetric key cryptography.</td>
</tr>
<tr>
<td>Public key infrastructure (PKI)</td>
<td>An arrangement that binds public keys with respective user identities by means of a certificate authority. X.509 is a standard that is an example PKI. X.509 specifies standards for public key certificates and an algorithm for validating certification paths.</td>
</tr>
<tr>
<td>Private key cryptography</td>
<td>A system that uses the same key for encoding and decoding text. Because both sides of the transaction need the same key, they need a secure way to communicate which key to use in a particular communication session. Usually, they set up secure communication using public key cryptography and then generate a temporary symmetric key to use for the rest of the session. This is also known as symmetric key cryptography.</td>
</tr>
<tr>
<td>Root certificate</td>
<td>A certificate that is the topmost certificate in a certificate tree structure. All certificates below the root certificate inherit the trustworthiness of the root certificate. Root certificates can be unsigned public key certificates or self-signed certificates.</td>
</tr>
<tr>
<td>Self-signed certificate</td>
<td>A digital certificate where the certificate authority is the same as the certificate creator.</td>
</tr>
</tbody>
</table>
HTTPS Basics

HTTPS is a web protocol that acts as a secure form of HTTP. HTTPS is secure because the HTTP request and response data is encrypted before it is sent across the network. HTTPS works similarly to HTTP, except that the HTTP layer is sent on top of a security layer using either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). SSL and TLS are very similar, so this User Guide uses “SSL” to refer to both SSL and TLS, unless otherwise specified.

Figure 10-1 shows the different OSI network layers for HTTPS and HTTP. It shows that HTTPS is the HTTP protocol at the application layer over SSL or TLS at the security layer.

The URL typically determines whether the client application should use HTTP or HTTPS to contact a server:

- **http://servername**. The client application opens a connection to the server on port 80 by default and sends HTTP commands in plaintext.
- **https://servername**. The client application opens a connection to the server on port 443 by default and starts to engage in the SSL “handshake” to establish a secure connection between the client and server. Once the secure connection is established, the client application sends encrypted HTTP commands. For more information about the SSL handshake, see SSL Handshake, page 10-9.
Chapter 10  Decryption Policies

Digital Certificates

SSL Handshake

The SSL “handshake” is a set of steps a client and server engage in using the SSL protocol to establish a secure connection between them. The client and server must complete the following steps before they can send and receive encrypted HTTP messages:

Step 1  Exchange protocol version numbers. Both sides must verify they can communicate with compatible versions of SSL or TLS.

Step 2  Choose a cipher that each side knows. First, the client advertises which ciphers it supports and requests the server to send its certificate. Then, the server chooses the strongest cipher from the list and sends the client the chosen cipher and its digital certificate.

Step 3  Authenticate the identity of each side. Typically, only the server gets authenticated while the client remains unauthenticated. The client validates the server certificate. For more information about certificates and using them to authenticate servers, see Digital Certificates, page 10-9.

Step 4  Generate temporary symmetric keys to encrypt the channel for this session. The client generates a session key (usually a random number), encrypts it with the server’s public key, and sends it to the server. The server decrypts the session key with its private key. Both sides compute a common master secret key that will be used for all future encryption and decryption until the connection closes.

Digital Certificates

A digital certificate is an electronic document that identifies and describes an organization, and that has been verified and signed by a trusted organization. A digital certificate is similar in concept to an identification card, such as a driver’s license or a passport. The trusted organization that signs the certificate is also known as a certificate authority.

Certificates allow a client to know that it is talking to the organization it thinks it is talking to. When a server certificate is signed by a well-known or trusted authority, the client can better assess how much it trusts the server.

X.509 is a standard example of a public key infrastructure (PKI). X.509 specifies standards for certificates and an algorithm for validating certification paths. The Web Security appliance uses the X.509 standard.
X.509 certificates contain the following information:

- Subject’s identity, such as the name of a person, server, or organization
- Certificate validity period
- Certificate authority who is vouching for the certificate
- Digital signature of the certificate created by the certificate authority using its private key
- Public key of the subject

For an example digital certificate you can view from a web browser, see Working with Root Certificates, page 10-16.

Although anyone can create a digital certificate, not everyone can get a well-respected certificate authority to vouch for the certificate’s information and sign the certificate with its private key. For more information about validating the certificate authority in a digital certificate, see Validating Certificate Authorities, page 10-10.

**Validating Certificate Authorities**

The X.509 standard allows certificate authorities to issue digital certificates that are signed by other certificate authorities. Due to this system, there is a hierarchy of certificate authorities in a tree structure.

The top-most certificate authorities in the tree structure are called root certificates. Root certificates are not signed by a separate certificate authority because they are at the top of the tree structure. Therefore, by definition, all root certificates are self-signed certificates. The certificate authority listed in the root certificate is the certificate creator.

All certificates below the root certificate inherit the trustworthiness of the root certificate. For example, if CertificateAuthorityABC is a trusted certificate authority and it signs the certificate for certificate authority CertificateAuthorityXYZ, then CertificateAuthorityXYZ is automatically a trusted certificate authority.

Figure 10-2 shows the certification path for a certificate viewed in a web browser.
In Figure 10-2, the certificate for the URL investing.schwab.com was signed by certificate authority “VeriSign Class 3 Extended Validation SSL CA,” which in turn was signed by certificate authority VeriSign.

By definition, root certificates are always trusted by applications that follow the X.509 standard. The Web Security appliance uses the X.509 standard.

Standard web browsers ship with a set of trusted root certificates. The list of root certificates is updated regularly. You can view the root certificates installed on the web browser.

For example, to view the root certificates installed with Mozilla Firefox 2.0, go to Tools > Options > Advanced > Encryption > View Certificates. To view the root certificates installed with Internet Explorer 7, go to Tools > Internet Options > Content > Certificates > Trusted Root Certification Authorities.

In Figure 10-2, the VeriSign certificate is a root certificate that shipped with the web browser.
The Web Security appliance also installs with a set of trusted root certificates. However, you can upload additional root certificates that the Web Proxy deems to be trusted. For more information about this, see Importing a Trusted Root Certificate, page 10-37.

Validating Digital Certificates

Certificates can be valid or invalid. A certificate may be in invalid for different reasons. For example, the current time may be before or after the certificate validity period, the root authority in the certificate may not be recognized, or the Common Name of the certificate does not match the hostname specified in the HTTP “Host” header.

The Web Security appliance verifies that a server certificate is valid before it inspects and decrypts an HTTPS connection from a server. You can configure how the appliance handles connections to servers with invalid certificates. The appliance can perform one of the following actions for invalid server certificates:

- **Drop.** The appliance drops the connection and does not notify the client. This is the most restrictive option.
- **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. For more information about how the appliance decrypts HTTPS traffic, see Decrypting HTTPS Traffic, page 10-13.
- **Monitor.** The appliance does not drop the connection, and instead it continues comparing the server request with the Decryption Policy groups. This is the least restrictive option.

**Note** When an invalid server certificate is monitored, the errors in the certificate are maintained and passed along to the end-user.

For more information about configuring the appliance to handle invalid server certificates, see Enabling the HTTPS Proxy, page 10-21.
Decrypting HTTPS Traffic

The request and response data is encrypted for HTTPS connections before it is sent across the network. Because the data is encrypted, third parties can view the data, but cannot decrypt it to read its contents without the private key of the HTTPS server.

Figure 10-3 shows an HTTPS connection between a client and a HTTPS server.

The Web Security appliance does not have access to the server’s private key, so in order to inspect the traffic between the client and the server, it must intercept the connection and break the connection into two separate connections. The appliance acts as an intermediary between the client and the server pretending to be the server to the client, and the client to the server. This is sometimes referred to as being the “man in the middle.”

Figure 10-4 shows an HTTPS connection between a client and a HTTPS server that goes through the Web Security appliance.

Figure 10-3  HTTPS Connection

Figure 10-4  HTTPS Connection Decrypted by the Web Security Appliance
Notice that in Figure 10-4, there are two different HTTPS connections, one between the client and the appliance, and one between the appliance and the server. The appliance performs the SSL handshake twice, once with the client and again with the server:

- **SSL handshake with the server.** When the appliance performs the SSL handshake with the server, it acts as if it were the client sending a request to the server. After it establishes a secure connection with the server, it can begin receiving the encrypted data. Because it acts as the client and participates in the SSL handshake, it has agreed upon a temporary symmetric key with the server so it can decrypt and read the data the server sends. Also, the appliance receives the server’s digital certificate.

- **SSL handshake with the client.** When the appliance performs the SSL handshake with the client, it acts as if it were the requested server providing data the client requests. In order to perform the SSL handshake with the client, it must send the client its own digital certificate. However, the client expects the certificate of the requested server, so the appliance mimics the requested server’s certificate by specifying a root certificate authority uploaded or configured by an appliance administrator.

For more information about how the server mimics the server's certificate, see Mimicking the Server Digital Certificate, page 10-15.

---

**Note** Because the appliance signs the server certificate with a different root certificate authority and sends that to the client, you must verify the client applications on the network recognize the root certificate authority. For more information, see Working with Root Certificates, page 10-16.

---

After the two separate HTTPS connections are established, the following actions occur:

1. Encrypted data is received from the server.
2. The temporary, symmetric key negotiated with the server is used to decrypt the data.
3. Access Policies are applied to the decrypted traffic as if it were a plaintext HTTP connection. For more information about Access Policies, see Access Policies, page 8-1.
4. Assuming the Access Policy group allows the client to receive the data, the data is encrypted using the temporary, symmetric key negotiated with the client.

5. Encrypted data is sent to the client.

**Note**

No decrypted data is cached. However, access logs for decrypted HTTP transactions are saved to disk.

**Mimicking the Server Digital Certificate**

When the appliance performs the SSL handshake with the client, it mimics the server digital certificate and sends the new certificate to the client. To mimic the server digital certificate, it reuses most field values and changes some field values. The mimicked certificate is the same as the server certificate except for the following fields:

- **Issuer.** The issuer comes from the generated or uploaded root certificate configured in the appliance.

- **Signature Algorithm.** This field is always “sha1WithRSAEncryption” or “dsaWithSHA1” depending upon on whether the root certificate the appliance uses contains an RSA or DSA key.

- **Public Key.** The appliance replaces the public key in the original certificate with a public key it generates that matches bit strength from the original certificate and for which it has a matching private key generated as well. For example, if the server certificate uses a 2048 bit RSA key, the appliance generates a new 2048 bit RSA key.

- **X509v3 Extensions.** All X509v3 extensions are removed except for the following:
  - Basic Constraints
  - Subject Alternative Name
  - Key Usage
  - Subject Key Identifier
  - Extended Key Usage
For example, the appliance removes the Authority Key Identifier and the Authority Information Access X509v3 extensions.

**Working with Root Certificates**

The Web Security appliance mimics the HTTPS server to which a client originally sent a connection request. In order to establish a secure connection with the client pretending to be the requested server, the appliance must send a server certificate to the client signed by a root certificate authority configured in the appliance.

When you enable the HTTPS Proxy on the appliance, you can configure the root certificate information that the appliance uses to sign its server certificates. 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. You might want to generate a certificate and key when your organization does not have a certificate and key in use, or when it wants to create a new and unique certificate and key.

- **Upload.** You can upload a certificate file and its matching private key file created outside of the appliance. You might want to upload a certificate and key file if the clients on the network already have the root certificates on their machines.

  The certificate and key files you upload must be in PEM format. DER format is not supported. For more information about convert a DER formatted certificate or key to PEM format, see Converting Certificate and Key Formats, page 10-20.

  **Note**  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.

For more information about how to generate or upload a certificate and key, see Enabling the HTTPS Proxy, page 10-21.

However, 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.

You can also upload an intermediate certificate that has been signed by a root certificate authority. When the Web Proxy mimics the server certificate, it sends the uploaded certificate along with the mimicked certificate to the client application. That way, as long as the intermediate certificate is signed by a root certificate authority that the client application trusts, the application will trust the mimicked server certificate, too. You might want to upload an intermediate certificate if your organization uses its own root certificate authority, but does not want to upload the root certificate to the Web Security appliance for security reasons.

Figure 10-5 on page 17 shows an example error message when a user sends an HTTPS request through Netscape Navigator.

Figure 10-5  Unknown Certificate Authority Error Message
Typically, users can view the certificate and use the information in the certificate to choose whether or not to allow the secure connection with this website. In Figure 10-5, you can view the certificate contents by clicking Examine Certificate.

Figure 10-6 on page 18 shows an example root certificate issued by the appliance.

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. To verify you distribute the root certificate the appliance is
You can download the root certificate from the Security Services > HTTPS Proxy page. Click **Edit Settings**, and then click the Download Certificate link for either the generated or uploaded certificate.

You might want to download the root certificate from the appliance if a different person uploaded the root certificate to the appliance and you want to verify you distribute the same root certificate to the client machines.

### Using Decryption with the AVC Engine

Depending on how the HTTPS Proxy is configured and the configured Decryption Policies, the HTTPS Proxy may decrypt HTTPS connections to web applications. This allows the AVC engine to more accurately detect and block web applications that use HTTPS. These web applications may use web browsers or other client applications, such as instant messaging applications.

However, to ensure that all applications work properly when HTTPS connections are decrypted, you must add the root certificate for signing to all client machines on the network as a trusted root certificate authority. For example, on Windows machines, you must install the root certificate into Internet Explorer for many instant messaging client applications to work, such as Yahoo Instant Messenger, MSN Messenger, and Google Talk.

### Using Decryption with AOL Instant Messenger

Most AOL Instant Messenger (AIM) client applications do not allow you to add root certificates to their list of trusted certificates. Because you cannot add the appliance root certificate for signing to AIM client applications, AIM users are unable to log into AIM when the HTTPS connection to the AIM server is decrypted. Decryption to AIM servers might occur if the web reputation filters are configured to decrypt traffic to servers with the reputation score equal to the AIM server, or if a Decryption Policy is configured to decrypt all traffic.

To allow users to log into AIM, you must ensure that HTTPS traffic to the AIM servers are never decrypted and instead are passed through.

---

**Note**

Once users are logged into AIM, all instant messenger traffic uses HTTP and is subject to the configured Access Policies.

To pass through HTTPS traffic to AIM servers:
Step 1 Create a custom URL category in the first position of custom URL categories and enter the following addresses:

- aimpro.premiumservices.aol.com
- bos.oscar.aol.com
- kdc.uas.aol.com
- buddyart-d03c-sr1.blue.aol.com
- 205.188.8.207
- 205.188.248.133
- 205.188.13.36
- 64.12.29.131

Step 2 Create a Decryption Policy and use the custom URL category created in Step 1 as part of the policy group membership. Depending on the other Decryption Policies configured, you might want to place this Decryption Policy at the top of the list.

Step 3 Configure the Decryption Policy to pass through all traffic to the custom URL category.

Step 4 Choose pass through as the default action for the Decryption Policy.

Step 5 Submit and commit your changes.

Converting Certificate and Key Formats

The root certificate and private key files you upload to the appliance must be in PEM format. DER format is not supported. However, you can convert certificates and keys in DER format into the PEM format before uploading them. For example, you can use OpenSSL to convert the format.

Use the following OpenSSL command to convert a DER formatted certificate file to a PEM formatted certificate file:

```
openssl x509 -inform DER -in cert_in_DER -outform PEM -out out_file_name
```

You can also convert key files in DER format into the PEM format by running a similar OpenSSL command.

For RSA keys, use the following command:
Enabling the HTTPS Proxy

To monitor and decrypt HTTPS traffic, you must enable the HTTPS Proxy on the Security Services > HTTPS Proxy page. 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. You can no longer define Access and Routing Policy group membership by HTTPS, nor can you configure Access Policies to block HTTPS transactions. If some Access and Routing Policy group memberships are defined by HTTPS and if some Access Policies block HTTPS, then when you enable the HTTPS Proxy those Access and Routing Policy groups become disabled. You can choose to enable the policies at any time, but all HTTPS related configurations are removed.

Note

When you upload a certificate to the Web Security appliance, verify it is a signing certificate and not a server certificate. A server certificate cannot be used as a signing certificate, so decryption does not work when you upload a server certificate.

For more information about root certificates, see Working with Root Certificates, page 10-16.
Enabling the HTTPS Proxy

Also on this page, you can configure what the appliance does with HTTPS traffic when the server certificate is invalid.

Note

For information on importing a custom root authority certificate, see Importing a Trusted Root Certificate, page 10-37.

To enable the HTTPS Proxy:

Step 1

Navigate to the Security Services > HTTPS Proxy page, and 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.

The Edit HTTPS Proxy Settings page appears.

Edit HTTPS Proxy Settings

<table>
<thead>
<tr>
<th>HTTPS Proxy Settings</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ Enable HTTPS Proxy</td>
<td>☑ Transparent HTTPS Proxy</td>
<td>443</td>
</tr>
<tr>
<td>□ Applications that Use HTTPS</td>
<td>☑ Use Generated Certificate and Key</td>
<td>Generate New Certificate and Key</td>
</tr>
<tr>
<td>□ Root Certificate for Signing</td>
<td>☑ Use Uploaded Certificate and Key</td>
<td>Uploaded Certificate and Key</td>
</tr>
<tr>
<td>□ Invalid Certificate Handling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No certificate has been generated.

No certificate has been uploaded.

No end-user notification will be provided for dropped HTTPS connections. Use this setting with caution. If the connection is not dropped, an equivalent certificate will be generated.
Step 3 Verify the Enable HTTPS Proxy field is enabled.

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

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

Step 5 In the HTTPS Transparent Request section, choose how the Web Proxy handles transparently redirected HTTPS transactions it receives before an HTTP request that was authenticated using an identity with an IP-based surrogate. 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.

For more information, see Understanding How Authentication Affects HTTPS and FTP over HTTP Requests, page 7-6.

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

Step 6 In the Applications that Use HTTPS section, choose whether or not to enable decryption for enhanced application visibility and control.

Enabling this setting allows the Web Proxy to detect applications that use HTTPS with better accuracy. This setting supersedes the “Pass Through” decision made by the Web Reputation Filters as configured in the Decryption Policies. However, the URL category decision still applies.

Note Decryption may cause some applications to fail unless the root certificate for signing is installed on the client. For more information, see Using Decryption with the AVC Engine, page 10-19. For more information on the appliance root certificate, see Working with Root Certificates, page 10-16.
Step 7  Choose which root certificate to use for signing self-signed certificates the appliance sends to clients:

- **Generated certificate and key.** Go to step 8 on page 24.
- **Uploaded certificate and key.** Go to step 9 on page 25.

For more information about how the appliance uses these root certificates, see Working with Root Certificates, page 10-16.

**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 8  To generate a certificate and key:

a.  Click the Use Generated Certificate and Key option.

b.  Click **Generate New Certificate and Key**.

c.  In the Generate Certificate and Key dialog box, enter the information to display in the root certificate.

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

d.  Click **Generate**. The Web Security appliance generates the certificate with the data you entered and generates a key.

The generated certificate information is displayed on the Edit HTTPS Proxy Settings page.
Chapter 10  Decryption Policies

Enabling the HTTPS Proxy

Note After you generate the certificate and key, you can download the generated certificate to transfer it to the client applications on the network. Do this using the Download Certificate link in the generated key area.

e. Go to step 10 on page 26.

Step 9 To upload a root certificate and key:

a. Click Use Uploaded Certificate and Key.

b. 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.

Note The certificate file must be in PEM format. DER format is not supported.

c. Click Browse for the Key field to navigate to the private key file. The private key must be unencrypted.

Note The key length must be 512, 1024, or 2048 bits. Also, the private key file must be in PEM format. DER format is not supported.

d. 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.

Note After you upload the certificate and key, you can download the certificate to transfer it to the client applications on the network. Do this using the Download Certificate link in the uploaded key area.
Step 10  In the Invalid Certificate Handling section, choose how the appliance handle HTTPS traffic when it encounters invalid server certificates. You can drop, decrypt, or monitor HTTPS traffic for the following types of invalid server certificates:

- **Expired.** The certificate is either not yet valid, or it is currently past its valid to date.

- **Mismatched hostname.** The hostname in the certificate does not match the hostname the client was trying to access. This might happen during a “man in the middle attack,” or when a server redirects a request to a different URL. For example, http://mail.google.com gets redirected to http://www.gmail.com.

  **Note** — The Web Proxy can only perform hostname match when it is deployed in explicit forward mode. When it is deployed in transparent mode, it does not know the hostname of the destination server (it only knows the IP address), so it cannot compare it to the hostname in the server certificate.

- **Unrecognized root authority.** The root certificate authority for the certificate is not in the set of trusted root authorities on the appliance.

- **All other error types.** Most other error types are due to the appliance not being able to complete the SSL handshake with the HTTPS server. For more information about additional error scenarios for server certificates, see http://www.openssl.org/docs/apps/verify.html.

**Note**  When a certificate is both expired and has an unrecognized root authority, the Web Security appliance performs the action specified for an unrecognized root authority.

For more information about handling invalid server certificates, see Validating Digital Certificates, page 10-12.

Step 11  Submit and commit your changes.
Evaluating Decryption Policy Group Membership

After the Web Proxy assigns an Identity to a client request, it evaluates the request against the other policy types to determine which policy group it belongs for each type. When the HTTPS Proxy is enabled, it applies HTTPS requests against the Decryption Policies. When the HTTPS Proxy is not enabled, it evaluates HTTP requests against the Access Policies.

When an HTTPS request gets decrypted, the Web Proxy evaluates the decrypted request against the Access Policies. For more information about how the Web Proxy evaluates Access Policies, see Evaluating Access Policy Group Membership, page 8-4.

The Web Proxy applies the configured policy control settings to a client request based on the client request’s policy group membership.

To determine the policy group that a client request matches, the Web Proxy follows a specific process for matching the group membership criteria. During this process, it considers the following factors for group membership:

- **Identity.** Each client request either matches an Identity, fails authentication and is granted guest access, or fails authentication and gets terminated. For more information about evaluating Identity group membership, see Evaluating Identity Group Membership, page 7-2.

- **Authorized users.** If the assigned Identity requires authentication, the user must be in the list of authorized users in the Decryption Policy group to match the policy group.

- **Advanced options.** You can configure several advanced options for Decryption Policy group membership. Some of the options (such as proxy port, and URL category) can also be defined within the Identity. When an advanced option is configured in the Identity, it is not configurable in the Decryption Policy group level.

The information in this section gives an overview of how the appliance matches client requests to Decryption Policy groups. For more details about exactly how the appliance matches client requests, see Matching Client Requests to Decryption Policy Groups, page 10-28.

The Web Proxy sequentially reads through each policy group in the policies table. It compares the client request status to the membership criteria of the first policy group. If they match, the Web Proxy applies the policy settings of that policy group.
If they do not match, the Web Proxy compares the client request to the next policy group. It continues this process until it matches the client request to a user defined policy group. If it does not match a user defined policy group, it matches the global policy group. When the Web Proxy matches the client request to a policy group or the global policy group, it applies the policy settings of that policy group.

**Matching Client Requests to Decryption Policy Groups**

*Figure 10-7 on page 29* shows how the Web Proxy evaluates a client request against the Decryption Policy groups.
Figure 10-7  Policy Group Flow Diagram for Decryption Policies

Receive request from client.

- Compare the client request against the next (or first) identity group in the policies table.

- Is the current policy group the global policy?
  - Yes
  - No
    - Is the transaction assigned to one of the policy group’s configured identities, or does the policy group use “All Identities”?
      - Yes
      - No
        - Is the current time in the policy group’s configured time range in the Advanced section?
          - Yes, or no time range defined
          - No
            - Is the client subnet in the policy group’s list of subnet(s) in the Advanced section?
              - Yes, or none defined
              - No
                - Is the proxy port in the policy group’s list of ports in the Advanced section?
                  - Yes, or none defined
                  - No
                    - Is the user agent in the policy group’s list of user agents in the Advanced section?
                      - Yes, or none defined
                      - No
                        - Is the URL category of the request URL in the policy group’s list of URL categories in the Advanced section?
                          - Yes, or none defined
                          - No
                            - Is the user one of the authorized users listed in the policy group?
                              - List of authorized users can be a list of user names, user groups, all authenticated users, guest users, or All Users. If the policy group only uses identities with no authentication, then all clients are authorized.
                              - Yes
                              - No
                                - Apply the Decryption Policy group settings to the client request.
Creating Decryption Policies

You can create Decryption Policy groups based on combinations of several criteria, such as Identity or the URL category of the destination site. You must define at least one criterion for policy group membership. When you define multiple criteria, the client request must meet all criteria to match the policy group.

For more information about how the appliance matches a client request with a policy group, see Evaluating Decryption Policy Group Membership, page 10-27 and Matching Client Requests to Decryption Policy Groups, page 10-28.

You define policy group membership on the Web Security Manager > Decryption Policies page.

To create a Decryption Policy group:

Step 1  Navigate to the Web Security Manager > Decryption Policies page.

Step 2  Click Add Policy.

Step 3  In the Policy Name field, enter a name for the policy group, and in the Description field, optionally add a description.

Note  Each policy group name must be unique and only contain alphanumeric characters or the space character.

Step 4  In the Insert Above Policy field, choose where in the policies table to place the policy group.

When configuring multiple policy groups you must specify a logical order for each group. Carefully order your policy groups to ensure that correct matching occurs.

Step 5  In the Identities and Users section, choose one or more Identity groups to apply to this policy group.
Note
If the Identity requires authentication, then authentication information may not be available when a user tries to connect to an HTTPS server. For more information on how HTTPS and authentication work together, see Understanding How Authentication Affects HTTPS and FTP over HTTP Requests, page 7-6.

For more information on how to do this, see Configuring Identities in Other Policy Groups, page 7-28.

Step 6
Optionally, expand the Advanced section to define additional membership requirements.

Step 7
To define policy group membership by any of the advanced options, click the link for the advanced option and configure the option on the page that appears.
Table 10-2 describes the advanced options you can configure for Decryption Policy groups.

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Ports</td>
<td>Choose whether or not to define policy group membership by the proxy port used to access the Web Proxy. Enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas. For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. You might want to define policy group membership on the proxy port if you have one set of clients configured to explicitly forward requests on one port, and another set of clients configured to explicitly forward requests on a different port. Cisco recommends only defining policy group membership by the proxy port when the appliance is deployed in explicit forward mode, or when clients explicitly forward requests to the appliance. When you define policy group membership by the proxy port when clients requests get transparently redirected to the appliance, some requests might be denied. <strong>Note:</strong> If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Choose whether or not to define policy group membership by subnet or other addresses. You can choose to use the addresses that may be defined with the associated Identity, or you can enter specific addresses here. <strong>Note:</strong> If the Identity associated with this policy group defines its membership by addresses, then in this policy group you must enter addresses that are a subset of the Identity’s addresses. Adding addresses in the policy group further narrows down the list of transactions that match this policy group.</td>
</tr>
</tbody>
</table>
Chapter 10  Decryption Policies

Creating Decryption Policies

Table 10-2  Decryption Policy Group Advanced Options (continued)

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Time Range      | Choose whether or not to define policy group membership by a defined time range. Choose the time range from the Time Range field and then choose whether this policy group should apply to the times inside or outside the selected time range.  
For more information on creating time based policies, see Working with Time Based Policies, page 6-13.  
For more information on creating time ranges, see Creating Time Ranges, page 6-14. |
| URL Categories  | Choose whether or not to define policy group membership by URL categories. Select the user defined or predefined URL categories.  
**Note:** If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level. |
| User Agents     | Choose whether or not to define policy group membership by the user agent used in the client request. You can select some commonly defined browsers, or define your own using regular expressions. Choose whether this policy group should apply to the selected user agents or to any user agent that is not in the list of selected user agents.  
For more information on creating user agent based policies, see Working with User Agent Based Policies, page 6-16.  
**Note:** If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level. |
| User Location   | Choose whether or not to define policy group membership by user location, either remote or local.  
This option only appears when the Secure Mobility Solution is enabled. For more information, see Achieving Secure Mobility Overview, page 13-1. |

Step 8  Submit your changes.
Step 9  Configure Decryption Policy group control settings to define how the Web Proxy handles transactions.

The new policy group automatically inherits global policy group settings until you configure options for each control setting. For more information, see Controlling HTTPS Traffic, page 10-34.

Step 10  Submit and commit your changes.

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. For more information about the actions the appliance can take on an HTTPS request, see Decryption Policy Groups, page 10-3.


Figure 10-8 shows where you can configure control settings for the Decryption Policy groups.

Figure 10-8  Decryption Policies Table

You can configure the following settings to determine what action to take on the HTTPS connection:

- **URL categories.** You can configure the action to take on HTTPS requests for each predefined and custom URL category. Click the link under the URL Categories column for the policy group you want to configure. For more
information about working with URL filters, see URL Filters, page 16-1. For more information about configuring URL categories, see Configuring URL Filters for Decryption Policy Groups, page 16-10.

Note
If you want to block (with end-user notification) a particular URL category for HTTPS requests instead of drop (with no end-user notification), choose to decrypt that URL category in the Decryption Policy group and then choose to block the same URL category in the Access Policy group.

- **Web reputation.** You can configure the action to take on HTTPS requests based on the web reputation score of the requested server. Click the link under the Web Reputation column for the policy group you want to configure. For more information about working with web reputation scores, see Web Reputation in Decryption Policies, page 18-5.

- **Default action.** You can configure the action the appliance should take when none of the other settings apply. Click the link under the Default Action column for the policy group you want to configure.

Note
The configured default action only affects the transaction when no decision is made based on URL category or Web Reputation score. If Web Reputation filtering is disabled, the default action applies to all transactions that match a Monitor action in a URL category. If Web Reputation filtering is enabled, the default action is used only if the Monitor action is selected for sites with no score.

After a Decryption Policy group is assigned to an HTTPS request, the control settings for the policy group are evaluated to determine whether to drop, pass through, or decrypt the HTTPS connection request. For more information about assigning a Decryption Policy group to an HTTPS request, see Policy Group Membership, page 6-10.

Figure 10-9 on page 36 shows how the appliance determines which action to take on an HTTPS request after it has assigned a particular Decryption Policy to the request.
Figure 10-9 shows two different decision points that involve the web reputation score of the destination server. The web reputation score of the 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 defined for predefined URL categories.
Chapter 10      Decryption Policies

Importing a Trusted Root Certificate

When the Web Proxy receives a connection request for an HTTPS server, it validates the trustworthiness of the destination server by verifying the root certificate authority that signed the server certificate. If the Web Proxy does not recognize the root certificate that signed the server certificate, then it does not trust the server certificate. This happens when the HTTPS server uses a certificate authority that is not listed in the set of trusted certificate authorities that ship with the Web Security appliance. This might happen if your organization uses an internal certificate authority to sign certificates for servers on the internal network.

To prevent the Web Proxy from potentially blocking access to servers with unrecognized root certificate authorities, you can upload to the appliance root certificates that your organization trusts. For example, you might want to upload a root certificate used by the servers on your network.

You can upload multiple root certificate files to the appliance, and each file you upload can contain multiple root certificates. However, each certificate you upload must be a root certificate.

To import a trusted root certificate:

Step 1 Navigate to the Security Services > HTTPS Proxy page.

Step 2 In the Custom Root Authority Certificates section, click Import.
Step 3  In the Import Custom Root Authority Certificate File, click **Browse**.

Step 4  Navigate to the location where the custom root authority certificate file is located and click **Open**.

Step 5  Click **Submit**.

The uploaded root certificate is displayed in the “Custom Root Authority Certificates” section.

Step 6  Optionally, repeat steps 2 through 5 to upload additional trusted root certificates.

Step 7  Commit your changes.
Outbound Malware Scanning Overview

Malware is pervasive and persistent, and unfortunately, usually finds access to the computers inside your network. Users increasingly work with customers and partners to collaborate on projects and increase productivity. This increased collaboration poses challenges for information security professionals to determine how to prevent malware infections on internal systems from accidentally infecting key partners, and therefore adversely affecting their reputation.

The IronPort Web Security appliance provides the outbound malware scanning feature which allows you to stop malware that is already active on computers inside the network from escaping the network and affecting customers and partners.
The IronPort Dynamic Vectoring and Streaming (DVS) engine scans transaction requests as they leave the network in real time. By working with the IronPort DVS engine, the Web Security appliance enables you to prevent users from unintentionally uploading malicious data.

To prevent malicious data from leaving the network, the Web Security appliance provides the Outbound Malware Scanning policy groups. You define which uploads are scanned for malware, which anti-malware scanning engines to use for scanning, and which malware types to block.

For more information on anti-malware scanning, see Anti-Malware Services, page 19-1.

**User Experience with Blocked Requests**

When the IronPort DVS engine blocks an upload request, the Web Proxy sends a block page to the end user. However, not all websites display the block page to the end user. For example, some Web 2.0 websites display dynamic content using javascript instead of a static webpage and are not likely to display the block page. Users are still properly blocked from uploading malicious data, but they may not always be informed of this by the website.

**Outbound Malware Scanning Policy Groups**

Outbound Malware Scanning Policies define whether or not the Web Proxy blocks HTTP requests and decrypted HTTPS connections for transactions that upload data to a server (upload requests). An upload request is an HTTP or decrypted HTTPS request that has content in the request body.

When the Web Proxy receives an upload request, it compares the request to the Outbound Malware Scanning policy groups to determine which policy group to apply. After it assigns the request to a policy group, it compares the request to the policy group’s configured control settings to determine whether to block the request or monitor the request. When an Outbound Malware Scanning Policy determines to monitor a request, it is evaluated against the Access Policies, and the final action the Web Proxy takes on the request is determined by the applicable Access Policy.
For more information on configuring Outbound Malware Scanning Policies to block requests based on outbound malware, see Controlling Upload Requests Using Outbound Malware Scanning Policies, page 11-11.

**Note**

Upload requests that try to upload files with a size of zero (0) bytes are not evaluated against Outbound Malware Scanning Policies.

---

### Evaluating Outbound Malware Scanning Policy Group Membership

Each client request is assigned to an Identity and is then evaluated against the other policy types to determine to which policy group it belongs for each type. The Web Proxy evaluates upload requests against the Outbound Malware Scanning Policies.

The Web Proxy applies the configured policy control settings to a client request based on the client request’s policy group membership.

To determine the policy group that a client request matches, the Web Proxy follows a specific process for matching the group membership criteria. During this process, it considers the following factors for group membership:

- **Identity.** Each client request either matches an Identity, fails authentication and is granted guest access, or fails authentication and is terminated. For more information about evaluating Identity group membership, see Evaluating Identity Group Membership, page 7-2.

- **Authorized users.** If the assigned Identity requires authentication, the user must be in the list of authorized users in the Outbound Malware Scanning Policy group to match the policy group. The list of authorized users can be any of the specified groups or users or can be guest users if the Identity allows guest access.

- **Advanced options.** You can configure several advanced options for Outbound Malware Scanning Policy group membership. Some options, such as proxy port and URL category, can also be defined within the Identity. When an advanced option is configured in the Identity, it is not configurable in the Outbound Malware Scanning Policy group level.
The information in this section gives an overview of how the Web Proxy matches upload requests to Outbound Malware Scanning Policy groups. For more details about exactly how the Web Proxy matches client requests, see Matching Client Requests to Outbound Malware Scanning Policy Groups, page 11-4.

The Web Proxy reads sequentially through each policy group in the policies table. It compares the upload request status to the membership criteria of the first policy group. If they match, the Web Proxy applies the policy settings of that policy group.

If they do not match, the Web Proxy compares the upload request to the next policy group. It continues this process until it matches the upload request to a user defined policy group. If it does not match a user defined policy group, it matches the global policy group. When the Web Proxy matches the upload request to a policy group or the global policy group, it applies the policy settings of that policy group.

Matching Client Requests to Outbound Malware Scanning Policy Groups

Figure 11-1 on page 5 shows how the Web Proxy evaluates an upload request against the Outbound Malware Scanning groups.
Figure 11-1  Policy Group Flow Diagram for Outbound Malware Scanning Policies

1. Receive request from client.
2. Compare the client request against the next (or first) identity group in the policies table.
3. Is the current policy group the global policy?
   - Yes: Proceed to step 5.
   - No: Proceed to step 4.
4. Is the transaction assigned to one of the policy group's configured identities, or does the policy group use "All identities"?
   - Yes: Proceed to step 3.
   - No: Proceed to step 6.
5. Is the client subnet in the policy group's list of subnet(s) in the Advanced section?
   - Yes, or none defined: Proceed to step 6.
   - No: Proceed to step 7.
6. Is the proxy port in the policy group's list of ports in the Advanced section?
   - Yes, or none defined: Proceed to step 6.
   - No: Proceed to step 8.
7. Is the protocol in the policy group's list of protocol(s) in the Advanced section?
   - Yes, or none defined: Proceed to step 6.
   - No: Proceed to step 9.
8. Is the user agent in the policy group's list of user agents in the Advanced section?
   - Yes, or none defined: Proceed to step 6.
   - No: Proceed to step 10.
9. Is the URL category of the request URL in the policy group's list of URL categories in the Advanced section?
   - Yes, or none defined: Proceed to step 6.
   - No: Proceed to step 11.
10. Is the user one of the authorized users listed in the policy group? (List of authorized users can be a list of user names, user groups, all authenticated users, guest users, or All Users. If the policy group only uses identities with no authentication, then all clients are authorized.)
   - Yes: Proceed to step 5.
   - No: Proceed to step 6.

Apply the Outbound Malware Scanning Policy group settings to the client request.
Creating Outbound Malware Scanning Policies

You can create Outbound Malware Scanning Policy groups based on combinations of several criteria, such as one or more Identities or the URL category of the destination site. You must define at least one criterion for policy group membership. When you define multiple criteria, the upload request must meet all criteria to match the policy group. However, the upload request needs to match only one of the configured Identities.

For more information about how the Web Proxy matches an upload request with a policy group, see Evaluating Outbound Malware Scanning Policy Group Membership, page 11-3 and Matching Client Requests to Outbound Malware Scanning Policy Groups, page 11-4.

To create an Outbound Malware Scanning Policy group:

Step 1  Navigate to the Web Security Manager > Outbound Malware Scanning page, and click **Add Policy**.

Step 2  Enter a name and an optional description for the policy group.

Note  Each policy group name must be unique and only contain alphanumeric characters or the space character.

Step 3  In the Insert Above Policy field, select where in the policies table to place the policy group.

When configuring multiple policy groups, you must specify a logical order for each group. Carefully order your policy groups to ensure that correct matching occurs.

Step 4  In the Identities and Users section, select one or more Identity groups to apply to this policy group.

For more information, see Configuring Identities in Other Policy Groups, page 7-28.

Step 5  Optionally, expand the Advanced section to define additional membership requirements.
Step 6

To define policy group membership by any of the advanced options, click the link for the advanced option and configure the option on the page that appears.
Table 11-1 describes the advanced options you can configure for Outbound Malware Scanning Policy groups.

**Table 11-1 Outbound Malware Scanning Policy Group Advanced Options**

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
<td>Choose whether or not to define policy group membership by the protocol used in the client request. Select the protocols to include. “All others” means any protocol not listed above this option. <strong>Note:</strong> When the HTTPS Proxy is enabled, only Decryption Policies apply to HTTPS transactions. You cannot define policy membership by the HTTPS protocol for Access, Routing, Outbound Malware Scanning, Data Security, or External DLP Policies.</td>
</tr>
<tr>
<td>Proxy Ports</td>
<td>Choose whether or not to define policy group membership by the proxy port used to access the Web Proxy. Enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas. For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. You might want to define policy group membership on the proxy port if you have one set of clients configured to explicitly forward requests on one port, and another set of clients configured to explicitly forward requests on a different port. Cisco recommends defining policy group membership by the proxy port only when the appliance is deployed in explicit forward mode, or when clients explicitly forward requests to the appliance. If you define policy group membership by the proxy port when client requests are transparently redirected to the appliance, some requests might be denied. <strong>Note:</strong> If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</td>
</tr>
</tbody>
</table>
Chapter 11  Outbound Malware Scanning

Creating Outbound Malware Scanning Policies

Table 11-1  Outbound Malware Scanning Policy Group Advanced Options

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnets</td>
<td>Choose whether or not to define policy group membership by subnet or other addresses. You can select to use the addresses that may be defined with the associated Identity, or you can enter specific addresses here. <strong>Note:</strong> If the Identity associated with this policy group defines its membership by addresses, then in this policy group you must enter addresses that are a subset of the addresses defined in the Identity. Adding addresses in the policy group further narrows down the list of transactions that match this policy group.</td>
</tr>
<tr>
<td>URL Categories</td>
<td>Choose whether or not to define policy group membership by URL categories. Select the user defined or predefined URL categories. <strong>Note:</strong> If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</td>
</tr>
</tbody>
</table>
Creating Outbound Malware Scanning Policies

Step 7  Submit your changes.

Step 8  Configure Outbound Malware Scanning Policy group control settings to define how the Web Proxy handles transactions.

The new Outbound Malware Scanning Policy group automatically inherits global policy group settings until you configure options for each control setting. For more information, see Controlling Upload Requests Using Outbound Malware Scanning Policies, page 11-11.

Step 9  Submit and commit your changes.

Table 11-1  Outbound Malware Scanning Policy Group Advanced Options

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Agents</td>
<td>Choose whether or not to define policy group membership by the user agent used in the client request. You can select some commonly defined browsers, or define your own using regular expressions. Choose whether this policy group should apply to the selected user agents or to any user agent that is not in the list of selected user agents. For more information on creating user agent based policies, see Working with User Agent Based Policies, page 6-16. Note: If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</td>
</tr>
<tr>
<td>User Location</td>
<td>Choose whether or not to define policy group membership by user location, either remote or local. This option only appears when the Secure Mobility Solution is enabled. For more information, see Achieving Secure Mobility Overview, page 13-1.</td>
</tr>
</tbody>
</table>
Controlling Upload Requests Using Outbound Malware Scanning Policies

Each upload request is assigned to an Outbound Malware Scanning Policy group and inherits the control settings of that policy group. The control settings of the Outbound Malware Scanning Policy group determine whether or not to scan the upload request for malware and, if scanned, which malware types to block.

After the Web Proxy receives the upload request headers, it has all the information necessary to decide if it should scan the request body. The DVS engine scans the request and returns a verdict to the Web Proxy: either block or monitor (evaluate the request against the Access Policies). The block page appears to the end user, if applicable.

Figure 11-2 shows where you can configure control settings for the Outbound Malware Scanning Policy groups.

Figure 11-2 Creating Outbound Malware Scanning Policies

<table>
<thead>
<tr>
<th>Outbound Malware Scan Policies</th>
<th>Destinations</th>
<th>Anti-Malware Filtering</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>Outbound Malware Scan Policies</td>
<td>Destinations</td>
<td>Anti-Malware Filtering</td>
</tr>
<tr>
<td>1 exampleDMPL</td>
<td>Global Policy</td>
<td>Disabled/Text Only</td>
<td></td>
</tr>
<tr>
<td>Global Policy</td>
<td>Scan: None</td>
<td>Webroot: Enabled/Disabled</td>
<td></td>
</tr>
</tbody>
</table>

To configure control settings for an Outbound Malware Scanning Policy group:

**Step 1** Navigate to the Web Security Manager > Outbound Malware Scanning page.

**Step 2** In the Destinations column, click the link for the policy group you want to configure.

**Step 3** In the Edit Destination Settings section, select “Define Destinations Scanning Custom Settings” from the drop-down menu.
Figure 11-3  Scanning Destinations Settings for Outbound Malware Scanning Policies

Outbound Malware Scan Policies: Destinations: exampleOMSPolicy

<table>
<thead>
<tr>
<th>Scanning Destinations</th>
<th>Destinations to Scan:</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Do not scan any uploads</code></td>
<td>✓</td>
</tr>
<tr>
<td><code>Scan all uploads</code></td>
<td>✓</td>
</tr>
<tr>
<td><code>Scan uploads to specified custom URL categories</code></td>
<td>✓</td>
</tr>
</tbody>
</table>

Step 4  In the Destinations to Scan section, select one of the following options:

- **Do not scan any uploads.** The DVS engine scans no upload requests. All upload requests are evaluated against the Access Policies.

- **Scan all uploads.** The DVS engine scans all upload requests. The upload request is blocked or evaluated against the Access Policies, depending on the DVS engine scanning verdict.

- **Scan uploads to specified custom URL categories.** The DVS engine scans upload requests that belong in specific custom URL categories. The upload request is blocked or evaluated against the Access Policies, depending on the DVS engine scanning verdict. Click *Edit custom categories list* to select the URL categories to scan.

Step 5  Submit your changes.

Step 6  In the Anti-Malware Filtering column, click the link for the policy group.

Step 7  In the Anti-Malware Settings section, select “Define Anti-Malware Custom Settings” from the drop-down menu.
Step 8  In the IronPort DVS Anti-Malware Settings section, select which anti-malware scanning engines to enable for this policy group.

When you enable Sophos or McAfee scanning, you can select to monitor or block some additional categories in the Malware Categories on this page.

Step 9  In the Malware Categories section, select whether to monitor or block the various malware categories based on a malware scanning verdict.

The categories listed in this section depend on which scanning engines you enable.

**Note**  URL transactions are categorized as unscannable when the configured maximum time setting is reached or when the system experiences a transient error condition. For example, transactions might be categorized as unscannable during scanning engine updates or AsyncOS upgrades. The malware scanning verdicts SV_TIMEOUT and SV_ERROR are considered unscannable transactions.

Step 10  Submit and commit your changes.
Logging

The access logs indicate whether or not the DVS engine scanned an upload request for malware. The scanning verdict information section of each access log entry includes values for the DVS engine activity for scanned uploads. You can also add one of the fields in Table 11-2 to the W3C or access logs to more easily find this DVS engine activity:

Table 11-2  Log Fields in W3C Logs and Format Specifiers in Access Logs

<table>
<thead>
<tr>
<th>W3C Log Field</th>
<th>Format Specifier in Access Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-req-dvs-scanverdict</td>
<td>%X2</td>
</tr>
<tr>
<td>x-req-dvs-threat-name</td>
<td>%X4</td>
</tr>
<tr>
<td>x-req-dvs-verdictname</td>
<td>%X3</td>
</tr>
</tbody>
</table>

When the DVS engine marks an upload request as being malware and it is configured to block malware uploads, the ACL decision tag in the access logs is BLOCK_AMW_REQ.

However, when the DVS engine marks an upload request as being malware and it is configured to monitor malware uploads, the ACL decision tag in the access logs is actually determined by the Access Policy applied to the transaction.

To determine whether or not the DVS engine scanned an upload request for malware view the results of the DVS engine activity in the scanning verdict information section of each access log entry, or view the results of the fields from Table 11-2 added to the W3C or access logs.

For more information, see Understanding Scanning Verdict Information, page 24-30.
Data Security and External DLP Policies Overview

In the Information Age, your organization’s data is one of its most prized possessions. Your organization spends a lot of money making data available to your employees, customers, and partners. Data is always on the move by traveling over the web and email. This increased access poses challenges for information security professionals to figure out how to prevent the malicious, accidental, or unintentional loss of sensitive and proprietary information.
The IronPort Web Security appliance secures your data by providing the following capabilities:

- **IronPort Data Security Filters.** The IronPort Data Security Filters on the Web Security appliance evaluate data leaving the network over HTTP, HTTPS, and FTP to control what data goes where and how and by whom.

- **Third party data loss prevention (DLP) integration.** The Web Security appliance integrates with leading third party content-aware DLP systems that identify and protect sensitive data. The Web Proxy uses the Internet Content Adaptation Protocol (ICAP) which is a lightweight HTTP based protocol that allows proxy servers to offload content scanning to external systems. By offloading the content scanning to dedicated external systems, the Web Proxy can take advantage of the deep content scanning in other products while being free to perform other Web Proxy functions with minimal performance impact.

By working with the IronPort Data Security Filters and external DLP systems, the Web Security appliance allows you to protect information and intellectual property and enforce regulatory and organization compliance by preventing users from unintentionally uploading sensitive data. You define what kind of data is allowed to leave the network.

To restrict data that is leaving the network, the Web Security appliance provides the following types of policy groups:

- **IronPort Data Security Policies.** When you enable the IronPort Data Security Filters, you can create IronPort Data Security Policies to enforce business policies. For example, you can create a Data Security Policy that prevents users from sending out Excel or zip files. For more information, see Data Security Policy Groups, page 12-4.

- **External DLP Policies.** When you configure the appliance to work with an external DLP system, you can create External DLP Policies to pass data leaving the network to the external DLP system which scans the content and determines whether or not to block the request. For more information, see External DLP Policy Groups, page 12-6.

Depending on your organization’s needs, you might want to use both Data Security and External DLP Policies. For example, you might use the IronPort Data Security Policies to block data uploads to websites with a low reputation score. This way, the data is never sent to the external DLP system for a deep content scan, which improves overall performance.
Bypassing Upload Requests Below a Minimum Size

Many websites are interactive, meaning users send data as well as receive data. Users might send data when logging into a website or sending simple form data. A lot of web traffic can consist of relatively small POST requests that are harmless, but can take up many lines in the log files. This creates a lot of “noise” in the logs that can make it difficult to find and troubleshoot the true data security violations, such as users uploading company files using their personal email account.

To help reduce the number of upload requests recorded in the log files, you can define a minimum request body size, below which upload requests are not scanned by the IronPort Data Security Filters or the external DLP server.

To do this, use the following CLI commands:
- `datasecurityconfig`. Applies to the IronPort Data Security Filters.
- `externaldlpconfig`. Applies to the configured external DLP servers.

The default minimum request body size is 4 KB (4096 bytes) for both CLI commands. Valid values are 1 to 64 KB. The size you specify applies to the entire size of the upload request body.

Note

All chunk encoded uploads and all native FTP transactions are scanned by the IronPort Data Security Filters or external DLP servers when enabled. However, they can still be bypassed based on a custom URL category. For more information, see Figure 12-3 on page 16.

User Experience with Blocked Requests

When the IronPort Data Security Filters or an external DLP server blocks an upload request, it provides a block page that the Web Proxy sends to the end user. However, not all websites display the block page to the end user. For example, some Web 2.0 websites display dynamic content using javascript instead of a static webpage and are not likely to display the block page. Users are still properly blocked from performing data security violations, but they may not always be informed of this by the website.
Working with Data Security and External DLP Policies

IronPort Data Security Policies and External DLP Policies define how the Web Proxy handles HTTP requests and decrypted HTTPS connections for transactions that upload data to a server (upload requests). However, IronPort Data Security Policies use logic defined on the Web Security appliance and External DLP Policies use logic defined on the DLP system. An upload request is an HTTP or decrypted HTTPS request that has content in the request body.

When the Web Proxy receives an upload request, it compares the request to the Data Security and External DLP Policy groups to determine which policy group to apply. If both types of policies are configured, it compares the request to IronPort Data Security Policies before external DLP Policies. After it assigns the request to a policy group, it compares the request to the policy group’s configured control settings to determine what to do with the request.

How you configure the appliance to handle upload requests depends on the policy group type. For more information, see Data Security Policy Groups, page 12-4 and External DLP Policy Groups, page 12-6.

Note: Upload requests that try to upload files with a size of zero (0) bytes are not evaluated against IronPort Data Security or External DLP Policies.

Data Security Policy Groups

To configure the Web Security appliance to handle upload requests on the appliance itself, perform the following tasks:

Step 1. Enable the IronPort Data Security Filters. To scan upload requests on the appliance, you must first enable the IronPort Data Security Filters. Usually, the IronPort Data Security Filters feature is enabled during the initial setup using the System Setup Wizard. Otherwise, go to the Security Services > Data Security Filters page to enable it.
Chapter 12  Data Security and External DLP Policies

Step 2  Create and configure Data Security Policy groups. After the IronPort Data Security Filters feature is enabled, you create and configure Data Security Policy groups to determine how to handle upload requests from each user.

IronPort Data Security Policies use URL filtering, web reputation, and upload content information when evaluating the upload request. You configure each of these security components to determine whether or not to block the upload request. For more information about the security components that you can configure and how the Web Proxy uses Data Security Policy groups to control upload requests, see Controlling Upload Requests Using IronPort Data Security Policies, page 12-15.

When the Web Proxy compares an upload request to the control settings, it evaluates the settings in order. Each control setting can be configured to perform one of the following actions for IronPort Data Security Policies:

- **Block.** The Web Proxy does not permit the connection and instead displays an end user notification page explaining the reason for the block.

- **Allow.** The Web Proxy bypasses the rest of the Data Security Policy security service scanning and then evaluates the request against the Access Policies before taking a final action.

  For IronPort Data Security Policies, Allow bypasses the rest of data security scanning, but does not bypass External DLP or Access Policy scanning. The final action the Web Proxy takes on the request is determined by the applicable Access Policy (or an applicable external DLP Policy that may block the request).

- **Monitor.** The Web Proxy continues comparing the transaction to the other Data Security Policy group control settings to determine whether to block the transaction or evaluate it against the Access Policies.

  For IronPort Data Security Policies, only the Block action is a final action that the Web Proxy takes on a client request. A final action is an action that causes the Web Proxy to stop comparing the transaction to all other control settings. The Monitor and Allow actions are intermediary actions. In both cases, the Web Proxy evaluates the transaction against the External DLP Policies (if configured) and Access Policies. The Web Proxy determines which final action to apply based on the Access Policy group control settings (or an applicable external DLP Policy that may block the request).
Figure 12-3 on page 16 shows the order that the Web Proxy uses when evaluating control settings for IronPort Data Security Policies. The flow diagram shows that the only actions applied to a transaction are the final actions: Block and evaluate against the Access Policies.

For more information on the possible Access Policy actions, see Access Policy Groups, page 8-2. For more information on the Monitor action for Access Policies, see Understanding the Monitor Action, page 8-3.

External DLP Policy Groups

To configure the Web Security appliance to handle upload requests on an external DLP system, perform the following tasks:

**Step 1** Define an external DLP system. To pass an upload request to an external DLP system for scanning, you must define at least one ICAP-compliant DLP system on the Web Security appliance. Do this on the Network > External DLP Servers page. For more information, see Defining External DLP Systems, page 12-20.

**Step 2** Create and configure External DLP Policy groups. After an external DLP system is defined, you create and configure External DLP Policy groups to determine which upload requests to send to the DLP system for scanning.

When an upload request matches an External DLP Policy, the Web Proxy sends the upload request to the DLP system using the Internet Content Adaptation Protocol (ICAP) for scanning. The DLP system scans the request body content and returns a block or allow verdict to the Web Proxy. The allow verdict is similar to the Allow action for IronPort Data Security Policies in that the upload request will be compared to the Access Policies. The final action the Web Proxy takes on the request is determined by the applicable Access Policy.

For more information about configuring External DLP Policy groups, see Controlling Upload Requests Using External DLP Policies, page 12-25.
Evaluating Data Security and External DLP Policy Group Membership

Each client request is assigned to an Identity and then is evaluated against the other policy types to determine which policy group it belongs for each type. The Web Proxy evaluates upload requests against the Data Security and External DLP Policies.

The Web Proxy applies the configured policy control settings to a client request based on the client request’s policy group membership.

To determine the policy group that a client request matches, the Web Proxy follows a specific process for matching the group membership criteria. During this process, it considers the following factors for group membership:

- **Identity.** Each client request either matches an Identity, fails authentication and is granted guest access, or fails authentication and gets terminated. For more information about evaluating Identity group membership, see Evaluating Identity Group Membership, page 7-2.

- **Authorized users.** If the assigned Identity requires authentication, the user must be in the list of authorized users in the Data Security or External DLP Policy group to match the policy group. The list of authorized users can be any of the specified groups or users or can be guest users if the Identity allows guest access.

- **Advanced options.** You can configure several advanced options for Data Security and External DLP Policy group membership. Some options (such as proxy port and URL category) can also be defined within the Identity. When an advanced option is configured in the Identity, it is not configurable in the Data Security or External DLP Policy group level.

The information in this section gives an overview of how the Web Proxy matches upload requests to both Data Security and External DLP Policy groups. For more details about exactly how the Web Proxy matches client requests, see Matching Client Requests to Data Security and External DLP Policy Groups, page 12-8.

The Web Proxy sequentially reads through each policy group in the policies table. It compares the upload request status to the membership criteria of the first policy group. If they match, the Web Proxy applies the policy settings of that policy group.
If they do not match, the Web Proxy compares the upload request to the next policy group. It continues this process until it matches the upload request to a user defined policy group. If it does not match a user defined policy group, it matches the global policy group. When the Web Proxy matches the upload request to a policy group or the global policy group, it applies the policy settings of that policy group.

Matching Client Requests to Data Security and External DLP Policy Groups

Figure 12-1 on page 9 shows how the Web Proxy evaluates an upload request against the Data Security and External DLP Policy groups.
Figure 12-1  Policy Group Flow Diagram for Data Security and External DLP Policies

1. Receive request from client.
2. Compare the client request against the next (or first) identity group in the policies table.
3. Is the current policy group the global policy? Yes
4. Is the transaction assigned to one of the policy group’s configured identities, or does the policy group use “All Identities”? No
5. Is the client subnet in the policy group’s list of subnet(s) in the Advanced section? No
6. Is the proxy port in the policy group’s list of ports in the Advanced section? No
7. Is the protocol in the policy group’s list of protocol(s) in the Advanced section? No
8. Is the user agent in the policy group’s list of user agents in the Advanced section? No
9. Is the URL category of the request URL in the policy group’s list of URL categories in the Advanced section? No
10. Is the user one of the authorized users listed in the policy group? (List of authorized users can be a list of user names, user groups, all authenticated users, guest users, or All Users. If the policy group uses identities with no authentication, then all clients are authorized.) No
11. Apply the appropriate policy group settings to the upload request.

Yes
Creating Data Security and External DLP Policies

You can create Data Security and External DLP Policy groups based on combinations of several criteria, such as one or more Identities or the URL category of the destination site. You must define at least one criterion for policy group membership. When you define multiple criteria, the upload request must meet all criteria to match the policy group. However, the upload request needs to match only one of the configured Identities.

For more information about how the Web Proxy matches an upload request with a policy group, see Evaluating Data Security and External DLP Policy Group Membership, page 12-7 and Matching Client Requests to Data Security and External DLP Policy Groups, page 12-8.


To create a Data Security or External DLP Policy group:

---

**Step 1**  
Navigate to the Web Security Manager > IronPort Data Security page or the Web Security Manager > External Data Loss Prevention page.

**Step 2**  
Click Add Policy.

**Step 3**  
In the Policy Name field, enter a name for the policy group, and in the Description field, optionally add a description.

*Note*  
Each policy group name must be unique and only contain alphanumeric characters or the space character.

**Step 4**  
In the Insert Above Policy field, choose where in the policies table to place the policy group.

When configuring multiple policy groups you must specify a logical order for each group. Carefully order your policy groups to ensure that correct matching occurs.

**Step 5**  
In the Identities and Users section, choose one or more Identity groups to apply to this policy group.

For more information on how to do this, see Configuring Identities in Other Policy Groups, page 7-28.
Step 6  Optionally, expand the Advanced section to define additional membership requirements.

Step 7  To define policy group membership by any of the advanced options, click the link for the advanced option and configure the option on the page that appears.
Table 12-1 describes the advanced options you can configure for Data Security and External DLP Policy groups.

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Protocols       | Choose whether or not to define policy group membership by the protocol used in the client request. Select the protocols to include.  
“All others” means any protocol not listed above this option.  
**Note:** When the HTTPS Proxy is enabled, only Decryption Policies apply to HTTPS transactions. You cannot define policy membership by the HTTPS protocol for Access, Routing, Outbound Malware Scanning, Data Security, or External DLP Policies. |
| Proxy Ports     | Choose whether or not to define policy group membership by the proxy port used to access the Web Proxy. Enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas.  
For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. You might want to define policy group membership on the proxy port if you have one set of clients configured to explicitly forward requests on one port, and another set of clients configured to explicitly forward requests on a different port.  
Cisco recommends only defining policy group membership by the proxy port when the appliance is deployed in explicit forward mode, or when clients explicitly forward requests to the appliance. If you define policy group membership by the proxy port when client requests are transparently redirected to the appliance, some requests might be denied.  
**Note:** If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level. |
Creating Data Security and External DLP Policies

### Table 12-1 Data Security and External DLP Policy Group Advanced Options (continued)

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnets</td>
<td>Choose whether or not to define policy group membership by subnet or other addresses. You can choose to use the addresses that may be defined with the associated Identity, or you can enter specific addresses here. <strong>Note:</strong> If the Identity associated with this policy group defines its membership by addresses, then in this policy group you must enter addresses that are a subset of the addresses defined in the Identity. Adding addresses in the policy group further narrows down the list of transactions that match this policy group.</td>
</tr>
<tr>
<td>URL Categories</td>
<td>Choose whether or not to define policy group membership by URL categories. Select the user defined or predefined URL categories. <strong>Note:</strong> If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</td>
</tr>
</tbody>
</table>
Creating Data Security and External DLP Policies

Step 8
Submit your changes.

Step 9
If you are creating a Data Security Policy group, configure its control settings to define how the Web Proxy handles upload requests.

The new Data Security Policy group automatically inherits global policy group settings until you configure options for each control setting. For more information, see Controlling Upload Requests Using IronPort Data Security Policies, page 12-15.

Step 10
If you are creating an External DLP Policy group, configure its control settings to define how the Web Proxy handles upload requests.

The new External DLP Policy group automatically inherits global policy group settings until you configure custom settings. For more information, see Controlling Upload Requests Using External DLP Policies, page 12-25.

Step 11
Submit and commit your changes.

Table 12-1 Data Security and External DLP Policy Group Advanced Options (continued)

<table>
<thead>
<tr>
<th>Advanced Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Agents</td>
<td>Choose whether or not to define policy group membership by the user agent used in the client request. You can select some commonly defined browsers, or define your own using regular expressions. Choose whether this policy group should apply to the selected user agents or to any user agent that is not in the list of selected user agents. For more information on creating user agent based policies, see Working with User Agent Based Policies, page 6-16. Note: If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</td>
</tr>
<tr>
<td>User Location</td>
<td>Choose whether or not to define policy group membership by user location, either remote or local. This option only appears when the Secure Mobility Solution is enabled. For more information, see Achieving Secure Mobility Overview, page 13-1.</td>
</tr>
</tbody>
</table>
Controlling Upload Requests Using IronPort Data Security Policies

Each upload request is assigned to a Data Security Policy group and inherits the control settings of that policy group. The control settings of the Data Security Policy group determine whether the appliance blocks the connection or evaluates it against the Access Policies.


Figure 12-2 shows where you can configure control settings for the Data Security Policy groups.

**Figure 12-2  Creating Secure IronPort Data Security Policies**

You can configure the following settings to determine what action to take on upload requests:

- **URL Categories.** For more information, see URL Categories, page 12-17.
- **Web Reputation.** For more information, see Web Reputation, page 12-17.
- **Content.** For more information, see Content Blocking, page 12-17.

After a Data Security Policy group is assigned to an upload request, the control settings for the policy group are evaluated to determine whether to block the request or evaluate it against the Access Policies. For more information about assigning a Data Security Policy group to an upload request, see Policy Group Membership, page 6-10.

Figure 12-3 on page 16 shows how the appliance determines which action to take on an upload request after it has assigned a particular Data Security Policy to the request.
Controlling Upload Requests Using IronPort Data Security Policies

Figure 12-3 Applying Data Security Policy Actions

1. Receive upload request from client.
2. Is the request body size smaller than the minimum request body size (as determined by `dataset-size-config`)?
   - Yes
   - No
3. Is the request body size larger than the maximum allowed (as determined by the Content-Length header)?
   - Yes, action is Block.
   - No
4. Is the URL category of the request URL in the policy group's list of custom URL categories?
   - No, or Yes, action is Monitor.
5. Is the URL category of the request URL in the Access Policy group's list of predefined URL categories?
   - No, or Yes, action is Monitor.
6. Does the reputation score of the destination server indicate to block the connection?
   - Yes
   - No
7. Is the request body file name in the list of file names to block?
   - Yes
   - No
8. Is the request body file name in the list of regular expression file names to block?
   - Yes
   - No
9. Does the request body content match a blocked custom or predefined MIME type?
   - Yes
   - No
10. Is the size of the request body content greater than the maximum size allowed for the MIME type?
    - Yes
    - No
11. Block the connection.
12. Evaluate the request against the External DLP Policies, if configured. Otherwise, evaluate against the Access Policies.
URL Categories

AsyncOS for Web allows you to configure how the appliance handles a transaction based on the URL category of a particular request. Using a predefined category list, you can choose to monitor or block content by category. You can also create custom URL categories and choose to allow, monitor, or block traffic for a website in the custom category.

For more information about working with URL categories, see Configuring URL Filters for Data Security Policy Groups, page 16-13.

Web Reputation

The Web Reputation setting inherits the global setting. To customize web reputation filtering for a particular policy group, you can use the Web Reputation Settings pull-down menu to customize web reputation score thresholds.

Only negative and zero values can be configured for web reputation threshold settings for IronPort Data Security Policies. By definition, all positive scores are monitored.

For more information about configuring web reputation scores, see Configuring Web Reputation Scores, page 18-5.

Content Blocking

You can use the settings on the IronPort Data Security Policies > Content page to configure the Web Proxy to block data uploads based on the following file characteristics:

- **File size.** You can specify the maximum upload size allowed. All uploads with sizes equal to or greater than the specified maximum are blocked. You can specify different maximum file sizes for HTTP/HTTPS and native FTP requests.

  When the upload request size is greater than both the maximum upload size and the maximum scan size (configured in the “Object Scanning Limits” field on Security Services > Anti-Malware page), the upload request is still blocked, but the entry in the data security logs does not record the file name and content type. The entry in the access logs is unchanged.
• **File type.** You can block predefined file types or custom MIME types you enter. When you block a predefined file type, you can block all files of that type or files greater than a specified size. When you block a file type by size, the maximum file size you can specify is the same as the value for the “Object Scanning Limits” field on Security Services > Anti-Malware page. By default, that value is 32 MB.

IronPort Data Security Filters do not inspect the contents of archived files when blocking by file type. Archived files can be blocked by its file type or file name, not according to its contents.

**Note**
For some groups of MIME types, blocking one type blocks all MIME types in the group. For example, blocking application/x-java-applet blocks all java MIME types, such as application/java and application/javascript.

• **File name.** You can block files with specified names. You can use text as a literal string or a regular expression for specifying file names to block. For more information on using regular expressions, see Regular Expressions, page 16-28.

**Note**
Only enter file names with 8-bit ASCII characters. The Web Proxy only matches file names with 8-bit ASCII characters.

Figure 12-4 on page 19 shows the IronPort Data Security Policies > Content page where you configure the content control settings.
### Figure 12-4  IronPort Data Security Policies Content Settings

**IronPort Data Security Policies: Content: exampleIDSP**

<table>
<thead>
<tr>
<th>File Size</th>
<th>HTTP/HTTPS Maximum File Size:</th>
<th>No Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTIP Maximum File Size:</td>
<td><img src="image-url" alt="Image" /></td>
<td><img src="image-url" alt="Image" /></td>
</tr>
</tbody>
</table>

**Block File Types**

- Archives
- Document Types
- Executable Code
- Adrevt Plugin
- Windows Executable
- Java Program
- UNIX Executable
- MacOSX/MacOS Extension
- Installers
- Media
- P2P Metafiles
- Web Page Content
- Miscellaneous

**Custom MIME Types**

<table>
<thead>
<tr>
<th>Custom MIME Types:</th>
<th><img src="image-url" alt="Image" /></th>
</tr>
</thead>
</table>

(Enter multiple entries on separate lines. Example: `audio/mpeg`) or `audio/*` are valid entries.)

**File Names**

<table>
<thead>
<tr>
<th>File Names to Block:</th>
<th><img src="image-url" alt="Image" /></th>
</tr>
</thead>
</table>

(Enter multiple entries on separate lines. Example: `application/msword` or `application/*` are valid entries. File names are not case sensitive.)

Advanced: Match specific file names or regular expressions...
Defining External DLP Systems

The Web Security appliance can integrate with multiple external DLP servers from the same vendor by defining multiple DLP servers in the appliance. Define DLP systems and global settings that affect integration with all DLP systems on the Network > External DLP Servers page.

Figure 12-5  Network > External DLP Servers Page

You can define the load balancing technique the Web Proxy uses when contacting the DLP systems. This is useful when you define multiple DLP systems. For example, the Web Proxy can contact each DLP system using round-robin or a hash function.

To configure an external DLP server:

Step 1  Navigate to the Network > External DLP Servers page.
Step 2  Click Edit Settings.
### Figure 12-6 Configuring External DLP Servers

#### Edit External DLP Servers

<table>
<thead>
<tr>
<th>External DLP Servers:</th>
<th>Server</th>
<th>Port</th>
<th>Reconnection Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a1.example.com</td>
<td>1544</td>
<td>0</td>
</tr>
<tr>
<td>Service URL</td>
<td><a href="http://dlp.example.com">http://dlp.example.com</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

An ACAP URL must begin with `https://` and may not contain any whitespace.

Consult your DLP appliance vendor documentation for correct service URL for your system.

**Load Balancing:**
- Repeat Connections

**Service Request Timeout:**
- 60 seconds

**Maximum Simultaneous Connections:**
- 5

**Failure Handling:**
- Permit all data transfers to proceed without scanning
- Block data transfer for transactions where scanning was requested
Step 3  Enter the information in Table 12-2.
## Chapter 12  Data Security and External DLP Policies

### Defining External DLP Systems

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External DLP Servers</td>
<td>Enter the following information to access an ICAP compliant DLP system:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Server address and port.</strong> The hostname or IP address and TCP port for accessing the DLP system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reconnection attempts.</strong> The number of times the Web Proxy tries to connect to the DLP system before failing.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DLP Service URL.</strong> The ICAP query URL specific to the particular DLP server. The Web Proxy includes what you enter here in the ICAP request it sends to the external DLP server. The URL must start with the ICAP protocol: icap://</td>
</tr>
</tbody>
</table>
Table 12-2  *External DLP Server Settings (continued)*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Balancing</td>
<td>If multiple DLP servers are defined, select which load balancing technique the Web Proxy uses to distribute upload requests to different DLP servers. You can choose the following load balancing techniques:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None (failover).</strong> The Web Proxy directs upload requests to one DLP server. It tries to connect to the DLP servers in the order they are listed. If one DLP server cannot be reached, the Web Proxy attempts to connect to the next one in the list.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fewest connections.</strong> The Web Proxy keeps track of how many active requests are with the different DLP servers and it directs the upload request to the DLP server currently servicing the fewest number of connections.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hash based.</strong> The Web Proxy uses a hash function to distribute requests to the DLP servers. The hash function uses the proxy ID and URL as inputs so that requests for the same URL are always directed to the same DLP server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Round robin.</strong> The Web Proxy cycles upload requests equally among all DLP servers in the listed order.</td>
</tr>
<tr>
<td>Service Request Timeout</td>
<td>Enter how long the Web Proxy waits for a response from the DLP server. When this time is exceeded, the ICAP request has failed and the upload request is either blocked or allowed, depending on the Failure Handling setting. Default is 60 seconds.</td>
</tr>
</tbody>
</table>
Controlling Upload Requests Using External DLP Policies

Each upload request is assigned to an External DLP Policy group and inherits the control settings of that policy group. The control settings of the External DLP Policy group determine whether or not to send the upload request to the external DLP system for scanning.

Once the Web Proxy receives the upload request headers, it has all the information necessary to decide if the request should go to the external DLP system for scanning. The DLP system scans the request and returns a verdict to the Web Proxy, either block or monitor (evaluate the request against the Access Policies). The block page provided by the DLP system appears to the end user, if applicable.
If any Data Security Policy group applies to the upload request, the Web Proxy evaluates the policy group’s control settings against the upload request at the same time the external DLP system scans the request. If a Data Security Policy setting blocks the request before the DLP system is done scanning, the Web Proxy blocks the request and terminates the ICAP session with the DLP system.

Configure control settings for External DLP Policy groups on the Web Security Manager > External Data Loss Prevention page.

Figure 12-7 shows where you can configure control settings for the External DLP Policy groups.

**Figure 12-7 Creating External DLP Policies**

To configure control settings for an External DLP Policy group:

**Step 1** Navigate to the Web Security Manager > External Data Loss Prevention page.

**Step 2** Click the link under the Destinations column for the policy group you want to configure.

**Step 3** Under the Edit Destination Settings section, choose “Define Destinations Scanning Custom Settings” from the drop down menu if it is not selected already.
Figure 12-8  Scanning Destinations Settings for External DLP Policies

External DLP Policies: Destinations: exampleExternalDLPPolicy

Step 4  In the Destination to scan section, choose one of the following options:

- **Do not scan any uploads.** No upload requests are sent to the configured DLP system(s) for scanning. All upload requests are evaluated against the Access Policies.

- **Scan all uploads.** All upload requests are sent to the configured DLP system(s) for scanning. The upload request is blocked or evaluated against the Access Policies depending on the DLP system scanning verdict.

- **Scan uploads to specified custom URL categories only.** Upload requests that fall in specific custom URL categories are sent to the configured DLP system for scanning. The upload request is blocked or evaluated against the Access Policies depending on the DLP system scanning verdict. Click **Edit custom categories list** to select the URL categories to scan.

Step 5  Submit and commit your changes.

**Logging**

The access logs indicate whether or not an upload request was scanned by either the IronPort Data Security Filters or an external DLP server. The access log entries include a field for the IronPort Data Security scan verdict and another field for the External DLP scan verdict based. For more information, see **Understanding Scanning Verdict Information, page 24-30.**

In addition to the access logs, the Web Security appliance provides the following log file types to troubleshoot IronPort Data Security and External DLP Policies:

- **Data Security Logs.** Records client history for upload requests that are evaluated by the IronPort Data Security Filters.

Default Proxy Logs. In addition recording errors related to the Web Proxy, the default proxy logs include messages related to connecting to external DLP servers. This allows you to troubleshoot connectivity or integration problems with external DLP servers.

The following text illustrates a sample Data Security Log entry:


Table 12-3 describes the Data Security Log fields.

<table>
<thead>
<tr>
<th>Field Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Mar 30 03:02:13 2009 Info: 303</td>
<td>Timestamp and trace level</td>
</tr>
<tr>
<td>10.1.1.1</td>
<td>Transaction ID</td>
</tr>
<tr>
<td>-</td>
<td>Source IP address</td>
</tr>
<tr>
<td>-</td>
<td>User name</td>
</tr>
<tr>
<td>&lt;&lt;bar/text/plain,5120&gt;&lt;foo/text/plain,5120&gt;&gt;</td>
<td>Authorized group names</td>
</tr>
<tr>
<td>File name, file type, file size for each file uploaded at once</td>
<td></td>
</tr>
<tr>
<td>Note: This field does not include text/plain files that are less than the</td>
<td></td>
</tr>
<tr>
<td>configured minimum request body size, the default of which is 4096 bytes.</td>
<td></td>
</tr>
<tr>
<td>For more information on configuring the minimum request body size, see</td>
<td></td>
</tr>
<tr>
<td>Bypassing Upload Requests Below a Minimum Size, page 12-3.</td>
<td></td>
</tr>
<tr>
<td>BLOCK_WEBCAT_DLP-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting</td>
<td>IronPort Data Security Policy and action</td>
</tr>
<tr>
<td>ns</td>
<td>WBRS score</td>
</tr>
</tbody>
</table>
To learn when data transfer, such as a POST request, to a site was blocked by the external DLP server, search for the IP address or hostname of the DLP server in the access logs.

<table>
<thead>
<tr>
<th>Field Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server.com</td>
<td>Outgoing URL</td>
</tr>
<tr>
<td>nc</td>
<td>URL category</td>
</tr>
</tbody>
</table>
Achieving Secure Mobility Overview

Today, users and their devices are increasingly more mobile, connecting to the Internet from several locations, such as the office, home, airports, or cafes. Traditionally, users inside the network are protected from security threats, and users outside the traditional network boundary have no acceptable use policy enforcement, minimal protection against malware, and a high risk of data loss.

Employers want to create flexible working environments where employees and partners can work anywhere on any device, but they also want to protect corporate interests and assets from Internet-based threats at all times (always-on security).

Traditional network and content security solutions are great for protecting users and assets behind the network firewall, but are useless when users or devices are not connected to the network, or when data is not routed through the security solutions.
Cisco offers Secure Mobility Solution to extend the network perimeter to remote endpoints, enabling the seamless integration of web filtering services offered by the Web Security appliance. Secure Mobility Solution is a collection of features across multiple Cisco products that restores security and control in borderless networks. The Cisco products that work with Secure Mobility Solution are the Cisco IronPort Web Security appliance, Cisco ASA 5500 series adaptive security appliance, and Cisco AnyConnect secure mobility client.

Using Secure Mobility Solution, mobile and remote users have a seamless experience and are always protected from risks as if they were local users connected within the network.

When Secure Mobility Solution is enabled on the Web Security appliance, you can distinguish remote users from local users. This allows you to perform the following tasks:

- Create Identities and other policies for remote users.
- View reports for remote traffic.
- Enable single sign-on (SSO) for remote users.

For information on enabling single sign-on, see Transiently Identifying Remote Users, page 13-5.

**Note**

To enable Secure Mobility Solution, the appropriate license key must be installed on the Web Security appliance.

---

**Working with Remote Users**

When Secure Mobility Solution is enabled, you can configure Identities and other policies to apply to users by their location:

- **Remote users.** These users are connected to the network from a remote location using VPN (virtual private network). Users might be located in a home office, coffee shop, or hotel, for example. The Web Security appliance automatically identifies remote users when both the Cisco adaptive security appliance and Cisco AnyConnect client are used for VPN access. Otherwise, the Web Security appliance administrator must specify remote users by configuring a range of IP addresses.


- **Local users.** These users are connected to the network either physically or wirelessly.

You might want to create separate policies for remote and local users. For example, you can create Access Policies that allow access to Arts and Entertainment sites when users are outside the office (remote users), but block access when users are in the office (local users).

When you enable Secure Mobility Solution on the Security Services > Mobile User Security Page, you identify remote users using one of the following methods:

- **Associate by IP address.** Specify a range of IP addresses that the appliance should consider as assigned to remote devices. Typically, the Cisco adaptive security appliance assigns these IP addresses to devices that connect using VPN functionality. When the Web Security appliance receives a transaction from one of the configured IP addresses, it considers the user as a remote user.

- **Integrate with a Cisco ASA.** Specify one or more Cisco adaptive security appliances the Web Security appliance communicates with. The Cisco adaptive security appliance maintains an IP address-to-user mapping and communicates that information with the Web Security appliance. When the Web Proxy receives a transaction, it obtains the IP address and determines the user by checking the IP address-to-user mapping. When users are determined by integrating with a Cisco adaptive security appliance, you can enable single sign-on for remote users.

For information on enabling single sign-on, see [Transparencyly Identifying Remote Users, page 13-5](#).

---

### Enabling Secure Mobility

To protect remote users using always-on security, first you must enable the Secure Mobility Solution feature on the Web Security appliance. When Secure Mobility Solution is enabled, you can distinguish between remote users from local users when creating Identities.

- **Note**
  
  You can also configure Secure Mobility Solution using the CLI. For more information, see [Configuring Secure Mobility Using the CLI, page 13-7](#).

To enable Secure Mobility Solution:
Chapter 13      Achieving Secure Mobility

Enabling Secure Mobility


Step 2 Read the terms of the Mobile User Security License Agreement, and click **Accept**. The Mobile User Security Settings page appears.

**Mobile User Security Settings**

<table>
<thead>
<tr>
<th>Mobile User Security Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>When Mobile User Security is enabled, a policy can be created based on whether the user is physically in the corporate network or login through a VPN.</td>
</tr>
<tr>
<td><strong>Enable Mobile User Security</strong></td>
</tr>
<tr>
<td>Define Remote Users by: IP Range</td>
</tr>
<tr>
<td>(Examples: 10.1.1.1, 10.1.1.0/24, 10.1.1.2-20)</td>
</tr>
<tr>
<td><strong>Cisco ASA Integration</strong></td>
</tr>
<tr>
<td>ASA Hostname or IP Address</td>
</tr>
<tr>
<td>ASA Access Password:</td>
</tr>
</tbody>
</table>

**Step 3** Verify the Enable Mobile User Security field is enabled.

Configure how to identify remote users, by IP address or by integrating with one or more Cisco adaptive security appliances. For more information, see **Working with Remote Users, page 13-2**.

**Step 4** To identify remote users by IP address, select the IP Range option, enter a range of IP addresses in the IP Range field, and then go to step 10. Otherwise, go to step 5.

**Step 5** To identify remote users by integrating with one or more Cisco adaptive security appliances, select the Cisco ASA Integration option.
Step 6 Configure at least one Cisco adaptive security appliance by entering the Cisco adaptive security appliance host name or IP address in the ASA Host Name or IP Address field, and the port number used to access the ASA in the Port field. The default port number for the Cisco ASA is 11999.

Step 7 If multiple Cisco adaptive security appliances are configured in a cluster, click Add Row and configure each ASA in the cluster. If two Cisco adaptive security appliances are configured for high availability, enter only one host name or IP address for the active Cisco adaptive security appliance.

Step 8 In the ASA Access Password field, enter the access password for the Cisco adaptive security appliances specified in steps 6 and 7. The access password must be at least eight characters, and no more than 20 characters. The allowed characters are:

0-9 a-z A-Z . , : ; _ / -

Note The password you enter here must match the access password configured for the specified Cisco adaptive security appliances.

Step 9 Optionally, click Start Test to verify the Web Security appliance can connect to the configured Cisco adaptive security appliances.

Step 10 Submit and commit your changes.

**Transparently Identifying Remote Users**

When the Web Security appliance integrates with a Cisco adaptive security appliance, you can configure it to identify users by an authenticated user name transparently—that is, without prompting the end user. You might want to do this to achieve single sign-on for remote users.

Note You can also identify users transparently using Novell eDirectory. For more information, see Identifying Users Transparently, page 7-16.

To configure transparent user identification for remote users:
Step 1 Enable Secure Mobility Solution on the Security Services > Mobile User Security page.
For more information, see Enabling Secure Mobility, page 13-3.

Step 2 Create an Identity group that applies to remote users:
   a. In the “Define Members by User Location” section, select Remote Users Only.
   b. In the “Define Members by Authentication” section, select “Identify Users Transparently through Cisco ASA Integration.”
   c. Configure all other Identity options as desired.
For more information on creating Identities, see Creating Identities, page 7-20.

Step 3 Create policies that use the Identity for remote users.

Logging

The access logs indicate whether each transaction was made by a local or remote user. You can also add the same custom format specifier (%l) to the existing access logs, or you can add the equivalent W3C field (auth-user-type) to the W3C access logs.

In addition to the access logs, the Web Security appliance provides the following logs for troubleshooting potential Secure Mobility Solution issues.

- **User Discovery Service (UDS) log.** The UDS log 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 Secure Mobility Solution as well as integrating with the Novell eDirectory server for transparent user identification.

- **Mobile User Security Daemon log.** The Mobile User Security Daemon log records the interaction between the Web Security appliance and the AnyConnect client, including the status check.
Configuring Secure Mobility Using the CLI

Table 13-1 describes the CLI commands you can use to configure and monitor Secure Mobility Solution.

Table 13-1  Secure Mobility CLI Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| musconfig   | Use this command to enable Secure Mobility Solution and configure how to identify remote users, either by IP address or by integrating with one or more Cisco adaptive security appliances.  
  Note: Changes made using this command cause the Web Proxy to restart. 
  For more information on enabling and configuring Secure Mobility Solution, see Enabling Secure Mobility, page 13-3. |
| musstatus   | Use this command to display information related to Secure Mobility Solution when the Web Security appliance is integrated with an adaptive security appliance. 
  This command displays the following information: 
  • The status of the Web Security appliance connection with each adaptive security appliance. 
  • The duration of the Web Security appliance connection with each adaptive security appliance in minutes. 
  • The number of remote clients from each adaptive security appliance. 
  • The number of remote clients being serviced, which is defined as the number of remote clients that have passed traffic through the Web Security appliance. 
  • The total number of remote clients. |
Controlling Access to SaaS Applications

This chapter contains the following information:

- SaaS Access Control Overview, page 14-1
- Understanding How SaaS Access Control Works, page 14-2
- Configuring the Appliance as an Identity Provider, page 14-7
- Creating SaaS Application Authentication Policies, page 14-11

SaaS Access Control Overview

Organizations are increasingly choosing to use software as a service (SaaS) applications instead of owning and managing software applications within the organization. SaaS applications typically reside “in the cloud” instead of on-premise inside your network. There are many potential benefits to using SaaS applications, such as cost savings, but there are also challenges, especially for IT administrators who have to manage access control to the SaaS applications.

Cisco offers the SaaS Access Control feature which provides IT administrators with seamless, secure controls necessary for managing access to SaaS applications and enforcing security policies. SaaS Access Control allows IT administrators to easily control authentication and authorization for users who need to access SaaS applications.
When you enable Cisco SaaS Access Control, users log into the configured SaaS applications using their network authentication user credentials. That means they use the same user name and password for all SaaS applications as well as network access. You can choose whether users are transparently signed in (single sign-on functionality) or prompted to enter their authentication user name and password.

Using Cisco SaaS Access Control with the proper access controls of your SaaS application allows you to:

- Control which users can access SaaS applications and from where.
- Increase usability for end users by requiring them to remember only one password.
- Quickly disable access to all SaaS applications when users are no longer employed by the organization. This is sometimes referred to as “zero day revocation.”
- Reduce the risk of phishing attacks that ask users to enter their SaaS user credentials.

### Understanding How SaaS Access Control Works

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

SAML is an XML-based standard for exchanging authentication and authorization data between different secure networks, sometimes referred to as security domains. The main problem that SAML solves is single sign-on between different security domains. Typically, this is users in one domain accessing a network (a different domain) using a web browser. This is sometimes referred to as web browser single sign-on.

To achieve web browser single sign-on, a SAML dialogue must be engaged by an entity in each domain, which SAML defines using the following terms:

- **Identity provider.** An identity provider is an entity that produces SAML assertions. The identity provider is expected to authenticate its end users before producing a SAML assertion. The Web Security appliance is an identity provider.
**Service provider.** A service provider is an entity that consumes SAML assertions. The SaaS applications you configure on the Web Security appliance are service providers. The service provider relies on the identity provider to identify the end user and communicate that identification to the service provider in the SAML assertion. The service provider makes an access control decision based on the assertion.

SAML assertions are containers of information passed between identity providers and service providers inside SAML requests and responses. Assertions contain statements (such as authentication and authorization statements) that service providers use to make access control decisions. Assertions start with the `<saml:Assertion>` tag.

SAML dialogues are called flows, and flows can be initiated by either provider:

- **Service provider initiated flow.** The service provider is contacted by an end user requesting access so it starts a SAML dialogue by contacting the identity provider to provide identification for the user. For service provider initiated flows, the end user accesses the service provider using a URL that contains the service provider’s domain, such as http://www.serviceprovider.com/<URI>.

- **Identity provider initiated flow.** The identity provider starts a SAML dialogue by contacting the service provider requesting access on behalf of an end user. For identity provider initiated flows, the end user accesses the service provider using a URL that contains a local domain, such as http://saas.example.com/<URI>.

SaaS applications define whether they support service provider or identity provider initiated flows. For example, Salesforce supports identity provider initiated flows, Google Apps supports service provider initiated flows, and Cisco WebEx supports both.

The type of flow supported by a SaaS application determines how end users access the application. For more information, see Understanding the Single Sign-On URL, page 14-5.

---

**Note**

This section does not provide a comprehensive discussion of SAML, nor how identity and security providers communicate with each other. For more detailed information, read about SAML on the web at http://docs.oasis-open.org/security/saml/v2.0/.
Authenticating SaaS Users

When users access a SaaS application, you can allow them to transparently sign into the SaaS application using their local authentication credentials or always prompt them for their local authentication credentials.

When users are prompted to authenticate, the authentication credentials are sent to the Web Proxy using a secure HTTPS connection. The appliance uses its own certificate and private key to create an HTTPS connection with the client by default. Most browsers will warn users that the certificate is not valid. To prevent users from seeing the invalid certificate message, you can upload a certificate and key pair your organization uses. For information about uploading a certificate and key, see Uploading Certificates and Keys to Use with Credential Encryption and SaaS Access Control, page 20-38.

Note

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

Authentication Requirements

Some service providers require a particular authentication mechanism to allow users to access the SaaS application. If a service provider requires an authentication context that is not supported by an identity provider, users cannot access the service provider using single sign-on from the identity provider.

Therefore, SaaS Access Control only works with SaaS applications that require an authentication mechanism supported by the Web Security appliance. Currently, the Web Proxy uses the “PasswordProtectedTransport” authentication mechanism. You configure this value when you create a SaaS Application Authentication Policy using the Authentication Context setting. However, administrators typically choose “Automatic” as the Authentication Context setting.

For more information on creating SaaS Application Authentication Policies, see Creating SaaS Application Authentication Policies, page 14-11.
Enabling SaaS Access Control

To enable SaaS Access Control, you must configure settings on both the Web Security appliance and the SaaS application. It is very important that the settings you configure on the appliance and SaaS application match each other appropriately.

When enabling SaaS Access Control, it is easiest to keep open a connection to the Web Security appliance and the SaaS application simultaneously. You will need to go back and forth between both components and copy and paste information between both.

**Note**
For more information on configuring SaaS Access Control for particular SaaS applications, contact your technical sales representative or search the cisco.com website for additional information, such as white papers, knowledge base articles, or video tutorials.

To use SaaS Access Control, follow these steps:

1. **Configure the Web Security appliance as an identity provider.** For more information, see Configuring the Appliance as an Identity Provider, page 14-7.

2. **Configure the SaaS application for single sign-on.** When configuring the SaaS application, you must also upload the certificate used on the Security Services > Identity Provider for SaaS page. For more information, see the SaaS application documentation.

3. **Create one or more SaaS Application Authentication Policies for each SaaS application.** For more information, see Creating SaaS Application Authentication Policies, page 14-11.

Understanding the Single Sign-On URL

After you configure the Web Security appliance as an identity provider and create a SaaS Application Authentication Policy for the SaaS application, the appliance creates a single sign-on URL (SSO URL).

How administrators use this URL depends on the flow type:
Identity provider initiated flows. Administrators should make the single sign-on URL available to end users to access this SaaS application. For example, administrators can create an internal web page that includes this URL as a link. After users login, the appliance redirects users to the SaaS application.

Service Provider initiated flows. Administrators should configure this URL in the SaaS application. The SaaS application uses the single sign-on URL to redirect the browser session depending on the “SaaS SSO Authentication Prompt” setting in the policy group:

- Always prompt SaaS users for proxy authentication. A Web Security appliance page appears where users can enter their local authentication credentials. After entering valid credentials, users are logged into the SaaS application.
- Transparently sign in SaaS users. Users are logged into the SaaS application automatically.

The Web Security appliance uses the application name configured in the SaaS Application Authentication Policy to generate the single sign-on URL. You can view the single sign-on URL on the Web Security Manager > SaaS Policies page after you submit the changes.

The single sign-on URL format is:

http://IdentityProviderDomainName/SSOURL/ApplicationName

Therefore, when the appliance Identity Provider Domain Name is idp.example.com and the application name in the SaaS Application Authentication Policy is GoogleApps, the single sign-on URL is:

http://idp.example.com/SSOURL/GoogleApps

Using SaaS Access Control with Multiple Appliances

When you use multiple Web Security appliances with SaaS Access Control, you must perform the following steps:

- Configure the same Identity Provider Domain Name for each Web Security appliance.
- Configure the same Identity Provider Entity ID for each Web Security appliance.
• Upload the same certificate and private key to each appliance on the Security Services > Identity Provider for SaaS page. Then upload this certificate to each SaaS application you configure.

## Configuring the Appliance as an Identity Provider

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

After you choose which certificate and key to use for signing SAML assertions, you must upload the certificate to each SaaS application. You can do this using the Download Certificate link in the Signing Certificate area. Uploading the certificate ensures the SaaS application (service provider) has the Web Security appliance public key in order to form a trusted relationship between the service provider and the Web Security appliance (identity provider).

Consider the following rules and guidelines when you configure the Web Security appliance as an identity provider:

• The identity provider domain name must be resolvable within the network. For example, within the organization “example.com,” a transparent request to “http://idp.example.com/” should be network routable and can reach to the Web Security appliance within the network perimeter.

• If you intend to use multiple Web Security appliances with SaaS Access Control, you must enter the same Identity Provider Domain Name for each appliance and the same Identity Provider Entity ID for each appliance. For more information, see Using SaaS Access Control with Multiple Appliances, page 14-6.

• After you generate on or upload a certificate and key to the appliance, you must upload the same certificate to each SaaS application with which the Web Security appliance will communicate. You can do this by downloading the certificate from the appliance first.

• Make note of the settings you configure when you configure the Web Security appliance as an identity provider. Some of these settings must be used when configuring the SaaS application for single sign-on. It is easiest to keep open
a connection to the Web Security appliance and the SaaS application simultaneously. You will need to go back and forth between both components and copy and paste information between both

- The appliance constructs a single sign-on (SSO) login URL for each SaaS application based on the value you enter the Identity Provider Domain Name field and the SaaS application name configured in the SaaS policy. For more information, see Understanding the Single Sign-On URL, page 14-5.

To configure the Web Security appliance as an identity provider:

---

Step 1
Navigate to the Security Services > Identity Provider for SaaS page.

Step 2
Click Edit Settings.

---

Step 3
In the Identity Provider Domain Name field, enter a virtual domain name to use to access the Web Security appliance as an identity provider instance.

The identity provider domain name should be resolvable within the network. For example, within the organization “example.com,” a transparent request to “http://idp.example.com/” should be network routable and can reach to the Web Security appliance within the network perimeter.
Chapter 14      Controlling Access to SaaS Applications

Configuring the Appliance as an Identity Provider

Note
If you intend to use multiple Web Security appliances with SaaS Access Control, you must enter the same Identity Provider Domain Name for each Web Security appliance. If you have only one appliance, you can use the appliance hostname as the Identity Provider Domain Name. For more information, see Using SaaS Access Control with Multiple Appliances, page 14-6.

Step 4
In the Identity Provider Entity ID field, enter the text you want to use that uniquely identifies this Web Security appliance as an identity provider to all SaaS applications it will communicate with.

A URI format based string is recommended, but you can enter any unique string. The URI string does not have to be network accessible. Record the value you enter here because you will need to use the same value when you configure the SaaS application for single sign-on.

Note
If you intend to use multiple Web Security appliances with SaaS Access Control, you must enter the same Identity Provider Entity ID for each Web Security appliance. For more information, see Using SaaS Access Control with Multiple Appliances, page 14-6.

Step 5
Configure a signing certificate the appliance should use when it communicates using a secure connection (in the SAML flow) with service providers. You can use either of the following methods to configure the certificate:

- Generated certificate and key. Go to step 6 on page 9.
- Uploaded certificate and key. Go to step 7 on page 10.

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

Step 6
To generate a certificate and key:

a. Click the Use Generated Certificate and Key option.

b. Click Generate New Certificate and Key.

c. In the Generate Certificate and Key dialog box, enter the information to display in the signing certificate.
You can enter any ASCII character except the forward slash (/) in the Common Name field.

d. Click **Generate**. The Web Security appliance generates the certificate with the data you entered and generates a key.

The generated certificate information is displayed on the Edit Identity Provider Settings for SaaS Single Sign on page.

Note

After you generate the certificate and key, you can download the generated certificate to transfer it to the SaaS applications with which the Web Security appliance will communicate. Do this using the Download Certificate link in the generated key area.

e. Go to step 8 on page 11.

**Step 7**

To upload a root certificate and key:

a. Click **Use Uploaded Certificate and Key**.

b. 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.

Note

The certificate file must be in PEM format. DER format is not supported.

c. Click **Browse** for the Key field to navigate to the private key file. The private key must be unencrypted.

Note

The key length must be 512, 1024, or 2048 bits. Also, the private key file must be in PEM format. DER format is not supported.

d. Click **Upload Files** to transfer the certificate and key files to the Web Security appliance.
Creating SaaS Application Authentication Policies

After you configure the Web Security appliance as an identity provider and you configure a SaaS application for single sign-on, you can create a SaaS Application Authentication Policy so the Web Security appliance can communicate with the SaaS application and enable web browser single sign-on.

Consider the following rules and guidelines when you configure the SaaS application information in a SaaS Application Authentication Policy:

- The Assertion Consumer Service Location URL must be must be resolvable within the network.

- The appliance constructs a single sign-on (SSO) login URL for each SaaS application based on the value you enter the Identity Provider Domain Name field for the appliance and the SaaS application name configured in the SaaS policy. For more information, see Understanding the Single Sign-On URL, page 14-5.

To create a SaaS Application Authentication Policy:

**Step 1** Navigate to the Web Security Manager > SaaS Policies page.

**Step 2** Click Add Applications to create a new policy for a particular SaaS application.
### New SaaS Application

<table>
<thead>
<tr>
<th>SaaS Application</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metadata for Service Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure Keys Manually</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Provider Entity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name ID Format:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assertion Consumer Service URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Import file from hard disk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Sequence or Realm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SaaS SSO Authentication Prompt:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Always prompt SaaS users for proxy authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transparently sign SaaS users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAML Username Mapping:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No mapping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expression Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAML Attribute Mapping:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enter a list of attributes that will be sent to the service provider for attribute mapping.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAML Attribute</td>
<td>LDAP Attribute</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Context:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 14  Controlling Access to SaaS Applications

Creating SaaS Application Authentication Policies

Step 3  Configure the settings defined in Table 14-1.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>Enter a name to identify the SaaS application for this policy group. Each</td>
</tr>
<tr>
<td></td>
<td>application name must be unique and only contain alphanumeric characters or</td>
</tr>
<tr>
<td></td>
<td>the space character. The Web Security appliance uses the application name</td>
</tr>
<tr>
<td></td>
<td>to generate a single sign-on URL. For more information, see Understanding</td>
</tr>
<tr>
<td></td>
<td>the Single Sign-On URL, page 14-5.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a description for this SaaS application.</td>
</tr>
</tbody>
</table>
Creating SaaS Application Authentication Policies

The Web Security appliance uses the metadata to determine how to communicate with the SaaS application (service provider) using SAML. Contact the SaaS application to learn the correct settings to configure the metadata.

When you manually configure the metadata information, configure the following values:

- **Service Provider Entity ID.** Enter the text (typically in URI format) the SaaS application uses to identify itself as a service provider.

- **Name ID Format.** Enter the format the appliance should use to identify users in the SAML assertion it sends to service providers. The value you enter here must match the corresponding setting configured on the SaaS application.

- **Assertion Consumer Service Location.** Enter the URL to where the Web Security appliance should send the SAML assertion it creates. Read the SaaS application documentation to determine that correct URL to use. Sometimes, this is referred to as the login URL.

**Note:** The metadata file is an XML document following the SAML standard that describes a service provider instance. Not all SaaS applications use metadata files, but for those that do, contact the SaaS application provider for the file.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata for Service Provider</td>
<td>Configure the metadata that describes the service provider referenced in this policy group. You can either describe the service provider properties manually or upload a metadata file provided by the SaaS application.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
Chapter 14 Controlling Access to SaaS Applications

Creating SaaS Application Authentication Policies

Creating SaaS Application Authentication Policies

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Sequence or Realm</td>
<td>Choose the authentication realm or authentication sequence the Web Proxy should use to authenticate users accessing this SaaS application. Users must be a member of the authentication realm or authentication sequence to successfully access the SaaS application.</td>
</tr>
<tr>
<td>Single Sign On</td>
<td>Choose whether to allow users to transparently sign into the SaaS application using their local authentication credentials, or to always prompt users for their credentials when accessing the SaaS application. You might want to prompt users for their credentials for applications that store sensitive data, such as sales or HR data, and transparently sign in users for applications that do not store sensitive data. For more information, see Authenticating SaaS Users, page 14-4.</td>
</tr>
</tbody>
</table>
| User Name Identifier Mapping | Specify how the Web Proxy should represent user names to the service provider in the SAML assertion. You can pass the user names as they are used inside your network (no mapping), or you can change the internal user names into a different format using one of the following methods:  
  - Fixed Rule mapping. The user names sent to the service provider are based on the internal user name with a fixed string added before or after the internal user name. Enter the fixed string and %s for the internal user name.  
  - LDAP query. The user names sent to the service provider are based on one or more LDAP query attributes. Enter an expression containing LDAP attribute fields and optional custom text. You must enclose attribute names in angled brackets. You can include any number of attributes. For example, for the LDAP attributes “user” and “domain,” you could enter <user>@<domain>.com. |
### Attribute Mapping Options

Optionally, you can provide to the SaaS application additional information about the internal users from the LDAP authentication server if required by the SaaS application. Map each LDAP server attribute to a SAML attribute.

For example, you could map the LDAP attribute “mail” to the SAML attribute “email.”

### Authentication Context

Specify the authentication mechanism the Web Proxy uses to authenticate its internal users. Currently, the Web Proxy uses “PasswordProtectedTransport,” however, administrators typically choose “Automatic.”

**Note:** The authentication context informs the service provider which authentication mechanism the identity provider used to authenticate the internal users. Some service providers require a particular authentication mechanism to allow users to access the SaaS application. If a service provider requires an authentication context that is not supported by an identity provider, users cannot access the service provider using single sign-on from the identity provider.

### Step 4

Submit and commit your changes.
CHAPTER 15

Notifying End Users

This chapter contains the following information:

- Notifying End Users of Organization Policies, page 15-1
- Configuring General Settings for Notification Pages, page 15-3
- Working With IronPort End-User Notification Pages, page 15-5
- Working with User Defined End-User Notification Pages, page 15-14
- End-User Acknowledgement Page, page 15-18
- Configuring the End-User URL Filtering Warning Page, page 15-21
- Working with IronPort FTP Notification Messages, page 15-23
- Custom Text in Notification Pages, page 15-23
- Notification Page Types, page 15-25

Notifying End Users of Organization Policies

The Web Security appliance helps your organization implement and enforce policies for accessing the web. When a policy blocks a user from a website, you can configure the appliance to notify the user why it blocked the URL request. Web users see a webpage that explains that they were blocked from accessing a website and why they were blocked. These pages are called end-user notification pages. The Web Proxy can display different end-user notification pages depending on the reason it blocked the URL request. You can use the provided end-user notification pages or define your own.
Configure end-user notification pages on the Security Services > End-User Notification page. Figure 15-1 shows where you configure end-user notification settings.

### End-User Notification

<table>
<thead>
<tr>
<th>End-User Notification Settings</th>
<th>Language: English</th>
<th>Logo Image: No Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP End-User Acknowledgement Page</td>
<td>End-User Acknowledgement: Disabled</td>
<td>Custom Message: Undefined</td>
</tr>
<tr>
<td>HTTP End-User Notification Pages</td>
<td>Notification Type: Use IronPort notification Pages</td>
<td>Custom Message: Undefined</td>
</tr>
<tr>
<td></td>
<td>Contact Information: your corporate network administrator</td>
<td>End-User Classification Reporting: Disabled</td>
</tr>
<tr>
<td>End-User URL Category Warning Page</td>
<td>Time Between Warnings: 1h</td>
<td>Custom Message: Undefined</td>
</tr>
<tr>
<td>Native FTP End-User Notification Pages</td>
<td>Language: English</td>
<td>Custom Message: Undefined</td>
</tr>
</tbody>
</table>

You can configure the following types of notification pages and settings:

- **IronPort notification pages.** The Web Proxy displays different, predefined notification pages depending on the reason for blocking the URL request. You can customize these pages. For example, you can use your own logo or add custom text. For more information about IronPort notification pages, see Working With IronPort End-User Notification Pages, page 15-5.

- **User defined notification pages.** You can configure the Web Proxy to redirect all HTTP end-user notification pages to a specific URL. The Web Proxy includes parameters in the redirected URL that explain the reasons for the block so the server in the redirected URL can customize the page it displays. For more information about user defined notification pages, see Working with User Defined End-User Notification Pages, page 15-14.

- **End-user acknowledgement page.** You can configure the Web Proxy to inform users that it is filtering and monitoring their web activity. The Web Proxy does this by displaying an end-user acknowledgement page when a user first accesses a browser after a certain period of time. When the end-user acknowledgement page appears, users must click a link to access the original
site requested or any other website. Language and logo settings apply to the end-user acknowledgement page as well as the notification pages. For more information about configuring the end-user acknowledgement page, see End-User Acknowledgement Page, page 15-18.

- **End-user URL filtering warning page.** You can configure the Web Proxy to warn users that a site does not meet the organization’s acceptable use policies and allow them to continue if they choose. The Web Proxy does this by displaying an end-user URL filtering warning page 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. When the warning page appears, users can click a link to access the original site requested. Language and logo settings apply to the end-user URL filtering warning page as well as the notification pages. For more information about configuring the end-user URL filtering warning page, see Warning Users and Allowing Them to Continue, page 16-24.

- **FTP notification messages.** The FTP Proxy displays a different, predefined notification messages depending on the reason for blocking a native FTP transaction. You can customize these pages with a custom message. For more information, see Working with IronPort FTP Notification Messages, page 15-23.

- **General notification settings.** You can configure the language used in IronPort notification pages for both HTTP and FTP. You can also configure a logo to use for IronPort notification pages for HTTP requests. For more information, see Configuring General Settings for Notification Pages, page 15-3.

---

### Configuring General Settings for Notification Pages

You can configure the following general settings:

- **Language.** You can configure a different language for HTTP and FTP end-user notification pages. The HTTP language setting applies to all HTTP notification pages (acknowledgement, IronPort end-user, end-user URL filtering warning, and user defined end-user), and the FTP language applies to all FTP end-user notification messages.
Chapter 15 Notifying End Users

Configuring General Settings for Notification Pages

- **Logo.** You can configure a logo for HTTP end-user notification pages only. The logo setting applies to all HTTP notification pages.

To configure the general settings for HTTP notification pages and FTP notification messages:

**Step 1** Navigate to the Security Services > End-User Notification page.

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

**Step 3** In the General Settings section under the HTTP/HTTPS section, select the language the Web Proxy should use when displaying HTTP notification pages. You can choose any of the following languages:

- English
- French
- German
- Italian
- Spanish
- Japanese
- Korean
- Portuguese
- Russian
- Thai
- Traditional Chinese
- Simplified Chinese
Step 4  Choose whether or not to use a logo on each notification page. You can specify the IronPort logo or any graphic file referenced at the URL you enter in the Use Custom Logo field.

Note  See Custom Text and Logos: Authentication, and End-User Acknowledgement Pages, page 15-24 for more information about working with custom logos.

Step 5  Submit and commit your changes.

**Working With IronPort End-User Notification Pages**

When you choose end-user notification pages defined by IronPort, the Web Proxy displays a different page depending on the reason why it blocked the original page. However, you can still customize each page to make them specific to your organization.

You can customize the following features:
- Custom message
- Contact information
- Allow end-users to report misclassified pages to IronPort

You can also edit the IronPort notification pages stored on the Web Security appliance. For more information about how to do this, see Editing IronPort Notification Pages, page 15-8.

**Configuring IronPort Notification Pages**

To configure IronPort notification pages:

Step 1  Navigate to the Security Services > End-User Notification page, and click **Edit Settings**.

The Edit End-User Notification page appears.
Step 2  From the Notification Type field, choose Use IronPort Notification Pages.

Step 3  Configure the IronPort notification page settings.
Table 15-1 describes the settings you can configure for IronPort notification pages.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Message</td>
<td>Choose whether or not to include additional text you specify on each notification page.</td>
</tr>
<tr>
<td></td>
<td>When you enter a custom message, AsyncOS places the message before the last sentence on the notification page which includes the contact information.</td>
</tr>
<tr>
<td></td>
<td>You can include some HTML tags in lower case to format the text. For a list of supported HTML tags, see Supported HTML Tags in Notification Pages, page 15-23.</td>
</tr>
<tr>
<td></td>
<td>See Custom Text and Logos: Authentication, and End-User Acknowledgement Pages, page 15-24 for more information about working with custom messages.</td>
</tr>
</tbody>
</table>
Step 4 Click the “Preview Notification Page Customization” link to view the current end-user notification page in a separate browser window.

Step 5 Submit and commit your changes.

Editing IronPort Notification Pages

Each IronPort Notification page is stored on the Web Security appliance as an HTML file. You can edit the content of these HTML pages to include additional text or to edit the overall look and feel of each page.
You can use variables in the HTML files to display specific information to the user. You can also turn each variable into a conditional variable to create if-then statements. For more information, see Using Variables in Customized IronPort Notification Pages, page 15-13.

Table 15-2 describes the variables you can include in customized end-user notification pages.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Always Evaluates to TRUE if Used as Conditional Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>%a</td>
<td>Authentication realm for FTP</td>
<td>No</td>
</tr>
<tr>
<td>%A</td>
<td>ARP address</td>
<td>Yes</td>
</tr>
<tr>
<td>%b</td>
<td>User-agent name</td>
<td>No</td>
</tr>
<tr>
<td>%B</td>
<td>Blocking reason, such as BLOCK-SRC or BLOCK-TYPE</td>
<td>No</td>
</tr>
<tr>
<td>%c</td>
<td>Error page contact person</td>
<td>Yes</td>
</tr>
<tr>
<td>%C</td>
<td>Entire Set-Cookie: header line, or empty string</td>
<td>No</td>
</tr>
<tr>
<td>%d</td>
<td>Client IP address</td>
<td>Yes</td>
</tr>
<tr>
<td>%D</td>
<td>User name</td>
<td>No</td>
</tr>
<tr>
<td>%e</td>
<td>Error page email address</td>
<td>Yes</td>
</tr>
<tr>
<td>%E</td>
<td>The error page logo URL</td>
<td>No</td>
</tr>
<tr>
<td>%f</td>
<td>User feedback section</td>
<td>No</td>
</tr>
<tr>
<td>%F</td>
<td>The URL for user feedback</td>
<td>No</td>
</tr>
<tr>
<td>%g</td>
<td>The web category name, if available</td>
<td>Yes</td>
</tr>
<tr>
<td>%G</td>
<td>Maximum file size allowed in MB</td>
<td>No</td>
</tr>
<tr>
<td>%h</td>
<td>The hostname of the proxy</td>
<td>Yes</td>
</tr>
<tr>
<td>%H</td>
<td>The server name of the URL</td>
<td>Yes</td>
</tr>
<tr>
<td>%i</td>
<td>Transaction ID as a hexadecimal number</td>
<td>Yes</td>
</tr>
<tr>
<td>%I</td>
<td>Management IP Address</td>
<td>Yes</td>
</tr>
<tr>
<td>%j</td>
<td>URL category warning page custom text</td>
<td>No</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Always Evaluates to TRUE if Used as Conditional Variable</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>%k</td>
<td>Redirection link for the end-user acknowledgement page and end-user URL filtering warning page</td>
<td>No</td>
</tr>
<tr>
<td>%K</td>
<td>Response file type</td>
<td>No</td>
</tr>
<tr>
<td>%I</td>
<td>WWW-Authenticate: header line</td>
<td>No</td>
</tr>
<tr>
<td>%L</td>
<td>Proxy-Authenticate: header line</td>
<td>No</td>
</tr>
<tr>
<td>%M</td>
<td>The Method of the request, such as “GET” or “POST”</td>
<td>Yes</td>
</tr>
<tr>
<td>%n</td>
<td>Malware category name, if available</td>
<td>No</td>
</tr>
<tr>
<td>%N</td>
<td>Malware threat name, if available</td>
<td>No</td>
</tr>
<tr>
<td>%o</td>
<td>Web reputation threat type, if available</td>
<td>No</td>
</tr>
<tr>
<td>%O</td>
<td>Web reputation threat reason, if available</td>
<td>No</td>
</tr>
<tr>
<td>%p</td>
<td>String for the Proxy-Connection HTTP header</td>
<td>Yes</td>
</tr>
<tr>
<td>%P</td>
<td>Protocol</td>
<td>Yes</td>
</tr>
<tr>
<td>%q</td>
<td>Identity policy group name</td>
<td>Yes</td>
</tr>
<tr>
<td>%Q</td>
<td>Policy group name for non-Identity policies</td>
<td>Yes</td>
</tr>
<tr>
<td>%r</td>
<td>Redirect URL</td>
<td>No</td>
</tr>
<tr>
<td>%R</td>
<td>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. For more information, see Using Variables in Customized IronPort Notification Pages, page 15-13. For more information on re-authentication, see Allowing Users to Re-Authenticate, page 20-39.</td>
<td>No</td>
</tr>
<tr>
<td>%S</td>
<td>The signature of the proxy</td>
<td>No, always evaluates to FALSE</td>
</tr>
</tbody>
</table>
Working With IronPort End-User Notification Pages

To edit the IronPort Notification pages:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Always Evaluates to TRUE if Used as Conditional Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>%t</td>
<td>Timestamp in Unix seconds plus milliseconds</td>
<td>Yes</td>
</tr>
<tr>
<td>%T</td>
<td>The date</td>
<td>Yes</td>
</tr>
<tr>
<td>%u</td>
<td>The URI part of the URL (the URL excluding the server name)</td>
<td>Yes</td>
</tr>
<tr>
<td>%U</td>
<td>The full URL of the request</td>
<td>Yes</td>
</tr>
<tr>
<td>%v</td>
<td>HTTP protocol version</td>
<td>Yes</td>
</tr>
<tr>
<td>%W</td>
<td>Management WebUI port</td>
<td>Yes</td>
</tr>
<tr>
<td>%X</td>
<td>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.</td>
<td>Yes</td>
</tr>
<tr>
<td>%Y</td>
<td>Administrator custom text string, if set, else empty</td>
<td>No</td>
</tr>
<tr>
<td>%y</td>
<td>End-user acknowledgement page custom text</td>
<td>Yes</td>
</tr>
<tr>
<td>%z</td>
<td>Web reputation score</td>
<td>Yes</td>
</tr>
<tr>
<td>%Z</td>
<td>DLP metadata</td>
<td>Yes</td>
</tr>
<tr>
<td>%%</td>
<td>Prints the percent symbol (%) in the notification page</td>
<td>N/A</td>
</tr>
</tbody>
</table>

To edit the IronPort Notification pages:

**Step 1**  Use an FTP client to connect to the Web Security appliance.

**Step 2**  Navigate to the `configuration\eun` directory.

In this directory are subdirectories for each supported language for end-user notification pages.
Step 3  Download the language directory files for the IronPort notification pages you want to edit.

Step 4  On your local machine, use a text or HTML editor to edit each HTML file for the IronPort notification pages.

   For a list of rules and guidelines, see Rules and Guidelines for Editing IronPort Notification Pages, page 15-12.

Step 5  Use the FTP client to upload the customized HTML files to the same directory from which you downloaded them in step 3.

Step 6  Open an SSH client and connect to the Web Security appliance.

Step 7  Run the `advancedproxyconfig > EUN` CLI command.

Step 8  Type 2 to use the custom end-user notification pages.

Note  If the custom end-user notification pages option is currently enabled when you update the HTML files, you must type 1 to refresh the custom end-user notification pages. If you do not do this, the new files do not take effect until the Web Proxy restarts.

Step 9  Commit your change, and close the SSH client.

Rules and Guidelines for Editing IronPort Notification Pages

Use the following rules and guidelines when editing IronPort notification pages:

- Each customized IronPort notification page file must be a valid HTML file. For a list of HTML tags you can include, see Supported HTML Tags in Notification Pages, page 15-23.

- The customized IronPort notification page file names must exactly match the file names shipped with the Web Security appliance.

- Do not include any links to URLs in the HTML files. Any link included in the notification pages are subject to the access control rules defined in the Access Policies and users might end up in a recursive loop.

- If the configuration's eun directory does not contain a particular file with the required name, then the appliance displays the standard IronPort notification page.
For new IronPort notification pages to go into effect, you must first upload the customized files to the appliance and then enable the customized files using the `advancedproxyconfig > miscellaneous` CLI command.

### Using Variables in Customized IronPort Notification Pages

When editing IronPort notification pages, you can include conditional variables to create if-then statements to take different actions depending on the current state. For example, you can create an IronPort notification page that includes a redirect URL (%r) if re-authentication is offered (%R). In this example, you would create a conditional variable out of %R.

Table 15-3 describes the different conditional variable formats.

<table>
<thead>
<tr>
<th>Conditional Variable Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%?V</td>
<td>This conditional variable evaluates to TRUE if the output of variable %V is not empty.</td>
</tr>
</tbody>
</table>
| %!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.

```html
<?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 Table 15-2, 'Variables for Customized End-User Notification Pages,' on page 9 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. For example, the %t variable (timestamp in Unix seconds plus milliseconds) always evaluates to TRUE, so there is little value in making an if-then statement based on it.

## Working with User Defined End-User Notification Pages

When you choose end-user notification pages defined by someone in your organization, 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.

AsyncOS passes the parameters to the web server as standard URL Parameters in the HTTP GET request. It uses the following format:

```html
<notification_page_url>?param1=value1&param2=value2
```
Table 15-4 describes the parameters AsyncOS includes in the query string.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Date and time of the transaction.</td>
</tr>
<tr>
<td>ID</td>
<td>Transaction ID.</td>
</tr>
<tr>
<td>Client_IP</td>
<td>IP address of the client.</td>
</tr>
<tr>
<td>User</td>
<td>Username of the client making the request, if available.</td>
</tr>
<tr>
<td>Site</td>
<td>Hostname of the destination in the HTTP request.</td>
</tr>
<tr>
<td>URI</td>
<td>URL path specified in the HTTP request.</td>
</tr>
<tr>
<td>Status_Code</td>
<td>HTTP status code for the request.</td>
</tr>
<tr>
<td>Decision_Tag</td>
<td>ACL decision tag as defined in the Access Log entry that indicates how the DVS engine handled the transaction. For more information about ACL decision tags, see ACL Decision Tags, page 24-24.</td>
</tr>
<tr>
<td>URL_Cat</td>
<td>URL category that the URL filtering engine assigned to the transaction request. For a list of the different URL categories, see URL Category Descriptions, page 16-32. Note: AsyncOS for Web sends the entire URL category name for both predefined and user defined URL categories. It performs URL encoding on the category name, so spaces are written as “%20”.</td>
</tr>
<tr>
<td>WBRS</td>
<td>WBRS score that the Web Reputation Filters assigned to the URL in the request.</td>
</tr>
<tr>
<td>DVS_Verdict</td>
<td>Malware category that the DVS engine assigns to the transaction. For more information about malware categories, Malware Scanning Verdict Values, page 24-52.</td>
</tr>
</tbody>
</table>
AsyncOS always includes all parameters in each redirected URL. If no value exists for a particular parameter, AsyncOS passes a hyphen (-).

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.

Consider the following rules and guidelines when entering the custom URL:

- You can use any HTTP or HTTPS URL.

<table>
<thead>
<tr>
<th>DVS_ThreatName</th>
<th>The name of the malware found by the DVS engine.</th>
</tr>
</thead>
</table>
| 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 Reauth_URL 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. For more information, see Allowing Users to Re-Authenticate, page 20-39. |

For more information, see Allowing Users to Re-Authenticate, page 20-39.
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_sprrt,-,-,-,-,-,-,-,-,-,-,-,-,-,-,IW_sprrt,-> -
```

Then AsyncOS creates the following redirected URL:

```
```

To configure user defined end-user notification pages:

Navigate to the Security Services > End-User Notification page, and click **Edit Settings**.

The Edit End-User Notification page appears.

From the Notification Type field, choose Redirect to Custom URL.

In the Notification Page URL field, enter the URL to which you want to redirect blocked websites.
You can choose whether or not to preview the URL you enter by clicking the Preview Custom URL link.

Submit and commit your changes.

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 acknowledgement page when a user first accesses a browser after a certain period of time. When the end-user acknowledgement page appears, users must click a link to access the original site requested or any other website.

You might want to use an end-user acknowledgement page to force users to explicitly agree to the terms and conditions for browsing the World Wide Web from the organization’s network. This might be useful when the Web Proxy is in transparent mode because web users will not otherwise know that their web transactions are being filtered and monitored for security purposes.

When you configure the appliance to display an end-user acknowledgement page, it does so for every user accessing the web using HTTP or HTTPS. It displays the end-user acknowledgement page when a user tries to access a website for the first time, or after a configured time interval.

Native FTP transactions are exempt from the end-user acknowledgement page.

Users are tracked by username if authentication has made a username available, and tracked by IP address if no username is available.

When you enable the end-user acknowledgement page, you can configure the following settings:

**Time Between Acknowledgements.** The Time Between Acknowledgements determines how often the Web Proxy displays the end-user acknowledgement page for each user. Once a user clicks the link on the end-user acknowledgement page, the Web Proxy considers that user to have acknowledged the proxy for the time you enter for the Time Between
Acknowledgements. This setting applies to users tracked by username and users tracked by IP address. You can specify any value from 30 to 2678400 seconds (one month). Default is 1 day (86400 seconds).

Inactivity Timeout. The Inactivity Timeout determines how long a user tracked and acknowledged by IP address (unauthenticated users only) can be idle before the user is no longer considered acknowledged. You can specify any value from 30 to 2678400 seconds (one month). Default is four hours (14400 seconds).

Custom message. The custom message is text you enter that appears on every end-user acknowledgement page. You can include some simple HTML tags to format the text. For example, you can change the color and size of the text, or make it italicized. See Custom Text in Notification Pages, page 15-23 for more information.

You can only include a custom message when you configure the end-user acknowledgement page in the web interface, versus the CLI.

Consider the following rules and guidelines when enabling the end-user acknowledgement 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 acknowledgement page again.

The first transaction from a user must be an HTTP request, and the user must agree to the terms for all transactions to succeed. If users try to send an HTTPS or native FTP request before an HTTP request, the HTTPS or native FTP request fails.

When the Web Proxy restarts, the Web Proxy considers all users to have timed out, and it displays the end-user acknowledgement page again. The Web Proxy may restart based on different events, such as when the Default Proxy Log subscription changes or when changes are made to the global authentication settings or FTP Proxy settings.

When the appliance is deployed in explicit forward mode and a user goes to an HTTPS site, the end-user acknowledgement 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.
You can enable and configure the end-user acknowledgement page in the web interface or the command line interface. However, when you configure the end-user acknowledgement page in the web interface, you can include a custom message that appears on each page. You can include some simple HTML tags in the custom message, such as font color and size.

In the CLI, use advancedproxyconfig > authentication.

To configure the end-user acknowledgement page in the web interface:

Navigate to the Security Services > End-User Notification page.
Click Edit Settings.

**Edit End-User Notification**

**General Settings**

<table>
<thead>
<tr>
<th>Language</th>
<th>English</th>
</tr>
</thead>
</table>

**Logo Image:** Optionally, an image can be displayed by the web browser as part of every notification page.

- No Image
- Use Safari Logo
- Use Custom Logo:
  
  ![Image](http://example.com/image.png)

**End-User Acknowledgement Page**

**End-user Acknowledgement:**

- Require end-user to click through acknowledgement page

  - Time between Acknowledgements:

    - 5

  - Inactivity Timeout:

    - 10 (in seconds, or use text: 2 for seconds, m for minutes, h for hours (examples: 120s, 3m 30s, 4h)

**Custom Message:**

Specifies additional text to be displayed on every notification page, such as a link to your company policies.

Simple HTML text formatting (such as bold or italic and links (anchor tags) are supported.

In the End-User Acknowledgement Page section, enable the “Require end-user to click through acknowledgement page” field. See Custom Text and Logos: Authentication, and End-User Acknowledgement Pages, page 15-24 for information about how this feature works with custom messages.
In the Time Between Acknowledgements field, enter the time interval the appliance uses between displaying the end-user acknowledgement page.

You can specify any value from 30 to 2678400 seconds (one month). Default is 1 day (86400 seconds). You can enter the value in seconds, minutes, or days. Use ‘s’ for seconds, ‘m’ for minutes, and ‘d’ for days.

In the Inactivity Timeout field, enter the maximum IP address idle timeout.

You can specify any value from 30 to 2678400 seconds (one month). Default is four hours (14400 seconds). You can enter the value in seconds, minutes, or days. Use ‘s’ for seconds, ‘m’ for minutes, and ‘d’ for days.

In the Custom Message field, enter any text you want to appear on every end-user acknowledgement page.

You can include some HTML tags in lower case to format the text. For a list of supported HTML tags, see Supported HTML Tags in Notification Pages, page 15-23.

For example:

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

Click the “Preview Acknowledgment Page Customization” link to view the current end-user acknowledgement page in a separate browser window.

Submit and commit your changes.

You can configure the end-user URL filtering warning page on the Security Services > End-User Notification page. You can include some simple HTML tags in the custom message, such as font color and size.

To configure the end-user URL filtering warning page:

Navigate to the Security Services > End-User Notification page, and click Edit Settings.

Scroll down to the End-User URL Filtering Warning Page section.
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.

Once a user clicks the continue link on the end-user URL filtering warning page, the Web Proxy considers that user to have acknowledged the warning for the time you enter here. This setting applies to users tracked by username and users tracked by IP address.

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.

In the Custom Message field, enter any text you want to appear on every end-user URL filtering warning page.

You might want to include text for the organization’s acceptable use policies, or include a link to a page that details the acceptable use policies.

You can include some HTML tags in lower case to format the text. For a list of supported HTML tags, see Supported HTML Tags in Notification Pages, page 15-23.

For example:

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

Click the “Preview URL Category Warning Page Customization” link to view the current end-user URL filtering warning page in a separate browser window.

Submit and commit your changes.
The FTP Proxy displays a predefined notification message to native FTP clients when there is an error with FTP Proxy authentication. You can customize this FTP notification with a custom message.

To configure IronPort FTP notification messages:

- Navigate to the Security Services > End-User Notification page, and click **Edit Settings**.
- Scroll down to the Native FTP section.
- In the Language field, select the language to use when displaying native FTP notification messages.
- In the Custom Message field, enter the text you want to display in every native FTP notification message.
- Submit and commit your changes.

The following sections apply to custom text entered for IronPort notification and end-user acknowledgement pages.

You can format the text in IronPort notification and end-user acknowledgement pages using some HTML tags. Tags must be in lower case and follow standard HTML syntax (closing tags, etc.).

You can use the following HTML tags:

- `<a></a>`
- `<span></span>`
- `<b></b>`
- `<big></big>`
- `<br>`
For example, you can make some text italic:

Please acknowledge the following statements *before* 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 *before* accessing the Internet.

**Custom Text and Logos: Authentication, and End-User Acknowledgement Pages**

All combinations of URL paths and domain names in embedded links within custom text and the custom logo in IronPort notification, end-user acknowledgement, and end-user URL filtering warning pages are exempted from the following:

- User authentication
- End-user acknowledgment
- All scanning, such as malware scanning and web reputation scoring

For example, if the following URLs are embedded in custom text:

http://www.example.com/index.html
http://www.mycompany.com/logo.jpg

Then all of the following URLs will also be treated as exempt from all scanning:

http://www.example.com/index.html
http://www.mycompany.com/logo.jpg
http://www.example.com/logo.jpg
http://www.mycompany.com/index.html

Also, where an embedded URL is of the form:
<protocol>://<domain-name>/<directory path>/ then all sub-files and sub-directories under that directory path on the host will also be exempted from all scanning.

For example, if the following URL is embedded:
http://www.example.com/gallery2/ URLs such as
http://www.example.com/gallery2/main.php will also be treated as exempt.

This allows administrators to create a more sophisticated page with embedded content so long as the embedded content is relative to the initial URL. However, you administrators should also take care when deciding which paths to include as links and custom logos.

Notification Page Types

Users accessing the Internet sometimes cannot access the server they want. By default, the Web Proxy displays a notification page informing users they were blocked and the reason for the block. This section lists and describes all possible notification pages a user might see while accessing the Internet.

Possible reasons that cause notification pages to appear include the following:

- IronPort notification pages are enabled and the user accessed the Internet in a way that violated an Access Policy.
- IronPort notification pages are configured to allow end-users to report misclassified pages to IronPort and the user reported a misclassified page.
- The end-user acknowledgement page is enabled and the user accessed the Internet for the first time since the timeout period expired.
- The HTTPS Proxy is enabled and the appliance is configured to drop HTTPS requests to servers with invalid certificates.
- The Web Security appliance could not access the server requested due to an external error, such as DNS failure or an unavailable server.
Most notification pages display a different set of codes that may help administrators or IronPort Customer Support troubleshoot any potential problem. Some codes are for IronPort 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 Table 15-2 on page 9.

Table 15-5 describes the different notification pages users might encounter.

<table>
<thead>
<tr>
<th>File Name and Notification Title</th>
<th>Notification Text</th>
<th>Notification Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR_ACCEPTED Feedback Accepted, Thank You</td>
<td>The misclassification report has been sent. Thank you for your feedback.</td>
<td>N/A</td>
</tr>
<tr>
<td>ERR_ACCESS_FORBIDDEN Access Forbidden</td>
<td>Based on your corporate Access Policies, this web site &lt;URL&gt; has been blocked because it has been determined to be a security threat to your computer or the corporate network. Access could also be blocked because this request came from an unrecognized or unauthorized machine.</td>
<td>&lt;version&gt;, ACCESS_FORBIDDEN, %B, %N, %i, %t, %X, %U</td>
</tr>
<tr>
<td>ERR_ADULT_CONTENT Policy Acknowledgement</td>
<td>You are trying to visit a web page whose content are rated as explicit or adult. By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content. Data about your browsing behavior may be monitored and recorded. You will be periodically asked to acknowledge this statement for continued access to this kind of web page. Click here to accept this statement and access the Internet.</td>
<td>N/A</td>
</tr>
<tr>
<td>ERR_AUTH Policy: Authentication</td>
<td>Based on your corporate Access Policies, Internet access has been blocked because the login provided belongs to a user or group that is not allowed Internet access.</td>
<td>&lt;version&gt;, AUTH, %B</td>
</tr>
</tbody>
</table>
## Chapter 15  Notifying End Users

### Notification Page Types

<table>
<thead>
<tr>
<th>Notification Title</th>
<th>Notification Text</th>
<th>Notification Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR_AVC Policy: Application Controls</td>
<td>Based on your corporate access policies, access to application %1 of type %2 has been blocked.</td>
<td>&lt;version&gt;, AVC, %B, %i, %t, %X, %U</td>
</tr>
<tr>
<td>ERR_BAD_REQUEST Bad Request</td>
<td>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.</td>
<td>&lt;version&gt;, BAD_REQUEST</td>
</tr>
<tr>
<td>ERR_BLOCK_DEST Policy: Destination</td>
<td>Based on your corporate Access Policies, access to this web site &lt;URL&gt; has been blocked.</td>
<td>&lt;version&gt;, BLOCK_DEST, %B, %U</td>
</tr>
<tr>
<td>ERR_BLOCK_SRC Policy: Source</td>
<td>Based on your corporate Access Policies, access to this web site &lt;URL&gt; has been blocked because this request came from an unauthorized computer.</td>
<td>&lt;version&gt;, BLOCK_SRC, %B, %d, %U</td>
</tr>
<tr>
<td>ERR_BROWSER Security: Browser</td>
<td>Based on your corporate Access Policies, requests from your computer have been blocked because it has been determined to be a security threat to the corporate network. Your browser may have been compromised by a malware/spyware agent identified as &quot;&lt;malware name&gt;&quot;. Please contact &lt;contact name&gt; &lt;email address&gt; and provide the codes shown below. If you are using a non-standard browser and believe it has been misclassified, use the button below to report this misclassification.</td>
<td>&lt;version&gt;, BROWSER, %B, %b, %i, %t, %X, %U</td>
</tr>
<tr>
<td>ERR_BROWSER_CUSTOM Policy: Browser</td>
<td>Based on your corporate Access Policies, requests from your browser have been blocked. This browser &quot;&lt;browser type&gt;&quot; is not permitted due to potential security risks.</td>
<td>&lt;version&gt;, BROWSER_CUSTOM, %B, %b, %i, %t, %U</td>
</tr>
</tbody>
</table>
### Notification Page Types

<table>
<thead>
<tr>
<th>File Name and Notification Title</th>
<th>Notification Text</th>
<th>Notification Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR_CERT_INVALID</td>
<td>A secure session cannot be established because the site <code>&lt;hostname&gt;</code> provided an invalid certificate.</td>
<td><code>&lt;version&gt;</code>, INVALID_CERT, %B, %i, %t, %X, %U</td>
</tr>
<tr>
<td>ERR_CONTINUE_UNACKNOWLEDGED</td>
<td>You are trying to visit a web page that falls under the URL Category <code>%g</code>. By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content. Data about your browsing behavior may be monitored and recorded. You will be periodically asked to acknowledge this statement for continued access to this kind of web page. Click here to accept this statement and access the Internet.</td>
<td>N/A</td>
</tr>
<tr>
<td>ERR_DNS_FAIL</td>
<td>The hostname resolution (DNS lookup) for this hostname <code>&lt;hostname&gt;</code> has failed. The Internet address may be misspelled or obsolete, the host <code>&lt;hostname&gt;</code> may be temporarily unavailable, or the DNS server may be unresponsive. Please check the spelling of the Internet address entered. If it is correct, try this request later.</td>
<td><code>&lt;version&gt;</code>, DNS_FAIL, %H</td>
</tr>
<tr>
<td>ERR_EXPECTATION_FAILED</td>
<td>The system cannot process the request for this site <code>&lt;URL&gt;</code>. A non-standard browser may have generated an invalid HTTP request. If using a standard browser, please retry the request.</td>
<td><code>&lt;version&gt;</code>, EXPECTATION_FAILED, %U</td>
</tr>
<tr>
<td>ERR_FILE_SIZE</td>
<td>Based on your corporate Access Policies, access to this web site or download <code>&lt;URL&gt;</code> has been blocked because the download size exceeds the allowed limit.</td>
<td><code>&lt;version&gt;</code>, FILE_SIZE, %B, %U</td>
</tr>
</tbody>
</table>
### Notification Page Types

<table>
<thead>
<tr>
<th>File Name and Notification Title</th>
<th>Notification Text</th>
<th>Notification Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR_FILE_TYPE</td>
<td>Based on your corporate Access Policies, access to this web site or download <code>&lt;URL&gt;</code> has been blocked because the file type “&lt;file type&gt;” is not allowed.</td>
<td>&lt;version&gt;, FILE_TYPE, %B, %K, %U</td>
</tr>
<tr>
<td>ERR_FILTER_FAILURE</td>
<td>The request for page <code>&lt;URL&gt;</code> has been denied because an internal server is currently unreachable or overloaded. Please retry the request later.</td>
<td>&lt;version&gt;, FILTER_FAILURE, %U</td>
</tr>
<tr>
<td>ERR_FOUND</td>
<td>The page <code>&lt;URL&gt;</code> is being redirected to <code>&lt;redirected URL&gt;</code>.</td>
<td>&lt;version&gt;, FOUND, %r, %U</td>
</tr>
<tr>
<td>ERR_FTP_ABORTED</td>
<td>The request for the file <code>&lt;URL&gt;</code> did not succeed. The FTP server <code>&lt;hostname&gt;</code> unexpectedly terminated the connection. Please retry the request later.</td>
<td>&lt;version&gt;, FTP_ABORTED, %U</td>
</tr>
<tr>
<td>ERR_FTP_AUTH_REQUIRED</td>
<td>Authentication is required by the FTP server <code>&lt;hostname&gt;</code>. A valid user ID and password must be entered when prompted. In some cases, the FTP server may limit the number of anonymous connections. If you usually connect to this server as an anonymous user, please try again later.</td>
<td>&lt;version&gt;, FTP_AUTH_REQUIRED, %H</td>
</tr>
<tr>
<td>ERR_FTP_CONNECTION_FAILED</td>
<td>The system cannot communicate with the FTP server <code>&lt;hostname&gt;</code>. 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.</td>
<td>&lt;version&gt;, FTP_CONNECTION FAILED, %H</td>
</tr>
<tr>
<td>ERR_FTP_FORBIDDEN</td>
<td>Access was denied by the FTP server <code>&lt;hostname&gt;</code>. Your user ID does not have permission to access this document.</td>
<td>&lt;version&gt;, FTP_FORBIDDEN, %H</td>
</tr>
</tbody>
</table>
## Notification Page Types

<table>
<thead>
<tr>
<th>File Name and Notification Title</th>
<th>Notification Text</th>
<th>Notification Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR_FTP_NOT_FOUN UND</td>
<td>The file <code>&lt;URL&gt;</code> could not be found. The address is either incorrect or obsolete.</td>
<td>&lt;version&gt;, FTP_NOT_FOUND, %U</td>
</tr>
<tr>
<td>FTP Not Found</td>
<td>The file <code>&lt;URL&gt;</code> could not be found. The address is either incorrect or obsolete.</td>
<td>&lt;version&gt;, FTP_NOT_FOUND, %U</td>
</tr>
<tr>
<td>ERR_FTP_SERVER _ERR</td>
<td>The system cannot communicate with the FTP server <code>&lt;hostname&gt;</code>. 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.</td>
<td>&lt;version&gt;, FTP_SERVER_ERR, %H</td>
</tr>
<tr>
<td>FTP Server Error</td>
<td>The system cannot communicate with the FTP server <code>&lt;hostname&gt;</code>. 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.</td>
<td>&lt;version&gt;, FTP_SERVER_ERR, %H</td>
</tr>
<tr>
<td>ERR_FTP_SERVICE _UNAVAIL</td>
<td>The system cannot communicate with the FTP server <code>&lt;hostname&gt;</code>. 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.</td>
<td>&lt;version&gt;, FTP_SERVICE_UNAVAIL, %H</td>
</tr>
<tr>
<td>FTP Service Unavailable</td>
<td>The system cannot communicate with the FTP server <code>&lt;hostname&gt;</code>. 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.</td>
<td>&lt;version&gt;, FTP_SERVICE_UNAVAIL, %H</td>
</tr>
<tr>
<td>ERR_GATEWAY_TIMEOUT</td>
<td>The system cannot communicate with the external server <code>&lt;hostname&gt;</code>. 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.</td>
<td>&lt;version&gt;, GATEWAY_TIMEOUT, %H</td>
</tr>
<tr>
<td>Gateway Timeout</td>
<td>The system cannot communicate with the external server <code>&lt;hostname&gt;</code>. 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.</td>
<td>&lt;version&gt;, GATEWAY_TIMEOUT, %H</td>
</tr>
<tr>
<td>ERR_IDS_ACCESS _FORBIDDEN</td>
<td>Based on your corporate data transfer policies, your upload request has been blocked. File details: <code>%Z</code></td>
<td>&lt;version&gt;, IDS_ACCESS_FORBIDDEN, %B, %N, %i, %t, %X, %U</td>
</tr>
<tr>
<td>File Name and Notification Title</td>
<td>Notification Text</td>
<td>Notification Codes</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ERR_INTERNAL_ERROR</td>
<td>Internal system error when processing the request for the page <code>&lt;URL&gt;</code>.</td>
<td><code>&lt;version&gt;, INTERNAL_ERROR, %U</code></td>
</tr>
<tr>
<td>Internal Error</td>
<td>Please retry this request.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If this condition persists, please contact <code>&lt;contact name&gt; &lt;email address&gt;</code> and provide the code shown below.</td>
<td></td>
</tr>
<tr>
<td>ERR_MALWARE_GENERAL</td>
<td>Based on your corporate Access Policies, this web site <code>&lt;URL&gt;</code> has been blocked because it has been determined to be a security threat to your computer or the corporate network. This web site has been associated with malware/spyware.</td>
<td><code>&lt;version&gt;, MALWARE_GENERAL, %B, %N, %i, %t, %X, %U</code></td>
</tr>
<tr>
<td>Security: Malware Risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERR_MALWARE_SPECIFIC</td>
<td>Based on your corporate Access Policies, this web site <code>&lt;URL&gt;</code> has been blocked because it has been determined to be a security threat to your computer or the corporate network. Malware <code>&lt;malware name&gt;</code> in the category <code>&lt;malware category&gt;</code> has been found on this site.</td>
<td><code>&lt;version&gt;, MALWARE_SPECIFIC, %B, %N, %i, %t, %X, %U</code></td>
</tr>
<tr>
<td>Security: Malware Detected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERR_MALWARE_SPECIFIC_OUTGOING</td>
<td>Based on your corporate policy, the upload of the file to URL (%U) has been blocked because the file was detected to contain malware that will be harmful to the receiving end's network security. Malware Name: %N Malware Category: %n</td>
<td><code>&lt;version&gt;, MALWARE_SPECIFIC_OUTGOING, %B, %N, %i, %t, %X, %U</code></td>
</tr>
<tr>
<td>Security: Malware Detected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERR_MISS_ACCESS_FORBIDDEN</td>
<td>This web site <code>&lt;URL&gt;</code> has been blocked because it has been determined to be a security threat, based on your corporate Access Policies.</td>
<td><code>&lt;version&gt;, MISS_ACCESS_FORBIDDEN, %U</code></td>
</tr>
</tbody>
</table>
### Notification Page Types

<table>
<thead>
<tr>
<th>File Name and Notification Title</th>
<th>Notification Text</th>
<th>Notification Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR_NO_MORE_FORWARDS</td>
<td>The request for the page <code>&lt;URL&gt;</code> failed. The server address <code>&lt;hostname&gt;</code> may be invalid, or you may need to specify a port number to access this server.</td>
<td><code>&lt;version&gt;</code>, NO_MORE_FORWARDS, %U</td>
</tr>
<tr>
<td>No More Forwards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERR_ONLY_IF_CACHED_NOT_IN_CACHE</td>
<td>The page <code>&lt;URL&gt;</code> has been blocked based on your corporate policies.</td>
<td><code>&lt;version&gt;</code>, ONLY_IF_CACHED_NOT_IN_CACHE, %U</td>
</tr>
<tr>
<td>Only if Cached But Not in Cache</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERR_POLICY</td>
<td>Based on your corporate Access Policies, access to this web site <code>&lt;URL&gt;</code> has been blocked.</td>
<td><code>&lt;version&gt;</code>, POLICY, %B, %i, %t, %X, %U</td>
</tr>
<tr>
<td>Policy: General</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERR_PROTOCOL</td>
<td>Based on your corporate Access Policies, this request has been blocked because the data transfer protocol &quot;&lt;protocol type&gt;&quot; is not allowed.</td>
<td><code>&lt;version&gt;</code>, PROTOCOL, %B, %P, %i, %t, %U</td>
</tr>
<tr>
<td>Policy: Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERR_PROXY_AUTH_REQUIRED</td>
<td>Authentication is required to access the Internet using this system. A valid user ID and password must be entered when prompted.</td>
<td><code>&lt;version&gt;</code>, PROXY_AUTH_REQUIRED</td>
</tr>
<tr>
<td>Proxy Authorization Required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERR_PROXY_PREVENT_MULTIPLE_LOGIN</td>
<td>Based on your corporate policies, the request to access the Internet was denied because this user ID has an active session from another IP address. If you want to login as a different user, click on the button below and enter a different a user name and password.</td>
<td><code>&lt;version&gt;</code>, PROXY_PREVENT_MULTIPLE_LOGIN</td>
</tr>
<tr>
<td>Already Logged In From Another Machine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERR_PROXY_REDIRECT</td>
<td>This request is being redirected. If this page does not automatically redirect, click here to proceed.</td>
<td>N/A</td>
</tr>
<tr>
<td>Redirect</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 15 Notifying End Users

#### Notification Page Types

<table>
<thead>
<tr>
<th>File Name and Notification Title</th>
<th>Notification Text</th>
<th>Notification Codes</th>
</tr>
</thead>
</table>
| ERR_PROXY_UNACKNOWLEDGED Policy Acknowledgement | 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 corporate 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 corporate polices on Internet access.  
Click here to accept this statement and access the Internet. | N/A                                                   |
| ERR_PROXY_UNLICENSED Proxy Not Licensed | Internet access is not available without proper licensing of the security device.  
Please contact <contact name> <email address> and provide the code shown below.  
Note: To access the management interface of the security device, enter the configured IP address with port. | <version>, PROXY_UNLICENSED                              |
| ERR_RANGE_NOT_SATISFIABLE Range Not Satisfiable | 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.                                                                                      | <version>, RANGE_NOT_SATISFIABLE                         |
| ERR_REDIRECT_PERMANENT Redirect Permanent | The page <URL> is being redirected to <redirected URL>.                                                                                                   | <version>, REDIRECT_PERMANENT, %r, %U                   |
## Notification Page Types

<table>
<thead>
<tr>
<th>File Name and Notification Title</th>
<th>Notification Text</th>
<th>Notification Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR_REDIRECT_REPEAT_REQUEST</td>
<td>Please repeat your request.</td>
<td>&lt;version&gt;, REDIRECT_REPEAT_REQUEST</td>
</tr>
<tr>
<td>ERR_SAAS_AUTHENTICATION</td>
<td>Based on your corporate policy, the request to access %U 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.</td>
<td>N/A</td>
</tr>
<tr>
<td>ERR_SAAS_AUTHORIZATION</td>
<td>Based on your corporate policy, the access to the SaaS application %U is blocked because you are not an authorized user. If you want to login as a different user, enter a different username and password for a user that is authorized to access this application.</td>
<td>N/A</td>
</tr>
<tr>
<td>ERR_SAML_PROCESSING</td>
<td>The request to access %s did not go through because errors were found during the process of the single sign on request.</td>
<td>N/A</td>
</tr>
<tr>
<td>ERR_SERVER_NAME_EXPANSION</td>
<td>The server name &lt;hostname&gt; appears to be an abbreviation, and is being redirected to &lt;redirected URL&gt;.</td>
<td>&lt;version&gt;, SERVER_NAME_EXPANSION, %r, %H</td>
</tr>
<tr>
<td>ERR_SOCKS_FAIL</td>
<td>The server name &lt;hostname&gt; could not be processed while retrieving the page &lt;URL&gt;. This could be due to a problem communicating with the external server.</td>
<td>&lt;version&gt;, SOCKS_FAIL, %U</td>
</tr>
<tr>
<td>ERR_URI_TOO_LONG</td>
<td>The requested URL was too long and could not be processed. This may represent an attack on your network. Please contact &lt;contact name&gt; &lt;email address&gt; and provide the code shown below.</td>
<td>&lt;version&gt;, URI_TOO_LONG</td>
</tr>
</tbody>
</table>
### Notification Page Types

<table>
<thead>
<tr>
<th>File Name and Notification Title</th>
<th>Notification Text</th>
<th>Notification Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR_WBRS</td>
<td>Based on your corporate access policies, this web site %U has been blocked because it has been determined by Web Reputation Filters to be a security threat to your computer or the corporate network. This web site has been associated with malware/spyware. Threat Type: %o Threat Reason: %O</td>
<td>&lt;version&gt;, MALWARE, %o, %O, %B, %i, %t, %X, %U</td>
</tr>
<tr>
<td>ERR_WEBCAT</td>
<td>Based on your corporate Access Policies, access to this web site &lt;URL&gt; has been blocked because the web category “&lt;category type&gt;” is not allowed.</td>
<td>&lt;version&gt;, WEBCAT, %B, %i, %t, %X, %U</td>
</tr>
<tr>
<td>ERR_WWW_AUTH_REQUIRED</td>
<td>Authentication is required to access the requested web site &lt;hostname&gt;. A valid user ID and password must be entered when prompted.</td>
<td>&lt;version&gt;, WWW_AUTH_REQUIRED, %H</td>
</tr>
</tbody>
</table>

Cisco IronPort AsyncOS 7.1 for Web User Guide

OL-23207-01

15-35
URL Filters Overview

AsyncOS for Web allows administrators to control user access based on the web server category of a particular HTTP or HTTPS request. For example, you can block all HTTP requests for gambling web sites, or you can decrypt all HTTPS requests for web-based email websites.
Using policy groups, you can create secure policies that control access to web sites containing objectionable or questionable content. The sites that are actually blocked, dropped, allowed, or decrypted depend on the categories you select when setting up category blocking for each policy group.

To control user access based on a URL category, you must enable one of the following URL filtering engines:

- **Cisco IronPort Web Usage Controls.** This is a multi-layered URL filtering engine that uses domain prefixes and keyword analysis to categorize URLs, and real-time response content analysis using the Dynamic Content Analysis engine if no category is determined by prefixes and keywords. It includes over 65 predefined URL categories. This engine also allows end users and administrators to report to IronPort any miscategorized URLs as well as uncategorized URLs for future inclusion in the categorization database.

  For more information, see Dynamic Content Analysis Engine, page 16-3.

- **IronPort URL Filters.** This URL filtering engine categorizes URLs in the client request using domains stored in a database. It includes more than 50 predefined URL categories, and allows end users and administrators to report to IronPort any uncategorized URLs.

You can use URL categories when performing the following tasks:

- **Define policy group membership.** You can define policy group membership by the URL category of the request URL.

- **Control access to HTTP, HTTPS, and FTP requests.** You can choose to allow or block HTTP and FTP requests by URL category using Access Policies, and you can choose to pass through, drop, or decrypt HTTPS requests by URL category using Decryption Policies. You can also choose whether or not to block upload requests by URL category using IronPort Data Security Policies. For more information, see Filtering Transactions Using URL Categories, page 16-6.

In addition to the predefined URL categories included with the URL filtering engine, you can create user defined custom URL categories that specify specific hostnames and IP addresses. For more information, see Custom URL Categories, page 16-16.
Dynamic Content Analysis Engine

The Dynamic Content Analysis engine is a scanning engine called at response
time to categorize a transaction that failed categorization using only the URL in
the client request. You might want to enable Dynamic Content Analysis when
your organization’s traffic visits more of the newer, and therefore not yet
categorized, sites on the Internet.

Enable the Dynamic Content Analysis engine when you enable Cisco IronPort
Web Usage Controls on the Security Services > Acceptable Use Controls page.

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

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

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

It is possible for an Access Policy, or an Identity used in an Access Policy, to
define policy membership by a predefined URL category and for the Access
Policy to perform an action on the same URL category. In this case, it is also
possible for the URL in the request to be uncategorized when determining Identity
and Access Policy group membership, but to be categorized by the Dynamic
Content Analysis engine after receiving the server response. In this scenario,
Cisco IronPort Web Usage Controls ignores the category verdict from the
Dynamic Content Analysis engine and the URL retains the “uncategorized”
verdict for the remainder of the transaction. However, future transactions still
benefit from the new category verdict.
Uncategorized URLs

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

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

All transactions resulting in unmatched categories are reported on the Reporting > URL Categories page as “Uncategorized URLs.” A large number of uncategorized URLs are generated from requests to web sites within the internal network. Because this type of internal transaction can falsely inflate reporting data and misrepresent the efficacy of the URL filtering engine, Cisco recommends using custom URL categories to group internal URLs and allow all requests to internal web sites. This decreases the number of web transactions reported as “Uncategorized URLs” and instead reports internal transactions as part of “URL Filtering Bypassed” statistics.

For more information, see Understanding Unfiltered and Uncategorized Data, page 16-28.

For more information about creating custom URL categories, see Custom URL Categories, page 16-16.

Matching URLs to URL Categories

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

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

For more information about uncategorized URLs, see Uncategorized URLs, page 16-4.
The URL Categories Database

The Web Security appliance collects information and maintains its own filtering categories database. The different URL filtering engines maintain separate databases. The filtering categories databases periodically receive updates from the IronPort update server (https://update-manifests.ironport.com). Server updates are automated, and the update interval is set by the server as opposed to the appliance. Updates to the database occur with a regular degree of frequency, and require no administrator intervention.

Cisco IronPort Web Usage Controls shares some database components with the Web Reputation Filters (WBRS) database. Because of this shared information, Cisco recommends fully participating in the SenderBase Network because it allows Cisco IronPort Web Usage Controls to validate and categorize all URLs dynamically classified by the Dynamic Content Analysis engine, including all URLs that could not otherwise be classified, improving overall efficacy.

For information about update intervals and the IronPort update server, see Manually Updating Security Service Components, page 26-51.

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

Configuring the URL Filtering Engine

To apply predefined category settings to policy groups and configure custom settings to manage web transactions, you must first enable and choose a URL filtering engine, either the Cisco IronPort Web Usage Controls URL filtering engine or the IronPort URL Filters. By default, the Cisco IronPort Web Usage Controls URL filtering engine is enabled in the System Setup Wizard.

When you enable URL filtering, you can choose the default action the Web Proxy should use when the URL filtering engine is unavailable, either monitor or block.

To configure the URL filtering engine:
Filtering Transactions Using URL Categories

Step 1  Navigate to the Security Services > Acceptable Use Controls page.

Step 2  Click Edit Global Settings.

The Edit Acceptable Use Controls Settings page appears.

Edit Acceptable Use Controls Settings

<table>
<thead>
<tr>
<th>Acceptable Use Controls Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>When Acceptable Use Controls service is enabled, a user could configure acceptable use policies based on URL filtering and more.</td>
</tr>
</tbody>
</table>

- Enable Acceptable Use Controls
  - IronPort URL Filters
  - Cisco IronPort Web Usage Controls
  - Enable Application Visibility and Control
  - Enable Dynamic Content Analysis Engine

<table>
<thead>
<tr>
<th>Default Action for Unreachable Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor</td>
</tr>
</tbody>
</table>

Step 3  Verify the Enable Acceptable Use Controls property is enabled.

Step 4  In the Acceptable Use Controls Service area, choose which URL filtering engine to enable, either IronPort URL Filters or Cisco IronPort Web Usage Controls.

Step 5  If you enable Cisco IronPort Web Usage Controls, choose whether or not to enable the Dynamic Content Analysis Engine.

  For more information on the Dynamic Content Analysis Engine, see Dynamic Content Analysis Engine, page 16-3.

Step 6  Choose the default action the Web Proxy should use when the URL filtering engine is unavailable, either Monitor or Block. Default is Monitor.

Step 7  Submit and commit your changes.

Filtering Transactions Using URL Categories

The URL filtering engine configured allows you to filter transactions in Access, Decryption, and Data Security Policies. To configure URL filtering in a policy group, click the link in the policies table under the URL Categories column for the policy group you want to edit. For more information about the policies table, see Using the Policies Tables, page 6-7.

When you configure URL categories for policy groups, you can configure actions for custom URL categories, if any are defined, and predefined URL categories. For more information about custom URL categories, see Custom URL Categories, page 16-16.
Filtering Transactions Using URL Categories

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

- **Decryption Policies.** See Configuring URL Filters for Decryption Policy Groups, page 16-10.

## Configuring URL Filters for Access Policy Groups

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

To configure URL filtering in an Access Policy group:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Navigate to the Web Security Manager &gt; Access Policies page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the link in the policies table under the URL Categories column for the policy group you want to edit.</td>
</tr>
</tbody>
</table>

Optionally, in the Custom URL Category Filtering section, you can add custom URL categories on which to take action in this policy:

a. Click Select Custom Categories.

The Select Custom Categories for this Policy dialog box appears.

b. Choose which custom URL categories to include in this policy and click Apply.

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

The custom URL categories included in the policy appear in the Custom URL Category Filtering section.
Step 4  In the Custom URL Category Filtering section, choose an action for each included custom URL category. Table 16-1 describes each action.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use Global Setting| Uses the action for this category in the Global Policy Group. This is the default action for user defined policy groups. Applies to user defined policy groups only.  
**Note:** When a custom URL category is excluded in the global Access Policy, then the default action for included custom URL categories in user defined Access Policies is Monitor instead of Use Global Settings. You cannot choose Use Global Settings when a custom URL category is excluded in the global Access Policy. |
| Redirect          | Redirects traffic originally destined for a URL in this category to a location you specify. When you choose this action, the Redirect To field appears. Enter a URL to which to redirect all traffic.  
For more information about redirecting traffic, see Redirecting Traffic, page 16-23. |
| Allow             | Always allows client requests for web sites in this category. Allowed requests bypass all further filtering and malware scanning.  
Only use this setting for trusted web sites. You might want to use this setting for internal sites. |
| Monitor           | The Web Proxy neither allows nor blocks the request. Instead, it continues to evaluate the client request against other policy group control settings, such as web reputation filtering. |
Filtering Transactions Using URL Categories

Chapter 16   URL Filters

Filtering Transactions Using URL Categories

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

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

See Table 16-1 for details on these actions.

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

Submit and commit your changes.

Configuring URL Filters for Decryption Policy Groups

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

To configure URL filtering in a Decryption Policy group:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warn</td>
<td>The Web Proxy initially blocks the request and displays a warning page, but allows the user to continue by clicking a hypertext link in the warning page. For more information, see Warning Users and Allowing Them to Continue, page 16-24.</td>
</tr>
<tr>
<td>Block</td>
<td>The Web Proxy denies transactions that match this setting.</td>
</tr>
<tr>
<td>Time-Based</td>
<td>The Web Proxy blocks or monitors the request during the time ranges you specify. For more information about creating time based URL filtering actions, see Creating Time Based URL Filters, page 16-26.</td>
</tr>
</tbody>
</table>
Step 1  Navigate to the Web Security Manager > Decryption Policies page.

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

The Decryption Policies: URL Categories: policymame page appears.

Decryption Policies: URL Categories: DecryptionPolicy1

Custom URL Category Filtering
No Custom Categories are included for this Policy.

Select Custom Categories

Cancel  Submit

Predefined URL Category Filtering
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

<table>
<thead>
<tr>
<th>Category</th>
<th>Use Global Settings</th>
<th>Pass Through</th>
<th>Monitor</th>
<th>Decrypt</th>
<th>Drop F7</th>
<th>Time Based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult</td>
<td>Select all</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adult</td>
<td>Select all</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advertising</td>
<td>Select all</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alcohol and Tobacco</td>
<td>Select all</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arts and Entertainment</td>
<td>Select all</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business and Industry</td>
<td>Select all</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

a.  Click Select Custom Categories.

The Select Custom Categories for this Policy dialog box appears.

Select Custom Categories for this Policy

<table>
<thead>
<tr>
<th>Category</th>
<th>Setting Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>partners</td>
<td>Use Global Setting (Exclude from policy)</td>
</tr>
<tr>
<td>intranet</td>
<td>Use Global Setting (Exclude from policy)</td>
</tr>
</tbody>
</table>

b.  Choose which custom URL categories to include in this policy and click Apply.

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

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

### Step 4
Choose an action for each custom and predefined URL category. Table 16-2 describes each action.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Global Setting</td>
<td>Uses the action for this category in the global Decryption Policy group. This is the default action for user defined policy groups. Applies to user defined policy groups only. When a custom URL category is excluded in the global Decryption Policy, then the default action for included custom URL categories in user defined Decryption Policies is Monitor instead of Use Global Settings. You cannot choose Use Global Settings when a custom URL category is excluded in the global Decryption Policy.</td>
</tr>
<tr>
<td>Pass Through</td>
<td>Passes through the connection between the client and the server without inspecting the traffic content. You might want to pass through connections to trusted secure sites, such as well known banking and financial institutions.</td>
</tr>
<tr>
<td>Monitor</td>
<td>The Web Proxy neither allows nor blocks the request. Instead, it continues to evaluate the client request against other policy group control settings, such as web reputation filtering.</td>
</tr>
</tbody>
</table>
Chapter 16      URL Filters

Filtering Transactions Using URL Categories

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

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrypt</td>
<td>Allows the connection, but inspects the traffic content. The appliance decrypts the traffic and applies Access Policies to the decrypted traffic as if it were a plaintext HTTP connection. By decrypting the connection and applying Access Policies, you can scan the traffic for malware. You might want to decrypt connections to third party email providers, such as gmail or hotmail. For more information about how the appliance decrypts HTTPS traffic, see Decrypting HTTPS Traffic, page 10-13.</td>
</tr>
<tr>
<td>Drop</td>
<td>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. You might want to drop connections to third party proxies that allow users on the network bypass the organization’s acceptable use policies.</td>
</tr>
</tbody>
</table>

Step 5  In the Uncategorized URLs section, choose the action to take for client requests to web sites that do not fall into a predefined or custom URL category. You can choose any action listed in Table 16-2.

Step 6  Submit and commit your changes.

Configuring URL Filters for Data Security Policy Groups

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

To configure URL filtering in a Data Security Policy group:

Step 1  Navigate to the Web Security Manager > IronPort Data Security page.
Step 2  Click the link in the policies table under the URL Categories column for the policy group you want to edit.


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

a. Click Select Custom Categories.

The Select Custom Categories for this Policy dialog box appears.

b. Choose which custom URL categories to include in this policy and click Apply.

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

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

### Custom URL Category Filtering

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Global Setting</td>
<td>Uses the action for this category in the Global Policy Group. This is the default action for user defined policy groups. Applies to user defined policy groups only. When a custom URL category is excluded in the global IronPort Data Security Policy, then the default action for included custom URL categories in user defined IronPort Data Security Policies is Monitor instead of Use Global Settings. You cannot choose Use Global Settings when a custom URL category is excluded in the global IronPort Data Security Policy.</td>
</tr>
<tr>
<td>Allow</td>
<td>Always allows upload requests for web sites in this category. Applies to custom URL categories only. Allowed requests bypass all further data security scanning and the request is evaluated against Access Policies. Only use this setting for trusted web sites. You might want to use this setting for internal sites.</td>
</tr>
</tbody>
</table>

**Step 4** In the Custom URL Category Filtering section, choose an action for each custom URL category. Table 16-3 describes each action.
Chapter 16      URL Filters

Custom URL Categories

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

- Use Global Settings
- Monitor
- Block

See Table 16-3 for details on these actions.

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

Submit and commit your changes.

Custom URL Categories

The Web Security appliance ships with many predefined URL categories by default, such as Web-based Email and more. However, you can also create user defined custom URL categories that specify specific hostnames and IP addresses. You might want to create custom URL categories for internal sites or a group of external sites you know you can trust.

Create, edit, and delete custom URL categories on the Web Security Manager > Custom URL Categories page.
Chapter 16      URL Filters

Custom URL Categories

21-21

Edit custom URL category. Delete custom URL category.

Add a custom URL category.

Note

The Web Security appliance uses the first four characters of custom URL category names preceded by “c_” in the access logs. Consider the custom URL category name if you use Sawmill for IronPort to parse the access logs. If the first four characters of the custom URL category include a space, Sawmill for IronPort cannot properly parse the access log entry. Instead, only use supported characters in the first four characters if you will use Sawmill for IronPort to parse the access logs. If you want to include the full name of a custom URL category in the access logs, add the %XF format specifier to the access logs. For more information on how to do this, see Custom Formatting in Access Logs and W3C Logs, page 24-39.

It is possible to create multiple custom URL categories and include the same URL in each category. The order of the custom URL categories matters. Categories listed higher in the list take priority over categories listed lower. When you include these custom URL categories in the same Access, Decryption, or IronPort Data Security Policy group and define different actions to each category, the action of the higher included custom URL category takes effect.

To create or edit a custom URL category:

Step 1  Navigate to the Web Security Manager > Custom URL Categories page.

Step 2  To create a custom URL category, click Add Custom Category. To edit an existing custom URL category, click the name of the URL category.
Step 3 Enter the settings in Table 16-4 for the custom URL category.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category Name</td>
<td>Enter a name for the URL category. This name appears when you configure URL filtering for policy groups.</td>
</tr>
<tr>
<td>List Order</td>
<td>Choose the order in the list of custom URL categories to place this category. Enter &quot;1&quot; for the topmost URL category. The URL filtering engine evaluates a client request against the custom URL categories in the order specified.</td>
</tr>
</tbody>
</table>
Chapter 16      URL Filters

Custom URL Categories

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sites</td>
<td>Enter one or more addresses that belong in the custom category.</td>
</tr>
<tr>
<td></td>
<td>You can enter multiple addresses separated by line breaks or commas. You can enter addresses using any of the following formats:</td>
</tr>
<tr>
<td></td>
<td>• IP address, such as 10.1.1.0</td>
</tr>
<tr>
<td></td>
<td>• CIDR address, such as 10.1.1.0/24</td>
</tr>
<tr>
<td></td>
<td>• Domain name, such as example.com</td>
</tr>
<tr>
<td></td>
<td>• Hostname, such as crm.example.com</td>
</tr>
<tr>
<td></td>
<td>• Partial hostname, such as .example.com</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Entering a partial hostname, such as .example.com, also matches <a href="http://www.example.com">www.example.com</a>.</td>
</tr>
</tbody>
</table>

| Advanced: Regular Expressions | You can use regular expressions to specify multiple web servers that match the pattern you enter.                                           |
|                              | **Note:** The URL filtering engine compares URLs with addresses entered in the Sites field first. If the URL of a transaction matches an entry in the Sites field, it is not compared to any expression entered here. |
|                              | For more information about using regular expressions in the Web Security appliance, see Regular Expressions, page 16-28.                  |

**Step 4** Optionally, click **Sort URLs** to sort all addresses in the Sites field.

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

**Step 5** Submit and commit your changes.
Filtering Adult Content

You can configure the Web Security appliance to filter adult content from some web searches and websites. You might want to do this to allow access to these sites, such as google.com and youtube.com, while still restricting potentially unsafe content from reaching users. For example, a school district could allow access to educational videos on youtube.com, but block inappropriate contents for students.

AsyncOS for Web offers the following features to filter adult content:

- **Enforce safe searches.** Many search engines support a filtering technology feature that classifies inappropriate content on the web as adult. When this filtering feature is enabled, content classified as adult is filtered from the search results before presented to the user. This feature is commonly called safe search. However, for most search engines, this feature is enabled and disabled by end users. You can configure the Web Security appliance so that outgoing search requests appear to search engines as safe search requests. This gives the control to an administrator on the network instead of the end user. You might want to do this to prevent users from bypassing acceptable use policies using search engines.

- **Enforce site content ratings.** Many content sharing sites that serve user-generated photos and videos classify some of their content as adult. They allow users to restrict their own access to the adult content on these sites by either enforcing their own safe search feature or blocking access to adult content, or both. This classification feature is commonly called content ratings.

You enforce safe searches and site content ratings for different users by enabling the feature at the Access Policy level. Not all search engines or content sharing websites are supported, but AsyncOS for Web can support additional search engines and websites during URL filtering engine updates. The Access Policies > URL Filtering > policyname page always lists the currently supported search engines and websites for each feature. The list of supported search engines and content sharing websites may increase with AVC engine updates.

Consider the following rules and guidelines when enforcing safe search and site content ratings:

- To use the safe search and site content ratings features, AsyncOS for Web must use the URL filtering engine included with Cisco IronPort Web Usage Controls.
• The safe search feature enforces strict safe searches.
• When the URL of one of the supported search engines or supported content ratings websites is included in a custom URL category with the Allow action applied, then users can access that URL as if the safe search or content ratings features were disabled. That is, no search results are blocked and all content is visible.
• You can choose whether or not to block users from search engines that are not currently supported by the Web Security appliance safe search feature.
• Due to the limitations inherent in youtube.com, the Web Proxy is not able to block embedded YouTube videos from a third party website.
• When configuring the site content ratings feature, you can choose whether to block users from adult content or to provide them with end-user URL filtering warning page that allows them to view the adult content after clicking a link to accept the warning message. For more information, see Warning Users and Allowing Them to Continue, page 16-24.
• Any Access Policy that has either the safe search or site content ratings feature enabled is considered a safe browsing Access Policy.

To enforce safe searches and site content ratings:

Step 1  Navigate to the Web Security Manager > Access Policies page.
Step 2  Click the link under the URL Categories column for an Access Policy group or the Global Policy Group. The Access Policies: URL Filtering: policyname page appears.
Step 3  When editing a user-defined Access Policy, choose Define Content Filtering Custom Settings in the Content Filtering section.
Step 4  Click the Enable Safe Search check box to enable the safe search feature.
Step 5  Choose whether to block users from search engines that are not currently supported by the Web Security appliance safe search feature.

Step 6  Click the Enable Site Content Rating check box to enable the site content ratings feature.

Step 7  Choose whether to block all adult content from the supported content ratings websites or to display the end-user URL filtering warning page.

Step 8  Submit and commit your changes.

Logging Adult Content Access

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

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

Table 16-5 describes the safe browsing scanning verdict values.

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

For more information on logging, see Access Log File, page 24-19.
Requests blocked due to either the safe search or site content rating features, use one of the following ACL decision tags in the access logs:

- BLOCK_SEARCH_UNSAFE
- BLOCK_CONTENT_UNSAFE
- BLOCK_UNSUPPORTED_SEARCH_APP
- BLOCK_CONTINUE_CONTENT_UNSAFE

For more information on the ACL decision tags, see ACL Decision Tags, page 24-24.

**Redirecting Traffic**

In addition to using the Web Security appliance to monitor and block traffic to certain websites, you can also use it to redirect users to a different website. You can configure the appliance to redirect traffic originally destined for a URL in a custom URL category to a location you specify. This allows you to redirect traffic at the appliance instead of at the destination server.

You might want to redirect traffic at the appliance if your organization published the links to an internal site, but the location of the site changed since publication, or if you do not have control over the web server.

Configure the appliance to redirect custom URL categories to another location when you configure the URL categories for an Access Policy group. You can redirect traffic for a custom Access Policy group or the Global Policy Group.

---

**Note**
To redirect traffic, you must define at least one custom URL category. For more information about creating custom URL categories, see Custom URL Categories, page 16-16.

**Note**
Beware of infinite loops when you configure the appliance to redirect traffic. For example, if you redirect traffic destined for http://A.example.com to http://B.example.com and you also inadvertently redirect traffic destined for http://B.example.com to http://A.example.com, then you create an infinite loop. In this case, the appliance redirects the traffic back and forth between the two URLs indefinitely.
To redirect traffic:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Navigate to the Web Security Manager &gt; Access Policies page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the link under the URL Categories column for an Access Policy group or the Global Policy Group. The Access Policies: URL Filtering: <em>policynames</em> page appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Custom URL Category Filtering section, verify the custom URL category you want to redirect is included. If the Include link displays, click it. If the Exclude link displays, the category is already included.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the Redirect column for the custom category you want to redirect.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter the URL to which you want to redirect traffic in the Redirect To field for the custom category.</td>
</tr>
</tbody>
</table>

**Warning Users and Allowing Them to Continue**

In addition to using the Web Security appliance to block traffic to certain websites, you can also use it to warn users that a site does not meet the organization’s acceptable use policies and allow them to continue if they choose. You might want to warn users and allow them to continue if your organization wants to discourage its users from accessing certain sites, but does not want to or is not allowed by law to block access to those sites.

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

- Choose the Warn action for a URL category in an Access Policy group.
Warning Users and Allowing Them to Continue

- Enable the site content ratings feature and warn users that access adult content instead of blocking them. For more information on the site content ratings feature, see Filtering Adult Content, page 16-20.

When users access a URL that is configured to warn and continue, they initially see an IronPort notification page with a warning about accessing sites of this category or content. The end-user URL filtering warning page includes the following elements:

- Default warning text provided by IronPort
- Custom text provided by the Web Security appliance administrator (optional)
- Notification code listing the invoked Access Policy and the URL category being warned or the safe browsing scanning verdict.
- A hypertext link to the originally requested URL

Users are tracked in the access log by user name if authentication has made a user name available, and tracked by IP address if no user name is available.

When you use the warn and continue feature, you can configure the following settings that affect the end-user URL filtering warning page:

- **Time Between Warning.** The Time Between Warning determines how often the Web Proxy displays the end-user URL filtering warning page for each URL category per user. Once a user clicks the continue link on the end-user URL filtering warning page, the Web Proxy considers that user to have acknowledged the warning for the time you enter for the Time Between Warning. This setting applies to users tracked by username and users tracked by IP address. You can specify any value from 30 to 2678400 seconds (one month). Default is 1 hour (3600 seconds).

- **Custom message.** The custom message is text you enter that appears on every end-user URL filtering warning page. You might want to include text for the organization’s acceptable use policies, or include a link to a page that details the acceptable use policies. You can include some simple HTML tags to format the text. For example, you can change the color and size of the text, or make it italicized. See Custom Text in Notification Pages, page 15-23 for more information.

Configure these settings on the Security Services > End-User Notification page. For more information, see Configuring the End-User URL Filtering Warning Page, page 15-21.
The warn and continue feature only works for HTTP and decrypted HTTPS transactions. It does not work with native FTP transactions.

User Experience When Warning Users

When the URL filtering engine warns users for a particular request, it provides a warning page that the Web Proxy sends to the end user. However, not all websites display the warning page to the end user. For example, some Web 2.0 websites display dynamic content using javascript instead of a static webpage and are not likely to display the warning page from the Web Proxy. When this happens, users are blocked from the URL that is assigned the Warn option without being given the chance to continue accessing the site anyway.

Creating Time Based URL Filters

You can configure how the Web Security appliance handles requests for URLs in particular categories differently based on time and day. For example, you can block access to social networking sites, such as blogs and forums, during business hours.

To define URL filtering actions by time you must first define at least one time range. For information about time ranges, see Working with Time Based Policies, page 6-13.

To create time based URL filtering actions for an Access Policy:

Step 1 Navigate to the Web Security Manager > Access Policies page.

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


Step 3 Select Time-Based for the custom or predefined URL category you want to configure based on time range.
Chapter 16      URL Filters

Viewing URL Filtering Activity

When you select Time-Based for the URL category, additional fields appear under the category name where you can choose the actions.

Step 4  In the In Time Range field, choose the defined time range to use for the URL category.

For information about defining time ranges, see Creating Time Ranges, page 6-14.

Step 5  In the Action field, choose the action to enact on transactions in this URL category during the defined time range.

Step 6  In the Otherwise field, choose the action to enact on transactions in this URL category outside the defined time range.

Step 7  Submit and commit your changes.

Viewing URL Filtering Activity

The Reporting > URL Categories page provides a collective display of URL statistics that includes information about top URL categories matched and top URL categories blocked. Additionally, this page displays category-specific data for bandwidth savings and web transactions. For detailed information about monitoring and reporting functionality, see Reporting, page 22-1.
Understanding Unfiltered and Uncategorized Data

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

- **URL Filtering Bypassed** — This data represents policy, port, and admin user agent blocking that occurs before URL filtering.
- **Uncategorized URL** — This data represents all transactions for which the URL filtering engine is queried, but no category is matched.

Access Log File

The access log file records the URL category for each transaction in the scanning verdict information section of each entry. For more information about the access log, see Access Log File, page 24-19. For a list of each URL category, see URL Category Descriptions, page 16-32.

Regular Expressions

Regular expressions are pattern matching descriptions that contain normal printable characters and special characters that are used to match patterns in text strings. For example, a text string such as “welcome” matches “welcome” or “welcomemyfriend.” When a match occurs, the function returns true. If no match occurs, the function returns false. Actions are executed only when a pattern-matching expression is true.

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

**Note**

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

You can use regular expressions in the following locations:
Custom URL categories for Access Policies. When you create a custom URL category to use with Access Policy groups, you can use regular expressions to specify multiple web servers that match the pattern you enter. For more information about creating custom URL categories, see Custom URL Categories, page 16-16.

Custom user agents to block. When you edit the applications to block for an Access Policy group, you can use regular expressions to enter specific user agents to block, such as Skype or Microsoft Internet Explorer. For more information about using regular expressions to block user agents, see Policy: Protocols and User Agents, page 8-18.

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

Forming Regular Expressions

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

\.*blocksite\.*com

Consider the following regular expression example:

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

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

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

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

Avoid using regular expressions strings that are redundant because they can cause higher CPU usage on the Web Security appliance. A redundant regular expression is one that starts or ends with “.*".
You must enclose regular expressions that contain blank spaces or non-alphanumeric characters in ASCII quotation marks.

### Regular Expression Character Table

Table 16-6 describes characters that are commonly used to form regular expressions:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Matches a single character.</td>
</tr>
<tr>
<td>*</td>
<td>Matches zero or more occurrences of the preceding regular expression.</td>
</tr>
<tr>
<td></td>
<td>For example: [0-9]* matches any number of digits</td>
</tr>
<tr>
<td></td>
<td>&quot;.*&quot; matches any arbitrary string of characters</td>
</tr>
<tr>
<td>^</td>
<td>Matches the beginning of a line as the first character of a regular expression.</td>
</tr>
<tr>
<td>$</td>
<td>Matches the end of a line as the last character of a regular expression.</td>
</tr>
<tr>
<td>+</td>
<td>Matches one or more occurrences of the preceding regular expression.</td>
</tr>
<tr>
<td>?</td>
<td>Matches zero or one occurrence of the preceding regular expression.</td>
</tr>
<tr>
<td>l</td>
<td>Matches the preceding regular expression or the following regular expression.</td>
</tr>
<tr>
<td></td>
<td>For example: xly matches either x or y</td>
</tr>
<tr>
<td></td>
<td>abclxyz matches either of the strings abc or xyz</td>
</tr>
</tbody>
</table>
Chapter 16      URL Filters

Regular Expressions

Note

To match the literal version of any of the special characters, the character must be preceded by a backslash “\”. For example, to exactly match a period “.” the regular expression must use “\.” as in “\example\com”. However, the appliance does not support using a backward slash to escape a forward slash. If you need to use a forward slash in a regular expression, type the forward slash without a backward slash.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>Matches the characters or digits that are enclosed within the brackets. For example:</td>
</tr>
<tr>
<td>[ ]</td>
<td>[a-z] matches any character between a and z</td>
</tr>
<tr>
<td>[ ]</td>
<td>[r-u] matches any of the characters r, s, t, or u</td>
</tr>
<tr>
<td>[ ]</td>
<td>[0-3] matches any of the single digits 0, 1, 2, 3</td>
</tr>
<tr>
<td>{ }</td>
<td>Specifies the number of times to match the previous pattern. For example:</td>
</tr>
<tr>
<td>{ }</td>
<td>D{1,3} matches one to three occurrences of the letter D</td>
</tr>
<tr>
<td>()</td>
<td>Group characters in a regular expression. For example:</td>
</tr>
<tr>
<td>()</td>
<td>(abc)* matches abc or abcabcabc</td>
</tr>
<tr>
<td>&quot;...&quot;</td>
<td>Literally interprets any characters enclosed within the quotation marks.</td>
</tr>
<tr>
<td>\</td>
<td>Escape character.</td>
</tr>
</tbody>
</table>
URL Category Descriptions

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

Note: The URL category abbreviations for Cisco IronPort Web Usage Controls include the prefix “IW_” before each abbreviation so that the “art” category becomes “IW_art.”

Table 16-7 lists and describes the URL categories for the Cisco IronPort Web Usage Controls.

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult</td>
<td>adlt</td>
<td>1006</td>
<td>These are sites directed to adults, not necessarily pornographic sites. Adult clubs: strip clubs,</td>
<td>cybereroticanews.com/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>swingers clubs, escort services, strippers; general information about sex, non-pornographic in</td>
<td>dansex.dk/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>nature; genital piercing; adult products, adult greeting cards; information about sex not in the</td>
<td>eqsex.com/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>context of health or disease.</td>
<td>crotchrocket.us/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>toperotique.com</td>
</tr>
<tr>
<td>Advertisements</td>
<td>adv</td>
<td>1027</td>
<td>Banner and pop-up ads that often accompany a web page; other advertising sites that provide</td>
<td>doubleclick.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>advertisement content.</td>
<td>banners.yellowpages.co.uk</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ads.msn.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>affiliateclicks.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>arc6.msn.com</td>
</tr>
</tbody>
</table>
### URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
</table>
| Alcohol and Tobacco          | at           | 1048 | Beer, wine, spirits: beer and wine making, cocktail recipes, liquor sellers, wineries, vineyards, breweries; mixed drinks; tobacco; pipes and smoking products. | smokers.com/  
michiganbrewersguild.org/  
johnniewalker.com/  
cigaraficionado.com/  
lvcwines.com/ |
| Arts and Entertainment       | art          | 1002 | Galleries and exhibitions; artists and art; photography; literature and books, publishing; movies; performing arts and theater; music and radio; television; celebrities and fan sites; design; architecture; entertainment news, venues; humor. | kidrock.com  
guitarist.co.uk  
entertainment.yahoo.com/  
drudgereportarchives.com  
nycballet.com |
<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business and Industry</td>
<td>busi</td>
<td>1019</td>
<td>Sites involved in business-to-business transactions of all kinds. Advertising, marketing, commerce, corporations, business practices, workforce, human resources, transportation, payroll, security, venture capital, etc; office supplies; industrial equipment (process equipment), machines and mechanical systems; heating equipment, cooling equipment; materials handling equipment; packaging equipment; manufacturing: solids handling, metal fabrication construction and building; passenger transportation; commerce; industrial design; construction, building materials; industrial design; shipping and freight: freight services, trucking, freight forwarders, truckload carriers, freight/transportation brokers, expedited services, load &amp; freight matching, track &amp; trace, NVOCC, railroad shipping, ocean shipping, road feeder services, moving &amp; storage; online meetings.</td>
<td>smithbearing.com/paychex.com/newholland.com/adsonwheels.com/cat.com</td>
</tr>
</tbody>
</table>
| Cheating and Plagiarism| plag         | 1051 | Sites promoting cheating and selling written work (e.g., term papers) for plagiarism.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | schoolsucks.com/thesis-statements.com/academietermpapers.com/cheathouse.com/nursingpapers.com/
## URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Child Porn</td>
<td>cprn</td>
<td>1064</td>
<td>Sites that host child pornography and pedophilia.</td>
<td>No examples can be legally/ethically given.</td>
</tr>
<tr>
<td>Computer Security</td>
<td>csec</td>
<td>1065</td>
<td>Sites that offer security product and services for corporate and home users.</td>
<td>abuse.net&lt;br&gt;activesecuritymonitor.com&lt;br&gt;iisprotect.com&lt;br&gt;securityfocus.com&lt;br&gt;sectools.org</td>
</tr>
<tr>
<td>Computers and Internet</td>
<td>comp</td>
<td>1003</td>
<td>Information about computers and software such as: hardware, software, software support sites; information for software engineers, programming and networking; website design, and the web and Internet in general; computer science; computer graphics and clipart.</td>
<td>wallpapers.com&lt;br&gt;unicode.org&lt;br&gt;redhat.com/&lt;br&gt;msexchange.org&lt;br&gt;geeksquad.com</td>
</tr>
<tr>
<td>Cults</td>
<td>cult</td>
<td>1041</td>
<td>Cults and cult behavior.</td>
<td>churchofsatan.com&lt;br&gt;voodoo.de&lt;br&gt;hexen.org&lt;br&gt;magical-lights.de&lt;br&gt;heavensgate.com</td>
</tr>
<tr>
<td>Dating</td>
<td>date</td>
<td>1055</td>
<td>Dating sites, online personals, matrimonial agencies, etc., for adults.</td>
<td>catholicmatch.com&lt;br&gt;collegeluv.com&lt;br&gt;allpersonals.com&lt;br&gt;eharmony.com&lt;br&gt;farmersonly.com</td>
</tr>
</tbody>
</table>
### URL Category Abbreviation Code Description Example URLs

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dining and Drinking</td>
<td>food</td>
<td>1061</td>
<td>Eating and drinking establishments; restaurants, bars, taverns, brewpubs;</td>
<td>southcitygrill.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>restaurant guides and reviews.</td>
<td>chilis.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>elnuevorodeo.com/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>pizzahut.co.uk</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>mcdonalds.com</td>
</tr>
<tr>
<td>Education</td>
<td>edu</td>
<td>1001</td>
<td>Education-related sites and web pages such as schools, colleges, universities,</td>
<td>ucla.edu</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>teaching materials, teachers resources; technical and vocational training;</td>
<td>pearsonhighered.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>online training; education issues and policy; financial aid; school funding;</td>
<td>k12.ca.us/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>testing.</td>
<td>homeworknow.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>gedpractice.com</td>
</tr>
<tr>
<td>File Transfer Services</td>
<td>fts</td>
<td>1071</td>
<td>Sites with the primary purpose of providing download services and hosted</td>
<td>yousendit.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>file sharing.</td>
<td>rapidshare.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>techsofttools.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sharefile.com/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2large2email.com</td>
</tr>
<tr>
<td>Filter Avoidance</td>
<td>filt</td>
<td>1025</td>
<td>Web pages that promote and aid undetectable and anonymous surfing.</td>
<td>proxyblind.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>the-cloak.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>proxybuster.net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>youhide.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>zend2.com</td>
</tr>
</tbody>
</table>
## URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>fnnc</td>
<td>1015</td>
<td>Sites and information that are primarily financial in nature such as:</td>
<td>finance.yahoo.com/usbank.com/nasdaq.com/lendingtree.com/shopyourmortgage.ca</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>accounting practices and accountants; taxation; banking; insurance; investing;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>information relating to the stock market, stocks, bonds, mutual funds, brokers,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>stock analysis and commentary, stock screens, stock charts, IPOs, stock</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>splits; the national economy; personal finance involving insurance of all</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>types; credit cards; retirement and estate planning; loans; mortgages; taxes.</td>
<td></td>
</tr>
<tr>
<td>Freeware and</td>
<td>free</td>
<td>1068</td>
<td>Sites that provide downloading of freeware and shareware software.</td>
<td>all-freeware.com/download.com/freewarefiles.com/onlyfreewares.com/uberdownloads.com</td>
</tr>
<tr>
<td>Shareware</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gambling</td>
<td>gamb</td>
<td>1049</td>
<td>Casinos and online gambling sites; bookmakers and odds; gambling advice;</td>
<td>eurobet.co.uk/pokerworld.com/onlinepokernews.com/bodog.com/blindbetpoker.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>horse and dog racing in a gambling context; sports book; sports gambling.</td>
<td></td>
</tr>
<tr>
<td>Games</td>
<td>game</td>
<td>1007</td>
<td>Various card games, board games, word games, video games; computer games,</td>
<td>netdevil.com/games.com/games.yahoo.com/pogo.com/cheatworld.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Internet games (RPGs and D&amp;D); combat games; sports games; downloadable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>games; game reviews; cheat sheets.</td>
<td></td>
</tr>
</tbody>
</table>
### URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
</table>
| Government and Law   | gov          | 1011 | Foreign relations; news and information relating to politics and elections such as: politics, political parties, election news and voting; sites and information relating the field of law such as: attorneys, law firms, law publications, legal reference material, courts, dockets, legal associations; legislation and court decisions; civil rights issues; immigration; patents and copyrights; sites and information relating to law enforcement and correctional systems; sites related to crime, crime reporting, law enforcement, crime statistics, etc; sites relating to the military such as: the armed forces, military bases, military organizations, and military equipment; anti-terrorism. | texas.gov  
legalzoom.com  
fenwick.com  
comcast.net/news/politics/  
barackobama.com |
| Hacking              | hack         | 1050 | Sites discussing ways to hack into web sites, software, and computers.                                                                                                                                         | crackfind.com/  
hackthissite.org/  
dirkster.com/  
trinsic.org/  
sweethacks.com/ |
### URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
</table>
| Hate Speech          | hate         | 1016 | Hate-related sites, involving racism, sexism, racist theology; hate music; Christian identity religions; World Church of the Creator; Neo-Nazi organizations: Aryan Nations, American Nazi parties, Neo-Nazis, Ku Klux Klan, National Alliance, White Aryan Resistance, white supremacists; National Socialist Movement; Holocaust denial. | panzerfaust.com  
                        |              |      | bloodandhonour.com  
                        |                      |      | kkk.com  
                        |                      |      | nazi.org  
                        |                      |      | blacksandjews.com  |
| Health and Nutrition | hlth         | 1009 | Health care; disease and disabilities; medical care; hospitals; doctors; medicinal drugs; mental health; psychiatry; pharmacology; exercise and fitness; physical disabilities; vitamins and supplements; sex in a context of health (disease and health care); tobacco use, alcohol use, drug use, and gambling in a context of health (disease and health care); food in general; food and beverage; cooking and recipes; food and nutrition, health, dieting; cooking, including recipe and culinary sites. | webmd.com  
                        |              |      | health.gov  
                        |                      |      | stjohns.com  
                        |                      |      | lowcarb.ca  
                        |                      |      | fitness.com  
                        |                      |      | chefmoz.org  
                        |                      |      | cookingmarvel.com  |
| Illegal Activities   | crmr         | 1022 | Pages that promote crime such as stealing, fraud, phreaking and cracking; warez and pirated software; computer viruses; terrorism, bombs, and anarchy; sites depicting murder and suicide as well as explaining ways to commit them. | lockpicksonline.com  
                        |              |      | grokster.com  
                        |                      |      | anarchistcookbook.com  
                        |                      |      | directwarez.com  
<pre><code>                    |                      |      | ddlshark.com  |
</code></pre>
<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illegal Drugs</td>
<td>drug</td>
<td>1047</td>
<td>Information about recreational drugs, drug paraphernalia, marijuana seeds; advice on how to grow marijuana.</td>
<td>marijuana.com, sporeworks.com, clearest.com, bcseeds.com, drugs-plaza.com</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>misc</td>
<td>1018</td>
<td>Content delivery infrastructure and dynamically-generated content - these cannot be more specifically categorized because the pages are secured or otherwise difficult to categorize</td>
<td>example.com, akamai.net, imagenet.co.uk, edgecastcdn.net, webstat.net</td>
</tr>
<tr>
<td>Instant Messaging</td>
<td>im</td>
<td>1039</td>
<td>Web-based instant messaging.</td>
<td>messenger.yahoo.com, meebo.com, friendvox.com, aimonpsp.com, buddy4u.com</td>
</tr>
<tr>
<td>Internet Telephony</td>
<td>voip</td>
<td>1067</td>
<td>Sites that provide telephonic services using the Internet</td>
<td>aussievoip.com.au, downloadsquad.com/category/voip, skypepc.com, simplecall.net, packet8.net</td>
</tr>
<tr>
<td>Job Search</td>
<td>job</td>
<td>1004</td>
<td>Career advice; advice on resume writing and interviewing skills; job placement services; job databanks; employment and temp agencies; employer sites.</td>
<td>jobs.com, siena.edu/careercenter, policeemployment.com, novastaffinginc.com, monster.de</td>
</tr>
<tr>
<td>URL Category</td>
<td>Abbreviation</td>
<td>Code</td>
<td>Description</td>
<td>Example URLs</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------</td>
<td>------</td>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lottery and Sweepstakes</td>
<td>lotr</td>
<td>1034</td>
<td>Sweepstakes, contests and lotteries.</td>
<td>calottery.com/state.nj.us/lottery/powerball.com/hoosierlottery.com/national-lottery.co.uk/</td>
</tr>
<tr>
<td>Mobile Phones</td>
<td>cell</td>
<td>1070</td>
<td>Sites that provide SMS services; ringtones.</td>
<td>shop.orange.co.uk/savemysms.fr/smartphonemag.com/sprint.com/jamster.com</td>
</tr>
</tbody>
</table>
### URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nature</td>
<td>natr</td>
<td>1013</td>
<td>Natural resources; ecology and conservation; forests; wilderness; plants; flowers; forest conservation; forest, wilderness, forestry practices; forest management (re-forestation, forest protection, conservation, harvesting, forest health, thinning, prescribed burning); agricultural practices: agriculture, gardening, horticulture, landscaping, planting, weed control, irrigation, pruning, harvesting; pollution issues: air quality, hazardous waste, pollution prevention, recycling, waste management, water quality, environmental clean-up industry; animals, pets, livestock, zoology; biology; botany.</td>
<td>nature.org/ enature.com/ fs.fed.us/ roselinebunnies.com chicagobotanic.org</td>
</tr>
<tr>
<td>Non-sexual</td>
<td>nsn</td>
<td>1060</td>
<td>Nudism/nudity; nudist camps; artistic nudes.</td>
<td>simplenudes.com barenakedgallery.com fineartnude.com grex.com erosgallery.net</td>
</tr>
</tbody>
</table>
## URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Communities</td>
<td>comm</td>
<td>1024</td>
<td>Personal web pages; affinity groups; special interest groups; professional organizations for social purposes; personal photo collections; web newsgroups; e-cards; message boards.</td>
<td>reptileforums.co.uk photo.net wendyjohnson.net threadoftheday.com startrek.com</td>
</tr>
<tr>
<td>Online Storage and Backup</td>
<td>osb</td>
<td>1066</td>
<td>Sites providing offsite, peer to peer, and could storage for backup, sharing and hosting.</td>
<td>angelbackup.com jbackup.com myotherdrive.com elephantdrive.com allmydata.com/</td>
</tr>
<tr>
<td>Online Trading</td>
<td>trad</td>
<td>1028</td>
<td>Online brokerages, sites which afford the user the ability to trade stocks online.</td>
<td>tdwaterhouse.com tradingdirect.com scottrade.com pricegroup.com orionfutures.com</td>
</tr>
<tr>
<td>Paranormal and Occult</td>
<td>nonm</td>
<td>1029</td>
<td>Non-mainstream approaches to life. Occult practices: esoteric magic, voodoo, witchcraft, casting spells; fortune telling practices: I Ching, numerology, psychic advice, Tarot; paranormal: out of body, astral travel, seances; astrology, horoscopes; UFOs and aliens.</td>
<td>witchcraft.com tarot.com spiritualguidance.com horoscopes.aol.com californiapsychics.com</td>
</tr>
<tr>
<td>Peer File Transfer</td>
<td>p2p</td>
<td>1056</td>
<td>Peer-to-peer file request sites. This does not track the file transfers themselves.</td>
<td>bittorrent.com/ downloadaccess.net/ filesoup.co.uk/ piratebay.org/ limewire.com</td>
</tr>
</tbody>
</table>
### URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Porn</td>
<td>porn</td>
<td>1054</td>
<td>Sexually explicit text or depictions. Includes the following: nude celebrities; anime and XXX cartoons; general XXX depictions; material of a sexually violent nature (bondage, domination, sadomasochism, torture, rape, spanking, snuff, fantasy death, necrophilia); other fetish material (foot/legs, infantilism, balloon sex, latex gloves, enema, pregnant women, pony-play, BBW, bestiality); XXX chat rooms; sex simulators; sites that offer strip poker; adult movies; lewd art; web-based pornographic e-mail.</td>
<td>playboy.com, penthouse.com, hustler.com, vivid.com, xxx.com</td>
</tr>
<tr>
<td>Real Estate</td>
<td>rest</td>
<td>1045</td>
<td>Information that would support the search for real estate. This includes: office and commercial space; real estate listings: rentals, apartments, homes; house building; roommates, etc.</td>
<td>realtor.com, zillow.com/, remax.com, joannekizerrealestate.com/, rockfordhomesinc.com/</td>
</tr>
<tr>
<td>Reference</td>
<td>fyi</td>
<td>1017</td>
<td>City and state guides; maps, weather, time; reference sources; dictionaries; libraries; museums; ski conditions; personal information; mass transportation: consumer mass transit information (bus, commuter train, subway, airport), schedules.</td>
<td>weather.com, timezoneconverter.com, metrocommute.com, maps.google.com, dictionary.com</td>
</tr>
</tbody>
</table>
### URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe for Kids</td>
<td>yc</td>
<td>1057</td>
<td>Sites directed toward and specifically approved for young children.</td>
<td>webkinz.com/kerkinz.com/kinderthemes.com/kids.nationalgeographic.com/nickjr.com/pingu.net/</td>
</tr>
<tr>
<td>Science and Technology</td>
<td>sci</td>
<td>1012</td>
<td>Sites involving science and technology: aerospace, electronics, engineering, mathematics, etc.; space exploration; meteorology; geography; environment; energy; oil, nuclear, wind, sun; communications; telephones, telecomm.</td>
<td>technologyreview.com/space.com/awea.org/ieee.org/carbonpower.com</td>
</tr>
<tr>
<td>Search Engines and Portals</td>
<td>srch</td>
<td>1020</td>
<td>Web directories and search engines that often serve as home pages such as Excite, MSN, Alta Vista, and Google.</td>
<td>google.com/baidu.com/bing.com/kablum.com/kellysearch.com</td>
</tr>
<tr>
<td>Sex Ed and Abortion</td>
<td>sxed</td>
<td>1052</td>
<td>Sexual health; information about, or descriptions of, abortion procedures such as: abortion pills, medical abortions, surgical abortions; abortion clinics and abortion providers.</td>
<td>prochoice.org/prolife.com/teensource.org/mens-sexual-health.org/dontcrossyourfingers.co.uk/</td>
</tr>
</tbody>
</table>
### URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shopping</td>
<td>shop</td>
<td>1005</td>
<td>Auctions; bartering; online purchasing; coupons and free offers; yellow pages; classified ads; general office supplies; online catalogs; online malls.</td>
<td>ticketmaster.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>radioshack.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>pier1.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>amazon.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ecco.com</td>
</tr>
<tr>
<td>Social Networking</td>
<td>snet</td>
<td>1069</td>
<td>Sites that provide social networking.</td>
<td>myspace.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>facebook.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>linkedin.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>twitter.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>badoo.com</td>
</tr>
<tr>
<td>Social Science</td>
<td>socs</td>
<td>1014</td>
<td>Sites related to: archaeology; anthropology; cultural studies; economics; history; linguistics; philosophy; political science; psychology; theology; women's studies.</td>
<td>templarhistory.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>civilwar.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>abrp.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>languagelearninglab.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sociologyonline.net</td>
</tr>
<tr>
<td>Society and Culture</td>
<td>scty</td>
<td>1010</td>
<td>Family and relationships; religions; ethnicity and race; social organizations; genealogy; seniors; clothing and fashion; spas; hair salons; cosmetics (skin care for diseases or conditions may be categorized as Health and Nutrition); hobbies; do-it-yourself; toys for kids; model and remote controlled cars; toy soldiers; childcare.</td>
<td>christianity.com/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>women.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>unitedway.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>safekids.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>hairfinder.com</td>
</tr>
</tbody>
</table>
## URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Updates</td>
<td>swup</td>
<td>1053</td>
<td>Sites that host updates for software packages.</td>
<td>windowsupdate.com, symantecliveupdate.com, updates.ironport.com, macupdate.com, rhn.redhat.com</td>
</tr>
<tr>
<td>Spiritual Healing</td>
<td>heal</td>
<td>1042</td>
<td>Spiritual healing; alternative approaches to health, both physical and mental.</td>
<td>touchingspirit.org, spiritual-medium.com, mountainvalleycenter.com, holisticmed.com, dancing-bear.com</td>
</tr>
<tr>
<td>Sports and Recreation</td>
<td>sprt</td>
<td>1008</td>
<td>All sports, professional and amateur; recreational activities; hunting; fishing; fantasy sports; gun and hunting clubs; public parks; amusement parks; water parks; theme parks; zoos and aquariums.</td>
<td>espn.go.com, sports.yahoo.com, nfl.com, fantasyfootball.com, hickoryhawks.org</td>
</tr>
<tr>
<td>Streaming Media</td>
<td>mdia</td>
<td>1026</td>
<td>Sites that involve: net radio; net TV; web casts; streaming audio; streaming video.</td>
<td>wired.com/news/radio, warm1069.com, pandora.com, blip.tv, capitalfm.co.uk</td>
</tr>
<tr>
<td>Tasteless or Obscene</td>
<td>obs</td>
<td>1033</td>
<td>Sites that offer tasteless, often gory photographs such as autopsy photos, photos of crime scenes, crime or accident victims; sites displaying excessive obscene material.</td>
<td>torture-museum.com, scatworld.net, theelectricchair.com, cadaver.org, ehowa.com</td>
</tr>
</tbody>
</table>
## URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tattoos</td>
<td>tat</td>
<td>1043</td>
<td>Pictures and text relating to body modification; tattoos and piercing venues; articles and information about tattoos and piercing; body painting.</td>
<td>tattoo.com/ tattoosbyhoss.com/ rankmytattoos.com/ coolshop.com/ alohamonkeytattoo.com/</td>
</tr>
<tr>
<td>Transportation</td>
<td>trns</td>
<td>1044</td>
<td>Sites about personal transportation; information about cars and motorcycles; shopping for new and used cars and motorcycles; car clubs; boats, airplanes, RVs, etc. (Note: auto and motorcycle racing is categorized as Sports and Recreation).</td>
<td>volkswagen.com/ transwestgmc.com/ mgscustombikes.com/ autobytel.com/ autos.msn.com/</td>
</tr>
<tr>
<td>Travel</td>
<td>trvl</td>
<td>1046</td>
<td>Business and personal travel: travel information; travel resources; travel agents; vacation packages; cruises; lodging and accommodations; travel transportation: flight booking, airfares, renting cars; vacation homes.</td>
<td>travelocity.com/ travel.yahoo.com/ yellowstone.net/ russia-travel.com/ hyatt.com/</td>
</tr>
<tr>
<td>Violence</td>
<td>viol</td>
<td>1032</td>
<td>Sites related to violence and violent behavior.</td>
<td>realfights.com severe-spanking.com justfights.com facesofdeath.com maafa.org/</td>
</tr>
</tbody>
</table>
## URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
</table>
| Weapons                      | weap         | 1036 | Sites or information relating to the purchase or use of conventional weapons such as: gun sellers; gun auctions; gun classified ads; gun accessories; gun shows; gun training; general information about guns; other weapons (e.g., knives, brass knuckles) may be included. | northcoastknives.com
gunworld.com
gunsmagazine.com
colt.com
army.mod.uk/equipment       |
| Web Hosting                  | whst         | 1037 | Sites that provide web site hosting services.                                                                                                                                                                | rackspace.com/
godaddy.com/
1and1.com/
startlogic.com/
doteasy.com/|
| Web Page Translation         | tran         | 1063 | Web sites that translate web pages into/from English. Also allow clicking to other pages on given site.                                                                                                       | babelfish.yahoo.com
google.com/language_tools
itools.com/lang/
ingro.com
online-translator.com       |
Table 16-8 lists the URL categories for IronPort URL Filters.

<table>
<thead>
<tr>
<th>URL Category</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Description</th>
<th>Example URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>mail</td>
<td>1038</td>
<td>Email portals and email messages</td>
<td>mail2web.com/ mail.google.com/ mail.yahoo.com/ webmail.covad.net/ outlook.monroecollege.edu/ exchange/</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>URL Category</th>
<th>URL Category Abbreviation</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Engines</td>
<td>Sear</td>
<td>7503</td>
</tr>
<tr>
<td>Sports</td>
<td>Spor</td>
<td>10</td>
</tr>
<tr>
<td>Travel</td>
<td>Trav</td>
<td>11</td>
</tr>
<tr>
<td>Hobbies &amp; Recreation</td>
<td>Hobb</td>
<td>12</td>
</tr>
<tr>
<td>Gambling</td>
<td>Gamb</td>
<td>13</td>
</tr>
<tr>
<td>Health &amp; Medicine</td>
<td>Heal</td>
<td>14</td>
</tr>
<tr>
<td>News</td>
<td>News</td>
<td>20</td>
</tr>
<tr>
<td>Finance &amp; Investment</td>
<td>Fina</td>
<td>25</td>
</tr>
<tr>
<td>Fashion &amp; Beauty</td>
<td>Fash</td>
<td>9501</td>
</tr>
<tr>
<td>URL Category</td>
<td>URL Category Abbreviation</td>
<td>Code</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Kids Sites</td>
<td>Kids</td>
<td>7003</td>
</tr>
<tr>
<td>Government</td>
<td>Gove</td>
<td>40</td>
</tr>
<tr>
<td>Games</td>
<td>Game</td>
<td>1202</td>
</tr>
<tr>
<td>Arts</td>
<td>Arts</td>
<td>50</td>
</tr>
<tr>
<td>Entertainment</td>
<td>Ente</td>
<td>51</td>
</tr>
<tr>
<td>Chat</td>
<td>Chat</td>
<td>3001</td>
</tr>
<tr>
<td>Society &amp; Culture</td>
<td>Soci</td>
<td>3003</td>
</tr>
<tr>
<td>Job Search &amp; Career Development</td>
<td>Job</td>
<td>60</td>
</tr>
<tr>
<td>Religion</td>
<td>Reli</td>
<td>3006</td>
</tr>
<tr>
<td>Real Estate</td>
<td>Real</td>
<td>3010</td>
</tr>
<tr>
<td>Philanthropic &amp; Professional Organizations</td>
<td>Phil</td>
<td>9803</td>
</tr>
<tr>
<td>Education</td>
<td>Educ</td>
<td>70</td>
</tr>
<tr>
<td>Peer-to-Peer</td>
<td>Peer</td>
<td>9801</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Infr</td>
<td>9802</td>
</tr>
<tr>
<td>Computing &amp; Internet</td>
<td>Comp</td>
<td>75</td>
</tr>
<tr>
<td>Ringtones/Mobile Phone Downloads</td>
<td>Ring</td>
<td>9804</td>
</tr>
<tr>
<td>Motor Vehicles</td>
<td>Moto</td>
<td>1101</td>
</tr>
<tr>
<td>Politics</td>
<td>Poli</td>
<td>9806</td>
</tr>
<tr>
<td>Suspect/Threat URLs</td>
<td>Susp</td>
<td>9101</td>
</tr>
<tr>
<td>Hacking</td>
<td>Hack</td>
<td>7504</td>
</tr>
<tr>
<td>Sex Education</td>
<td>Sex</td>
<td>1490</td>
</tr>
<tr>
<td>Web-based E-mail</td>
<td>Web-</td>
<td>7507</td>
</tr>
<tr>
<td>Streaming Media</td>
<td>Stre</td>
<td>7509</td>
</tr>
<tr>
<td>Reference</td>
<td>Refe</td>
<td>7001</td>
</tr>
<tr>
<td>Adult/Sexually Explicit</td>
<td>Adult</td>
<td>90</td>
</tr>
</tbody>
</table>
## URL Category Descriptions

<table>
<thead>
<tr>
<th>URL Category</th>
<th>URL Category Abbreviation</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal Activity</td>
<td>Crim</td>
<td>91</td>
</tr>
<tr>
<td>Intolerance &amp; Hate</td>
<td>Into</td>
<td>92</td>
</tr>
<tr>
<td>Violence</td>
<td>Viol</td>
<td>93</td>
</tr>
<tr>
<td>Weapons</td>
<td>Weap</td>
<td>94</td>
</tr>
<tr>
<td>Intimate Apparel &amp; Swimwear</td>
<td>Inti</td>
<td>95</td>
</tr>
<tr>
<td>Personals &amp; Dating</td>
<td>Pers</td>
<td>96</td>
</tr>
<tr>
<td>Photo Searches</td>
<td>Phot</td>
<td>97</td>
</tr>
<tr>
<td>Proxies &amp; Translators</td>
<td>Prox</td>
<td>98</td>
</tr>
<tr>
<td>Hosting Sites</td>
<td>Host</td>
<td>99</td>
</tr>
<tr>
<td>Business</td>
<td>Busi</td>
<td>100</td>
</tr>
<tr>
<td>Shopping</td>
<td>Shop</td>
<td>80</td>
</tr>
<tr>
<td>Food &amp; Dining</td>
<td>Food</td>
<td>3004</td>
</tr>
<tr>
<td>Blogs &amp; Forums</td>
<td>Blog</td>
<td>2002</td>
</tr>
<tr>
<td>Advertisements &amp; Popups</td>
<td>Adve</td>
<td>76</td>
</tr>
<tr>
<td>Downloads</td>
<td>Down</td>
<td>7501</td>
</tr>
<tr>
<td>Illegal Drugs</td>
<td>Ille</td>
<td>1403</td>
</tr>
<tr>
<td>Alcohol &amp; Tobacco</td>
<td>Alco</td>
<td>1404</td>
</tr>
<tr>
<td>Tasteless &amp; Offensive</td>
<td>Tast</td>
<td>9301</td>
</tr>
<tr>
<td>URL Filtering Bypassed</td>
<td>-</td>
<td>1073741824</td>
</tr>
<tr>
<td>Uncategorized URLs</td>
<td>nc</td>
<td>1073741825</td>
</tr>
<tr>
<td>URL Filtering Bypassed</td>
<td>err</td>
<td>1073741826</td>
</tr>
</tbody>
</table>
Understanding Application Visibility and Control

This chapter contains the following information:

- Controlling Applications Overview, page 17-1
- Understanding Application Control Settings, page 17-4
- Controlling Bandwidth, page 17-11
- Controlling Instant Messaging Traffic, page 17-17
- Viewing AVC Activity, page 17-19

Controlling Applications Overview

The Web has become the ubiquitous platform for application delivery in the enterprise, whether that is browser based application platforms like Salesforce.com and Google Apps, or rich media applications like Cisco WebEx using web protocols as a widely available transport in and out of enterprise networks.

Cisco IronPort Web Usage Controls includes the Application Visibility and Control engine (AVC engine) which enables administrators to apply deeper controls to particular application types. The AVC engine is an acceptable use policy component that inspects web traffic to gain deeper understanding and control of web traffic used for applications. Application control gives you more granular control over web traffic than just URL filtering, for example.
The AVC engine allows you to create policies to control application activity on the network without having to fully understand the underlying technology of each application.

Application control gives you more control over the following types of applications:

- Evasive applications, such as anonymizers and encrypted tunnels.
- Collaboration applications, such as Cisco Webex and instant messaging.
- Resource intensive applications, such as streaming media.

To control applications using the AVC engine, perform the following steps:

1. Enable the AVC engine. For more information, see Enabling the AVC Engine, page 17-3.
2. Define application control settings in the Access Policies. For more information, see Understanding Application Control Settings, page 17-4.

Using the AVC engine, you can block or allow applications by application type or a particular application. You can also apply deeper controls to particular application types. For example, you can perform the following tasks:

- **Limit bandwidth consumed by some application types to control congestion.** For more information, see Controlling Bandwidth, page 17-11.
- **Allow instant messaging traffic, but disallow file sharing using instant messenger.** For more information, see Controlling Instant Messaging Traffic, page 17-17.
- **Enforce safe search on search engines and user generated content sites.** For more information, see Filtering Adult Content, page 16-20.
- **Restrict access to adult content on some content sharing sites.** For more information, see Filtering Adult Content, page 16-20.

The AVC engine can dynamically receive updates from the Cisco IronPort update server, including support for new applications and application types. For more information, see AVC Engine Updates, page 17-3.

You can also view the AVC engine scanning activity in the Application Visibility report on the Reporting > Application Visibility page. For more information, see Viewing AVC Activity, page 17-19.
User Experience with Blocked Requests

When the AVC engine blocks a transaction, the Web Proxy sends a block page to the end user. However, not all websites display the block page to the end user. For example, some Web 2.0 websites display dynamic content using javascript instead of a static webpage and are not likely to display the block page. Users are still properly blocked from uploading malicious data, but they may not always be informed of this by the website.

AVC Engine Updates

AsyncOS periodically queries the update servers for new updates to all security service components, including the AVC engine. AVC engine updates can include support for new application types and applications as well as updated for support for existing applications if any application behavior changes. By updating the AVC engine in between AsyncOS versions, the Web Security appliance remains flexible without requiring a server upgrade.

AVC engine updates are maintained by the Cisco Security Intelligence Operations (SIO) center. Cisco SIO updates signatures as necessary to adapt to the changing marketplace.

Because the AVC engine can receive support for new applications and application types, AsyncOS for Web assigns the following default actions for the Global Access Policy:

- New application types default to Monitor.
- New application behaviors, such as block file transfer within a particular application, default to Monitor.
- New applications for an existing application type default to the application type default.

Enabling the AVC Engine

Enable the AVC engine when you enable Cisco IronPort Web Usage Controls.

To enable the AVC engine:
Understanding Application Control Settings

Step 1  Navigate to the Security Services > Acceptable Use Controls page.

Step 2  Click Edit Global Settings.

The Edit Acceptable Use Controls Settings page appears.

Edit Acceptable Use Controls Settings

<table>
<thead>
<tr>
<th>Acceptable Use Controls Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>When Acceptable Use Controls service is enabled, a user could configure acceptable use policies based on URL filtering and more.</td>
</tr>
<tr>
<td>☑ Enable Acceptable Use Controls</td>
</tr>
<tr>
<td>Acceptable Use Controls Service:</td>
</tr>
<tr>
<td>- IronPort URL Filters</td>
</tr>
<tr>
<td>- Cisco IronPort Web Usage Controls</td>
</tr>
<tr>
<td>- Enable Application Visibility and Control</td>
</tr>
<tr>
<td>- Enable Dynamic Content Analysis Engine</td>
</tr>
<tr>
<td>Default Action for Unreadable Service:</td>
</tr>
<tr>
<td>- Redirect</td>
</tr>
<tr>
<td>- Block</td>
</tr>
</tbody>
</table>

Step 3  Verify the Enable Acceptable Use Controls property is enabled.

Step 4  In the Acceptable Use Controls Service area, select Cisco IronPort Web Usage Controls, and then select Enable Application Visibility and Control.

Step 5  Submit and commit your changes.

Understanding Application Control Settings

Controlling applications involves configuring the following elements:

- **Application types.** A category that contains one or more applications. For example, Instant Messaging is an application type that contains Google Talk and AOL Instant Messenger.

- **Applications.** Particular applications that belong in an application type. For example, YouTube is an application in the Media application type.

- **Application behaviors.** Particular actions or behaviors that users can do within an application that administrators can control. For example, users can transfer files while using an application, such as Yahoo Messenger. Not all applications include application behaviors you can configure.

You can configure application control settings in Access Policy groups. From the Web Security Manager > Access Policies page, click the Applications link for the policy group you want to configure. The Access Policies: Applications Visibility and Control: policymame page appears, or the “Applications Visibility and Control page” for short.
The Applications Visibility and Control page shows the current applications you can configure as determined by the current AVC engine signature. Regardless of the particular applications you can configure, the Applications Visibility and Control page offers the following views for configuring applications:

- **Browse view.** You can browse for application types. You might want to use Browse view to configure applications of a particular type at the same time. For more information, see Working with Browse View, page 17-5.

- **Search view.** You can search for applications. You might want to use Search view when the total list of applications is long and you need to quickly find and configure a particular application. For more information, see Working with Search View, page 17-7.

You can configure most of the same control settings in both views. However, you can only configure the bandwidth control limits for application types in Browse view.

When configuration applications, you can choose the following actions:

- **Block.** This action is a final action. Users are prevented from viewing a webpage and instead an end-user notification page displays.

- **Monitor.** This action is an intermediary action. The Web Proxy continues comparing the transaction to the other control settings to determine which final action to apply. For more information, see Understanding the Monitor Action, page 8-3.

- **Restrict.** This action indicates that an application behavior is blocked. For example, when you block file transfers for a particular instant messaging application, the action for that application is Restrict.

## Working with Browse View

Figure 17-1 shows the Applications Visibility and Control page in Browse view for a user defined Access Policy.
Figure 17-2 shows the Applications Visibility and Control page in Browse view for the Global Access Policy.
Access Policies: Applications Visibility and Control: Global Policy

<table>
<thead>
<tr>
<th>Default Actions for Application Types</th>
<th>Default Action for Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant Messaging</td>
<td>Monitor</td>
</tr>
<tr>
<td>Media</td>
<td>Monitor</td>
</tr>
<tr>
<td>P2P / File Sharing</td>
<td>Monitor</td>
</tr>
<tr>
<td>Presentation / Conferencing</td>
<td>Monitor</td>
</tr>
<tr>
<td>Social Networking</td>
<td>Monitor</td>
</tr>
</tbody>
</table>

Configure the default action for the type.
Configure the bandwidth limit for the type.
Define global settings for each application and application behavior.

Working with Search View

Figure 17-3 shows the Applications Visibility and Control page in Search view for a user defined Access Policy.
Understanding Application Control Settings


Configure search criteria. Click to column headers to sort columns. Click to configure this application. Configure the settings for this application.
Rules and Guidelines

Consider the following rules and guidelines when configuring application control settings:

- The supported application types, applications, and application behaviors may change between AsyncOS for Web upgrades during AVC engine updates.
- When an application type is collapsed in Browse view, the summary for the application type lists the final actions for the applications and does not indicate whether the actions are inherited from the global policy or configured in the current Access Policy. To learn more about the action for an application, expand the application type.
- In the Global Access Policy, you can set the default action for each application type. You might want to set the default action for each application type so new applications introduced in an Application Visibility and Control engine update automatically inherit the default action.
- You can quickly configure the same action for all applications in an application type by clicking the “edit all” link for the application type in Browse view. However, you can only configure the application action, not application behavior actions. To configure application behaviors, you must edit the application individually instead of editing all applications for a type at once.
- In Search view, when you sort the table by the action column, the sort order is by the final action. For example, “Use Global (Block)” comes after “Block” in the sort order.
- Decryption may cause some applications to fail unless the root certificate for signing is installed on the client. For more information, see Using Decryption with the AVC Engine, page 10-19. For more information on the appliance root certificate, see Working with Root Certificates, page 10-16.

Configuring Application Control Settings

To configure Application settings in an Access Policy group:

Step 1 Navigate to the Web Security Manager > Access Policies page.
Step 2  Click the link in the policies table under the Applications column for the policy group you want to edit.

The Applications Visibility and Control page appears.


<table>
<thead>
<tr>
<th>Applications</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant Messaging</td>
<td>4 Monitor</td>
</tr>
<tr>
<td>Media</td>
<td>Bandwidth Limit: No Bandwidth Limit</td>
</tr>
<tr>
<td>P2P / File Sharing</td>
<td>3 Monitor</td>
</tr>
<tr>
<td>Presentation / Conferencing</td>
<td>1 Monitor</td>
</tr>
<tr>
<td>Social Networking</td>
<td>1 Monitor</td>
</tr>
</tbody>
</table>

Step 3  When configuring the Global Access Policy, define the default action for each application type in the Default Actions for Application Types section. For details on how to do this, see Figure 17-2 on page 7.

Step 4  When configuring a user defined Access Policy, choose Define Applications Custom Settings in the Edit Applications Settings section.

Step 5  In the Application Settings area, choose Browse view or Search view from the drop down menu.

Step 6  Configure the action for each application and application behavior.

For more information on work with each view, see Working with Browse View, page 17-5 and Working with Search View, page 17-7.

Step 7  Configure the bandwidth controls for each applicable application. For more information, see Controlling Bandwidth, page 17-11.

Step 8  Submit and commit your changes.
Controlling Bandwidth

The AVC engine allows administrators to control the amount of bandwidth used for particular application types. Not all application types support bandwidth controls.

You can define the following bandwidth limits:

- **Overall bandwidth limit.** Define an overall limit for all users on the network for the supported application types. The overall bandwidth limit affects the traffic between the Web Security appliance and web servers. It does not limit traffic served from the web cache. You might want to define an overall bandwidth limit to restrict the amount of network traffic used for high traffic sites, such as streaming media sites. For more information, see Configuring Overall Bandwidth Limits, page 17-11.

- **User bandwidth limit.** Define a limit for particular users on the network per application type. User bandwidth limits traffic from web servers as well as traffic served from the web cache. You might want to define user bandwidth limits to restrict the amount of traffic consumed by heavy usage users to enforce acceptable use policies. For more information, see Configuring User Bandwidth Limits, page 17-12.

When both the overall limit and user limit applies to a transaction, the most restrictive option applies.

You can define bandwidth limits for particular URL categories by defining an Identity group for a URL category and using it in an Access Policy that restricts the bandwidth.

---

**Note**

Defining bandwidth limits only throttles the data going to users. It does not block data based on reaching a quota.

Configuring Overall Bandwidth Limits

The overall bandwidth limit affects the traffic between the Web Security appliance and web servers for all users on the network.

To define an overall bandwidth limit:
Controlling Bandwidth

Step 1
Navigate to the Web Security Manager > Overall Bandwidth Limits page.

**Edit Overall Bandwidth Limit**

<table>
<thead>
<tr>
<th>Media:</th>
<th>Option 1</th>
<th>Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No overall limit</td>
<td>Limit to Mbps</td>
</tr>
</tbody>
</table>

Step 2
Select the Limit to option.

Step 3
Enter the amount of traffic to limit in either Megabits per second (Mbps) or kilobits per second (kbps).

Step 4
Submit and commit your changes.

Configuring User Bandwidth Limits

You define user bandwidth limits by configuring bandwidth control settings on the Applications Visibility and Control page of Access Policies. You can define the following types of bandwidth controls for users in Access Policies:

- **Default bandwidth limit for an application type.** In the Global Access Policy, you can define the default bandwidth limit for all applications of an application type. For more information, see Configuring the Default Bandwidth Limit for an Application Type, page 17-13.

- **Bandwidth limit for an application type.** In a user defined Access Policy, you can override the default bandwidth limit for the application type defined in the Global Access Policy. You can configure no bandwidth limit or a different bandwidth limit value. For more information, see Overriding the Default Bandwidth Limit for an Application Type, page 17-13.

- **Bandwidth limit for an application.** In a user defined or Global Access Policy, you can choose to apply the application type bandwidth limit or no limit (exempt the application type limit). You might choose no bandwidth limit for an application to exempt the application from the bandwidth limit established that application type. For more information, see Configuring Bandwidth Controls for an Application, page 17-15.
Configuring the Default Bandwidth Limit for an Application Type

To configure the default bandwidth limit for an application type:

2. Click the link in the policies table under the Applications column for the Global Access Policy.
   - The Applications Visibility and Control page appears.
3. In the Default Actions for Application Types section, click the link next to “Bandwidth Limit” for the application type you want to edit.
   - The Applications Visibility and Control page expands, allowing you to specify the bandwidth control settings.
4. Select Set Bandwidth Limit and enter the amount of traffic to limit in either Megabits per second (Mbps) or kilobits per second (kbps). See Figure 17-2 on page 7 for details on how to do this.
5. Click Done.
6. Submit and commit your changes.

Overriding the Default Bandwidth Limit for an Application Type

You can override the default bandwidth limit defined at the Global Access Policy group in the user defined Access Policies. You can only do this in Browse view.

To override the default bandwidth limit for an application type:

2. Click the link in the policies table under the Applications column for the user defined policy group you want to edit.
   - The Applications Visibility and Control page appears.
3. Choose Define Applications Custom Settings in the Edit Applications Settings section.

   Note: Ensure you remain in Browse view. Do not switch to Search view.
Controlling Bandwidth


Step 4 Click the link next to “Bandwidth Limit” for the application type you want to edit. The Applications Visibility and Control page expands, allowing you to specify the bandwidth control settings.

Step 5 To choose a different bandwidth limit value, select Set Bandwidth Limit and enter the amount of traffic to limit in either Megabits per second (Mbps) or kilobits per second (kbps). To specify no bandwidth limit, select No Bandwidth Limit for Application Type.

Step 6 Click Done.

Step 7 Submit and commit your changes.
Configuring Bandwidth Controls for an Application

To configure bandwidth controls for an application:

**Step 1** Navigate to the Web Security Manager > Access Policies page.

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

The Applications Visibility and Control page appears.

**Step 3** Expand the application type that contains the application you want to define.

The Applications Visibility and Control page expands to allow you to configure each application in the application type.
Controlling Bandwidth

Step 4  
Click the link for the application you want to configure.

The Applications Visibility and Control page expands, allowing you to specify the bandwidth control settings for the application.

Step 5  
Select Monitor, and then choose to use either the bandwidth limit defined for the application type or no limit.

Note  
The bandwidth limit setting is not applicable when the application is blocked or when no bandwidth limit is defined for the application type.

Step 6  
Click Done.

Step 7  
Submit and commit your changes.
Controlling Instant Messaging Traffic

You can use the AVC engine to apply control settings to some instant messenger (IM) traffic that runs on top of HTTP. You can block or monitor the IM traffic, and depending on the IM service, you can block particular activities (also known as application behaviors) in an IM session. For example, you can allow an IM session with a particular IM service provider, but block file transfers within that session.

The AVC engine does not control native IM traffic.

You control IM traffic by configuring Instant Messenger application settings on the Applications Visibility and Control page of Access Policies.

To control IM traffic:

---

Step 1  Navigate to the Web Security Manager > Access Policies page.

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

The Applications Visibility and Control page appears.

Step 3  Expand the Instant Messaging application type.
Step 4  Click the link next to the IM application you want to configure. The Applications Visibility and Control page expands, allowing you to specify control settings for the application.

Step 5  To block all traffic for this IM application, select Block.

Step 6  To monitor the IM application, but block particular activities within the application, select Monitor, and then select the application behavior to block.

Step 7  Click Done.
Step 8  Submit and commit your changes.

**Viewing AVC Activity**

The Reporting > Application Visibility page displays information about the top applications and application types used. It also displays the top applications and application types blocked. You can click the individual applications and application types to view more detailed information about each. For detailed information about monitoring and reporting functionality, see Reporting, page 22-1.

**Access Log File**

The access log file records the information returned by the Application Visibility and Control engine for each transaction. The scanning verdict information section in the access logs includes the fields listed in Table 17-1.

<table>
<thead>
<tr>
<th>Description</th>
<th>Custom Field in Access Logs</th>
<th>Custom Field in W3C Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td>%XO</td>
<td>x-avc-app</td>
</tr>
<tr>
<td>Application type</td>
<td>%Xu</td>
<td>x-avc-type</td>
</tr>
<tr>
<td>Application behavior</td>
<td>%Xb</td>
<td>x-avc-behavior</td>
</tr>
</tbody>
</table>

For more information about the access log, see Access Log File, page 24-19.
Chapter 17  Understanding Application Visibility and Control

Viewing AVC Activity
Web Reputation Filters Overview

IronPort Web Reputation Filters is a security feature that analyzes web server behavior and assigns a reputation score to a URL to determine the likelihood that it contains URL-based malware. It helps protect against URL-based malware that threatens end-user privacy and sensitive corporate information. The Web Security appliance uses URL reputation scores to identify suspicious activity and stop malware attacks before they occur.

You can use Web Reputation Filters with both Access and Decryption Policies.

The Web Reputation Database

The Web Security appliance collects information and maintains a filtering database that contains aggregated traffic statistics, request attributes, and information about how different types of requests are handled. Additionally, the
appliance can be configured to send web reputation statistics to a SenderBase server. SenderBase server information is leveraged with data feeds from the IronPort Common Security Database (SenderBase® Network) and the collective information is used to produce a Web Reputation Score.

**Note**
For more information, see *The SenderBase Network, page 2-5.*

### Maintaining the Database Tables

The web reputation filtering component periodically receives updates to its database tables from the IronPort update server ([https://update-manifests.ironport.com](https://update-manifests.ironport.com)). Server updates are automated, and the update interval is set by the server as opposed to the appliance. Updates to the database tables occur with a regular degree of frequency, and require no administrator intervention.

For information about update intervals and the IronPort update server, see *Manually Updating Security Service Components, page 26-51.*

### Web Reputation Scores

Web Reputation Filters use statistically significant data to assess the reliability of Internet domains and score the reputation of URLs. Data such as how long a specific domain has been registered, or where a web site is hosted, or whether a web server is using a dynamic IP address is used to judge the trustworthiness of a given URL.

The web reputation calculation associates a URL with network parameters to determine the probability that malware exists. The aggregate probability that malware exists is then mapped to a Web Reputation Score between -10 and +10, with +10 being the least likely to contain malware.

Example parameters include the following:

- URL categorization data
- Presence of downloadable code
- Presence of long, obfuscated End-User License Agreements (EULAs)
- Global volume and changes in volume
Enabling Web Reputation Filters

To use web reputation in policy groups, you must first enable Web Reputation Filters. By default, Web Reputation Filters are enabled in the System Setup Wizard. If it is not enabled in the System Setup Wizard, you can edit them in the web interface.

To enable Web Reputation Filters in the web interface:

1. Navigate to the Security Services > Web Reputation Filters page.
2. Click Enable.
   - The Web Reputation Filters License Agreement appears.
3. Read the terms of the Web Reputation Filters License Agreement, and click Accept.
4. Click Edit Settings.
   - The Edit Web Reputation Filters Settings page appears.
5. Verify the Enable Web Reputation Filters property is enabled.
6. Submit and commit your changes.

**Note**
IronPort does not collect personally identifiable information such as user names, passwords, or client IP addresses.
Understanding How Web Reputation Filtering Works

Web Reputation Scores are associated with an action to take on a URL request. The available actions depend on the policy group type that is assigned to the URL request:

- **Access Policies.** You can choose to block, scan, or allow.
- **Decryption Policies.** You can choose to drop, decrypt, or pass through.

You can configure each policy group to correlate an action to a particular Web Reputation Score.

### Web Reputation in Access Policies

Table 18-1 describes the default Web Reputation Scores for Access Policies.

<table>
<thead>
<tr>
<th>Score</th>
<th>Action</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>-10 to -6.0</td>
<td>Block</td>
<td>Bad site. The request is blocked, and no further malware scanning occurs.</td>
<td>• URL downloads information without user permission.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Sudden spike in URL volume.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• URL is a typo of a popular domain.</td>
</tr>
<tr>
<td>-5.9 to 5.9</td>
<td>Scan</td>
<td>Undetermined site. Request is passed to the DVS engine for further malware scanning. The DVS engine scans the request and server response content.</td>
<td>• Recently created URL that has a dynamic IP address and contains downloadable content.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Network owner IP address that has a positive Web Reputation Score.</td>
</tr>
<tr>
<td>6.0 to 10.0</td>
<td>Allow</td>
<td>Good site. Request is allowed. No malware scanning required.</td>
<td>• URL contains no downloadable content.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Reputable, high-volume domain with long history.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Domain present on several allow lists.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No links to URLs with poor reputations.</td>
</tr>
</tbody>
</table>
For example, 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 IronPort DVS engine where it is scanned for malware. Any URL in an HTTP request that has a very poor reputation is blocked.

### Web Reputation in Decryption Policies

Table 18-2 describes the default Web Reputation Scores for Access Policies.

<table>
<thead>
<tr>
<th>Score</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-10 to -9.0</td>
<td>Drop</td>
<td>Bad site. The request is dropped with no notice sent to the end user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use this setting with caution.</td>
</tr>
<tr>
<td>-8.9 to 5.9</td>
<td>Decrypt</td>
<td>Undetermined site. Request is allowed, but the connection is decrypted and the decrypted traffic is applied to Access Policies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about how the appliance decrypts HTTPS traffic, see Decrypting HTTPS Traffic, page 10-13.</td>
</tr>
<tr>
<td>6.0 to 10.0</td>
<td>Pass through</td>
<td>Good site. Request is passed through with no inspection or decryption.</td>
</tr>
</tbody>
</table>

### Configuring Web Reputation Scores

When you install and set up the Web Security appliance, it has default settings for Web Reputation Scores. However, you can modify threshold settings for web reputation scoring to fit your organization’s needs.

You configure the web reputation filter settings for each policy group.
Configuring Web Reputation for Access Policies

To edit the web reputation filter settings for an Access Policy group:

**Step 1** Navigate to the Web Security Manager > Access Policies page.

**Step 2** Click the link under the Web Reputation and Anti-Malware Filtering column for the Access Policy group you want to edit.

**Step 3** Under the Web Reputation and Anti-Malware Settings section, choose “Define Web Reputation and Anti-Malware Custom Settings” from the drop down menu if it is not selected already.

**Step 4** Verify the Enable Web Reputation Filtering field is enabled.

**Step 5** Move the markers to change the range for URL block, scan, and allow actions.

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

This allows you to override the web reputation and anti-malware settings from the Global Policy Group.
Configuring Web Reputation for Decryption Policies

To edit the web reputation filter settings for a Decryption Policy group:

**Step 1** Navigate to the Web Security Manager > Decryption Policies page.

**Step 2** Click the link under the Web Reputation column for the Decryption Policy group you want to edit.

**Step 3** Under the Web Reputation Settings section, choose “Define Web Reputation Custom Settings” from the drop down menu if it is not selected already.

This allows you to override the web reputation settings from the Global Policy Group.

**HTTPS Decryption Policies: Reputation Settings: exampleDecryptionGroup**

<table>
<thead>
<tr>
<th>Web Reputation Settings</th>
<th>Define Web Reputation Custom Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Reputation Settings</td>
<td>Enable Web Reputation Filtering</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web Reputation Score</th>
<th>DROP: -10.0 to -9.0</th>
<th>DECRYPT: -9.9 to 5.9</th>
<th>PASS THROUGH: 5.9 to 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Drop</th>
<th>Decrypt</th>
<th>Pass Through</th>
</tr>
</thead>
<tbody>
<tr>
<td>The requested HTTPS connection is immediately dropped. No end-user notification will be provided.</td>
<td>The HTTPS transaction will be decrypted for scanning and no decrypted to ensure user privacy and security. The scanning defined in the applicable web access policy will be performed.</td>
<td>The HTTPS request is passed through without decryption. No scanning will be performed.</td>
</tr>
</tbody>
</table>

**Sites with No Score**

Specify an action for sites that do not have a Web Reputation Score.

<table>
<thead>
<tr>
<th>Sites with No Score</th>
<th>Move these markers to change the Web Reputation threshold values.</th>
</tr>
</thead>
</table>

**Step 4** Verify the Enable Web Reputation Filtering field is checked.

**Step 5** Move the markers to change the range for URL drop, decrypt, and pass through actions.
Configuring Web Reputation Scores

Step 6 In the Sites with No Score field, choose the action to take on request for sites that have no assigned Web Reputation Score.

Step 7 Submit and commit your changes.

Configuring Web Reputation for IronPort Data Security Policies

Only negative and zero values can be configured for web reputation threshold settings for IronPort Data Security Policies. By definition, all positive scores are monitored.

To edit the web reputation filter settings for a Data Security Policy group:

Step 1 Navigate to the Web Security Manager > IronPort Data Security page.

Step 2 Click the link under the Web Reputation column for the Data Security Policy group you want to edit.

Step 3 Under the Web Reputation Settings section, choose “Define Web Reputation Custom Settings” from the drop down menu if it is not selected already.

Ironport Data Security Policies: Reputation Settings: IDSPolicy1

<table>
<thead>
<tr>
<th>Web Reputation Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Define Custom Web Reputation Settings</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web Reputation Settings</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Web Reputation Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLOCK: -10.0 to 0.0</td>
</tr>
<tr>
<td>MONITOR: -5.9 to 0.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BLOCK</th>
<th>MONITOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>The transaction will be immediately blocked.</td>
<td>The transaction will not be blocked based on Web Reputation, and will proceed to content checks (file type and size). Note: Sites with no score will be monitored.</td>
</tr>
</tbody>
</table>

Move the marker to change the Web Reputation threshold value.
Viewing Web Reputation Filtering Activity

This allows you to override the web reputation settings from the Global Policy Group.

**Step 4**
Move the marker to change the range for URL block and monitor actions.

For more information on these actions, see Data Security Policy Groups, page 12-4.

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

**Viewing Web Reputation Filtering Activity**

The S-Series appliance supports several options for generating feature specific reports, and displays of summary statistics.

**Monitoring Filter and Scoring Activity**

The Reporting > Web Reputation Filters page provides statistical displays of filtering activity. You can update these displays by specifying a time range of hour, day, week or month. Additionally, you have the option to print these display pages and export the raw data to a file.

You can use the following interactive displays and reporting tools to view the results of Web Reputation filtering and scoring activity:

<table>
<thead>
<tr>
<th>To view...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web reputation action and scoring activity</td>
<td>Reporting &gt; Web Reputation Filters</td>
</tr>
<tr>
<td>Web reputation log files</td>
<td>System Administration &gt; Log Subscriptions</td>
</tr>
<tr>
<td></td>
<td>• WBRS log files</td>
</tr>
<tr>
<td></td>
<td>• Access log file</td>
</tr>
</tbody>
</table>
Access Log File

The access log file provides a record of filtering activity. You can examine entries in the access log file and trace web reputation processing specific to individual requests.

For more information about reading access log files, see Access Log File, page 24-19. For more an example access log entry that explains web reputation processing, see Web Reputation Filters Example, page 24-34.
Anti-Malware Services

This chapter contains the following information:

- Anti-Malware Overview, page 19-1
- IronPort DVS™ (Dynamic Vectoring and Streaming) Engine, page 19-4
- Webroot Scanning, page 19-7
- McAfee Scanning, page 19-8
- Sophos Scanning, page 19-10
- Configuring Anti-Malware Scanning, page 19-10
- Viewing Anti-Malware Scanning Activity, page 19-15

Anti-Malware Overview

The Web Security appliance anti-malware feature is a security component that uses the IronPort DVS™ engine in combination with the Webroot™, McAfee, and Sophos technologies to identify and stop a broad range of web-based malware threats.

For more information about the DVS engine, see IronPort DVS™ (Dynamic Vectoring and Streaming) Engine, page 19-4.

To use the anti-malware component of the appliance, you must first configure global settings and then apply specific settings to different policies. For more information about configuring the appliance for anti-malware scanning, see Configuring Anti-Malware Scanning, page 19-10.
You can also view the anti-malware scanning activity in reports and in the Web Security Monitor. For more information, see Viewing Anti-Malware Scanning Activity, page 19-15.

**Malware Category Descriptions**

Table 19-1 describes the different categories of malware the Web Security appliance can block.

<table>
<thead>
<tr>
<th>Malware Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware</td>
<td>Adware encompasses all software executables and plug-ins that direct users towards products for sale. Some adware applications have separate processes that run concurrently and monitor each other, ensuring that the modifications are permanent. Some variants enable themselves to run each time the machine is started. These programs may also change security settings making it impossible for users to make changes to their browser search options, desktop, and other system settings.</td>
</tr>
<tr>
<td>Browser Helper Object</td>
<td>A browser helper object is a browser plug-in that may perform a variety of functions related to serving advertisements or hijacking user settings.</td>
</tr>
<tr>
<td>Commercial System Monitor</td>
<td>A commercial system monitor is a piece of software with system monitor characteristics that can be obtained with a legitimate license through legal means.</td>
</tr>
<tr>
<td>Dialer</td>
<td>A dialer is a program that utilizes your modem or another type of Internet access to connect you to a phone line or a site that causes you to accrue long distance charges to which you did not provide your full, meaningful, and informed consent.</td>
</tr>
<tr>
<td>Hijacker</td>
<td>A hijacker modifies system settings or any unwanted changes to a user’s system that may direct them to a website or run a program without a user’s full, meaningful, and informed consent.</td>
</tr>
</tbody>
</table>
## Anti-Malware Overview

### Phishing URL
A phishing URL is displayed in the browser address bar. In some cases, it involves the use of domain names and resembles those of legitimate domains. Phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal personal identity data and financial account credentials.

### PUA
Potentially Unwanted Application. A PUA is an application that is not malicious, but which may be considered to be undesirable.

### System Monitor
A system monitor encompasses any software that performs one of the following actions:
- Overtly or covertly records system processes and/or user action.
- Makes those records available for retrieval and review at a later time.

### Trojan Downloader
A trojan downloader is a Trojan that, after installation, contacts a remote host/site and installs packages or affiliates from the remote host. These installations usually occur without the user’s knowledge. Additionally, a Trojan Downloader’s payload may differ from installation to installation since it obtains downloading instructions from the remote host/site.

### Trojan Horse
A trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves.

### Trojan Phisher
A trojan phisher may sit on an infected computer waiting for a specific web page to be visited or may scan the infected machine looking for user names and passwords for bank sites, auction sites, or online payment sites.

<table>
<thead>
<tr>
<th>Malware Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing URL</td>
<td>A phishing URL is displayed in the browser address bar. In some cases, it involves the use of domain names and resembles those of legitimate domains. Phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal personal identity data and financial account credentials.</td>
</tr>
<tr>
<td>PUA</td>
<td>Potentially Unwanted Application. A PUA is an application that is not malicious, but which may be considered to be undesirable.</td>
</tr>
<tr>
<td>System Monitor</td>
<td>A system monitor encompasses any software that performs one of the following actions:</td>
</tr>
<tr>
<td></td>
<td>• Overtly or covertly records system processes and/or user action.</td>
</tr>
<tr>
<td></td>
<td>• Makes those records available for retrieval and review at a later time.</td>
</tr>
<tr>
<td>Trojan Downloader</td>
<td>A trojan downloader is a Trojan that, after installation, contacts a remote host/site and installs packages or affiliates from the remote host. These installations usually occur without the user’s knowledge. Additionally, a Trojan Downloader’s payload may differ from installation to installation since it obtains downloading instructions from the remote host/site.</td>
</tr>
<tr>
<td>Trojan Horse</td>
<td>A trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves.</td>
</tr>
<tr>
<td>Trojan Phisher</td>
<td>A trojan phisher may sit on an infected computer waiting for a specific web page to be visited or may scan the infected machine looking for user names and passwords for bank sites, auction sites, or online payment sites.</td>
</tr>
</tbody>
</table>
IronPort DVS™ (Dynamic Vectoring and Streaming) Engine

The IronPort Dynamic Vectoring and Streaming (DVS) engine inspects web traffic to provide protection against the widest variety of web-based malware ranging from commercially invasive adware applications, to malicious trojans, system monitors, and phishing attacks.

To configure the DVS engine, and Webroot, McAfee, and Sophos global settings, see Configuring Anti-Malware Scanning, page 19-10.

The IronPort DVS engine can use one or more scanning engines to determine malware risk. Depending on the features purchased with the appliance, you can enable any of the following scanning engines:

- **Webroot.** Webroot’s automated spyware detection system rapidly identifies existing and new spyware threats on the Internet by intelligently scanning millions of sites on a daily basis. Webroot uses a signature database to help detect threats on the Internet. For more information about the Webroot scanning engine, see Webroot Scanning, page 19-7.

- **McAfee.** The McAfee scanning engine can detect existing and new malware threats by using a signature database of malware information and heuristic analysis. For more information about the McAfee scanning engine, see McAfee Scanning, page 19-8.

- **Sophos.** The Sophos scanning engine detects existing and new malware threats using a signature database. For more information about the Sophos scanning engine, see Sophos Scanning, page 19-10.

<table>
<thead>
<tr>
<th>Malware Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td>A virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.</td>
</tr>
<tr>
<td>Worm</td>
<td>A worm is program or algorithm that replicates itself over a computer network and usually performs malicious actions.</td>
</tr>
</tbody>
</table>
The scanning engines inspect transactions to determine a malware scanning verdict to pass to the DVS engine. A malware scanning verdict is a value assigned to a URL request or server response that determines the probability that it contains malware. The DVS engine determines whether to monitor or block the request based on the malware scanning verdicts. For more information about malware scanning verdicts, see Malware Scanning Verdict Values, page 24-52.

For each Access or Outbound Malware Scanning Policy, you can enable either the Sophos or McAfee scanning engine, but not both simultaneously. You can also enable the Webroot scanning engine with either Sophos or McAfee. You might want to enable the Sophos scanning engine instead of the McAfee scanning engine if the client machines have McAfee anti-malware software installed.

In some cases, the DVS engine might determine multiple verdicts for a single URL. For more information about how the DVS handles multiple verdicts, see Working with Multiple Malverdits, page 19-6.

### Maintaining the Database Tables

The Webroot, Sophos, and McAfee databases periodically receive updates from the IronPort update server (https://update-manifests.ironport.com). Server updates are automated, and the update interval is set by the server, not the appliance. Updates to the database tables occur with a regular degree of frequency, and require no administrator intervention.

For information about update intervals and the IronPort update server, see Manually Updating Security Service Components, page 26-51.

### 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.

When you enable both Webroot and Sophos or McAfee, the DVS engine determines how to scan the content to optimize performance and efficacy.

### Working with Multiple Malware Verdicts

In some cases, 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.
- **Different verdicts from the same scanning engine.** A scanning engine might return multiple verdicts for a single object when the object contains multiple infections. For example, a zip file might contain multiple files, each infected with a different kind of malware.

When a URL causes multiple verdicts, the appliance takes different action depending on whether one or both enabled scanning engines return the multiple malware verdicts.

### Different Scanning Engines

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. Only the most restrictive verdict is logged and reported.

### Same Scanning Engine

When a URL causes multiple verdicts from the same scanning engine, the appliance takes action according to the verdict with the highest priority. Only the highest verdict is logged and reported. 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

Suppose the McAfee scanning engine detects both adware and a virus in the scanned object, and that the appliance is configured to block adware and monitor viruses. According to the list above, viruses belong in a higher priority verdict category than adware. Therefore, the appliance monitors the object and reports the verdict as virus in the reports and logs. It does not block the object even though it is configured to block adware.

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.

  For more information about how the DVS engine uses malware scanning verdicts to handle web traffic, see IronPort DVS™ (Dynamic Vectoring and Streaming) Engine, page 19-4.

  For information about Web Reputation Filtering and URL scores, see Web Reputation Filters, page 18-1.

**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

  For more information about how the DVS engine uses malware scanning verdicts to handle web traffic, see IronPort DVS™ (Dynamic Vectoring and Streaming) Engine, page 19-4.

**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 always uses this method to scan server response content.
Heuristic Analysis

New threats on the web appear almost daily. Using only virus signatures, the engine cannot detect a new virus or other malware because its signature is not yet known. However, by using heuristic analysis, the McAfee scanning engine can detect new classes of currently unknown viruses and malware in advance.

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 likelihood of catching viruses and malware before McAfee updates its virus signature database. However, it also increases the possibility of reporting false positives (clean content designated as a virus). It also might impact appliance performance.

When you enable McAfee, you can choose whether or not to also enable heuristic analysis when scanning objects.

McAfee Categories

Table 19-2 lists the McAfee verdicts and how they correspond to malware scanning verdict categories.

<table>
<thead>
<tr>
<th>McAfee Verdict</th>
<th>Malware Scanning Verdict Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known Virus</td>
<td>Virus</td>
</tr>
<tr>
<td>Trojan</td>
<td>Trojan Horse</td>
</tr>
<tr>
<td>Joke File</td>
<td>Adware</td>
</tr>
<tr>
<td>Test File</td>
<td>Virus</td>
</tr>
<tr>
<td>Wannabe</td>
<td>Virus</td>
</tr>
<tr>
<td>Wannabe</td>
<td>Virus</td>
</tr>
<tr>
<td>Commercial Application</td>
<td>Commercial System Monitor</td>
</tr>
<tr>
<td>Potentially Unwanted Object</td>
<td>Adware</td>
</tr>
</tbody>
</table>
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 the client machines have McAfee anti-malware software installed.

For more information about how the DVS engine uses malware scanning verdicts to handle web traffic, see IronPort DVS™ (Dynamic Vectoring and Streaming) Engine, page 19-4.

Configuring Anti-Malware Scanning

The DVS engine and Webroot, McAfee, and Sophos are enabled by default during system setup. Anytime after system setup, you can configure the anti-malware settings for the Web Security appliance. You configure the following anti-malware settings:

- **Global anti-malware settings.** Set object scanning parameters, specify global settings for URL matching, and control when to block the URL or allow processing to continue.

- **Access Policy anti-malware settings.** Enable monitoring or blocking for malware categories based on malware scanning verdicts.

To configure anti-malware settings:

<table>
<thead>
<tr>
<th>McAfee Verdict</th>
<th>Malware Scanning Verdict Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potentially Unwanted Software Package</td>
<td>Adware</td>
</tr>
<tr>
<td>Encrypted File</td>
<td>Encrypted File</td>
</tr>
</tbody>
</table>
Step 1 On the Security Services > Anti-Malware page, click Edit Global Settings.

The Edit Anti-Malware Settings page appears.

Step 2 Configure the anti-malware settings as necessary. Table 19-3 describes the anti-malware settings you can configure.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Scanning Limits</td>
<td>Specify a maximum request/response size. The Maximum Object Size value you specify applies to the entire size of requests and responses that might be scanned by security components on the Web Security appliance, such as the IronPort Data Security Filters or the Webroot scanning engine. When an upload or download size exceeds this size, the security component may abort the scan in progress and may not provide a scanning verdict to the Web Proxy.</td>
</tr>
<tr>
<td>Enable Webroot</td>
<td>Choose whether or not to enable the Webroot scanning engine.</td>
</tr>
<tr>
<td>Domain Levels for Malware Request Detection</td>
<td>This value specifies the number of domain name elements to match when processing a URL. If the URL matches a hostname in the Webroot signature database, URL checking continues to match the number of domain name elements specified in this parameter. Valid range for this parameter is 3-100 where a minimum value of 8 is recommended to avoid a level of matching that results in inaccurately blocked web sites. Applies to the Webroot scanning engine only.</td>
</tr>
</tbody>
</table>
## Configuring Anti-Malware Scanning

### Step 3
Submit and commit your changes.

### Step 4
Navigate to the Web Security Manager > Access Policies page.

### Step 5
Click the Web Reputation and Anti-Malware Filtering link for the Access Policy you want to configure.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Risk Threshold</td>
<td>The TRT (Threat Risk Threshold) assigns a numerical value to the probability that malware exists. Proprietary algorithms evaluate the result of a URL matching sequence and assign a TRR (Threat Risk Rating). This value is associated with the threat risk threshold setting. If the TRR value is greater than or equal to the TRT, the URL is considered malware and is passed on for further processing. Note: Setting the Threat Risk Threshold to a value lower than 90 dramatically increases the rate of URL blocking and denies legitimate requests. IronPort strongly recommends maintaining the TRT default value of 90. The minimum value for a TRT setting is 51. Applies to the Webroot scanning engine only.</td>
</tr>
<tr>
<td>Enable McAfee</td>
<td>Choose whether or not to enable the McAfee scanning engine.</td>
</tr>
<tr>
<td>Heuristic Scanning</td>
<td>Choose whether or not to enable heuristic scanning for the McAfee scanning engine. For more information about heuristic scanning, see McAfee Scanning, page 19-8. Note: Heuristic analysis increases security protection, but can result in false positives and decreased performance. Applies to the McAfee scanning engine only.</td>
</tr>
<tr>
<td>Enable Sophos</td>
<td>Choose whether or not to enable the Sophos scanning engine.</td>
</tr>
</tbody>
</table>
On this page, you can enable monitoring or blocking for malware categories based on malware scanning verdicts.

**Step 6**  Under the “Web Reputation and Anti-Malware Settings” section, choose Define Web Reputation and Anti-Malware Custom Settings if it is not chosen already.

**Web Access Policies: Reputation and Anti-Malware Settings: groupAuthPolicy**

This allows you to configure web reputation and anti-malware settings for this Access Policy that differ from the global policy.

**Step 7**  Scroll down to the Ironport DVS Anti-Malware Settings section.
**Step 8**  Configure the anti-malware settings for the policy as necessary. Table 19-4 describes the anti-malware settings you can configure for Access Policies.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Suspect User Agent Scanning</td>
<td>Choose whether or not to enable the appliance to scan traffic based on the user agent field specified in the HTTP request header. When you check this setting, you can choose to monitor or block suspect user agents in the Additional Scanning section at the bottom of the page.</td>
</tr>
<tr>
<td>Enable Webroot</td>
<td>Choose whether or not to enable the appliance to use the Webroot scanning engine when scanning traffic. When you enable Webroot scanning, you can choose to monitor or block some additional categories in the Malware categories on this page.</td>
</tr>
<tr>
<td>Enable Sophos or McAfee</td>
<td>Choose whether or not to enable the appliance to use either the Sophos or McAfee scanning engine when scanning traffic. When you enable Sophos or McAfee scanning, you can choose to monitor or block some additional categories in the Malware categories on this page.</td>
</tr>
<tr>
<td>Malware Categories</td>
<td>Choose whether to monitor or block the various malware categories based on a malware scanning verdict. The categories listed in this section depend on which scanning engines you enable above.</td>
</tr>
<tr>
<td>Other Categories</td>
<td>Choose whether to monitor or block the types of objects and responses listed in this section. Note: URL transactions are categorized as unscannable when the configured maximum time setting is reached or when the system experiences a transient error condition. For example, transactions might be categorized as unscannable during scanning engine updates or AsyncOS upgrades. The malware scanning verdicts SV_TIMEOUT and SV_ERROR, are considered unscannable transactions.</td>
</tr>
</tbody>
</table>

**Step 9**  Submit and commit your changes.
Viewing Anti-Malware Scanning Activity

The Web Security appliance supports several options for generating feature specific reports, and interactive displays of summary statistics.

Monitoring Scanning Activity

The Reporting > Anti-Malware page provides statistical displays of malware scanning activity. You can update these displays by specifying a time range of hour, day, week or month. Additionally, you have the option to print these display pages and export the raw data to a file. You can use the following interactive displays and reporting tools to view the results of anti-malware scanning and related activity:

<table>
<thead>
<tr>
<th>To View...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top anti-malware sites</td>
<td>Reporting &gt; Overview</td>
</tr>
<tr>
<td>Top malware categories and threats</td>
<td>Reporting &gt; Anti-Malware</td>
</tr>
<tr>
<td>Anti-malware log files</td>
<td>System Administration &gt; Log Subscriptions</td>
</tr>
<tr>
<td></td>
<td>• Webroot log files</td>
</tr>
<tr>
<td></td>
<td>• McAfee log files</td>
</tr>
<tr>
<td></td>
<td>• Sophos log files</td>
</tr>
<tr>
<td></td>
<td>• Access log file</td>
</tr>
</tbody>
</table>

Access Log File

The access log file provides a record of anti-malware scanning activity. You can examine entries in the access log file and trace the result of malware scanning for individual requests. For more information about reading access log files, see Access Log File, page 24-19.
Authentication Overview

Authentication is the act of confirming the identity of a user. By using authentication in the Web Security appliance, you can control access to the Web for each user or a group of users. This allows you to enforce the organization’s
policies and comply with regulations. When you enable authentication, the Web Security appliance authenticates clients on the network before allowing them to connect to a destination server.

The Web Security appliance supports the following authentication protocols:

- **Lightweight Directory Access Protocol (LDAP).** The appliance supports standard LDAP server authentication and secure LDAP authentication. You can use a Basic authentication scheme. For more information about LDAP configuration options, see [LDAP Authentication, page 20-43](#).

- **NT Lan Manager (NTLM).** The appliance supports NTLM to enable authentication between the appliance and a Microsoft Windows domain controller. You can use either NTLMSSP or Basic authentication schemes. For more information about NTLM configuration options, see [NTLM Authentication, page 20-51](#).

To enable authentication, you must create at least one authentication realm. An authentication realm is a set of authentication servers (or a single server) supporting a single authentication protocol with a particular configuration. For more information about authentication realms, see [Working with Authentication Realms, page 20-14](#).

When you create more than one realm, you can group the realms into an authentication sequence. An authentication sequence is a group of authentication realms listed in the order the Web Security appliance uses for authenticating clients. For more information about authentication sequences, see [Working with Authentication Sequences, page 20-16](#).

You configure some authentication options at a global level, independent of any realm. For more information, see [Configuring Global Authentication Settings, page 20-23](#).

By creating authentication realms and sequences, you can configure the Web Security appliance to use one or more authentication servers for authenticating clients on the network. For more information about how the appliance works when it uses multiple authentication servers, see [Appliance Behavior with Multiple Authentication Realms, page 20-19](#).

After creating an authentication realm and possibly a sequence, too, you can create or edit Identities based on authentication realms or sequences. Note, however, that if you delete an authentication realm or sequence, any Identity group that depends on the deleted realm or sequence becomes disabled. For more information about using authentication with Identities, see [Understanding How Authentication Affects Identity Groups, page 7-4](#).
Client Application Support

When the Web Security appliance is deployed in transparent mode and a transaction requires authentication, the Web Proxy replies to the client application asking for authentication credentials. However, not all client applications support authentication, so they have no method for prompting users to provide their user names and passwords. These applications cannot be used when the Web Security appliance is deployed in transparent mode.

The following is a partial list of applications that do not work when the appliance is deployed in transparent mode:

- Mozilla Thunderbird
- Adobe Acrobat Updates
- HttpBridge
- Subversion, by CollabNet
- Microsoft Windows Update
- Microsoft Visual Studio

![Note]

If users need to access a particular URL using one of these client applications, then create an Identity based on a custom URL category that does not require authentication and place the Identity above all other Identities that require authentication. When you do this, the client application will not be asked for authentication.

Working with Upstream Proxy Servers

When the Web Security appliance is connected to an upstream proxy server, you can configure the appliance or the upstream proxy to use authentication, but not both. Cisco recommends configuring the Web Security appliance to use authentication. This allows you to create policies based on user authentication.

If both the appliance and the upstream proxy use authentication, 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.

## Authenticating Users

When users access the web through the Web Security appliance, they might get prompted to enter a user name and password. The Web Proxy requires authentication credentials for some users depending on the configured Identity and Access Policy groups. Users should enter the user name and password of the credentials recognized by the organization’s authentication server.

When the Web Proxy uses NTLMSSP authentication with an NTLM authentication realm, users are typically not prompted to enter a user name and password if single sign-on is configured correctly. However, if users are prompted for authentication, they must type the name of their Windows domain before their user name. For example, if user jsmith is on Windows domain MyDomain, then the user should type the following text in the user name field:

```
MyDomain\jsmith
```

However, if the Web Proxy uses Basic authentication for an NTLM authentication realm, then entering the Windows domain is optional. If the user does not enter the Windows domain, then the Web Proxy prepends the default Windows domain.

---

**Note** When the Web Proxy uses authentication with an LDAP authentication realm, ensure users do not enter the Windows domain name.

## Working with Failed Authentication

Sometimes users are blocked from the web due to authentication failure. The following list describes reasons for authentication failure and remedial actions you can take:

- **Client application cannot perform authentication.** Some clients cannot perform authentication or cannot perform the type of authentication that is required. If a client application causes authentication to fail, you can define an Identity policy based on the user agent and exclude it from requiring...
authentication. Or, you can define an Identity policy based on a custom URL category to exclude all clients from requiring authentication when accessing particular URLs.

- **Authentication server is unavailable.** An authentication server might be unavailable if the network connection is broken or if the server is experiencing a problem. To avoid this problem, configure the “Action if Authentication Service Unavailable” global authentication setting. For more information, see Configuring Global Authentication Settings, page 20-23.

- **Invalid credentials.** When a client passes invalid authentication credentials, the Web Proxy continually requests valid credentials, essentially blocking access to the web by default. However, you can grant limited access to users who fail authentication. For more information, see Allowing Guest Access to Users Who Fail Authentication, page 7-13.

  **Note** You can configure the Web Proxy to request authentication again if an authenticated user is blocked from a website due to restrictive URL filtering or being prevented from logging into multiple machines simultaneously. To do this, enable the “Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction” global authentication setting. For more information, see Allowing Users to Re-Authenticate, page 20-39.

---

## Understanding How Authentication Works

To authenticate users who access the web, the Web Security appliance connects to an external authentication server. The authentication server contains a list of users and their corresponding passwords and it organizes the users into a hierarchy. For users on the network to successfully authenticate, they must provide valid authentication credentials (user name and password as stored in the authentication server).

When users access the web through a Web Security appliance that requires authentication, the Web Proxy asks the client for authentication credentials. The Web Proxy communicates with both the client and the authentication server to authenticate the user and process the request.

**Figure 20-1** shows how the Web Security appliance communicates with clients and authentication servers.
The Web Security appliance supports the following authentication protocols:

- **Lightweight Directory Access Protocol (LDAP).** The Web Proxy uses the LDAP Bind operation to query an LDAP-compatible authentication server. The appliance supports standard LDAP server authentication and secure LDAP authentication.
  
  For more information about LDAP configuration options, see [LDAP Authentication](#), page 20-43.

- **NT LAN Manager (NTLM).** The Web Proxy uses NTLM, a Microsoft proprietary protocol, to authenticate users which exist in Microsoft Active Directory. The NTLM protocol uses a challenge-response sequence of messages between the client and the Active Directory server. You can use either NTLMSSP or Basic authentication schemes on client side.
  
  For more information about NTLM configuration options, see [NTLM Authentication](#), page 20-51.

In addition to the preceding protocols, the Web Security appliance supports the following client side authentication schemes:

- **Basic.** Allows a client application to provide authentication credentials in the form of a user name and password when it makes a request. You can use the Basic authentication scheme with either an LDAP or Active Directory server.

- **NTLMSSP.** Allows the client application to provide authentication credentials in the form of a challenge and response. It uses a binary message format to authenticate clients that use the NTLM protocol to access network resources. You can use the NTLMSSP authentication scheme only with an Active Directory server. When the Web Proxy uses NTLMSSP, most client...
applications can use the Windows login credentials for authentication and users do not need to enter their credentials again. This is called “single sign-on.”

For more information, see Basic versus NTLMSSP Authentication Schemes, page 20-7.

Table 20-1 describes the different authentication scenarios you can configure between the Web Security appliance and the client and between the Web Security appliance and the authentication server.

<table>
<thead>
<tr>
<th>Client to Web Security Appliance</th>
<th>Web Security Appliance to Authentication Server</th>
<th>Authentication Server Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>LDAP</td>
<td>LDAP server</td>
</tr>
<tr>
<td>Basic</td>
<td>LDAP</td>
<td>Active Directory server using LDAP</td>
</tr>
<tr>
<td>Basic</td>
<td>NTLM</td>
<td>Active Directory server using NTLM</td>
</tr>
<tr>
<td>NTLMSSP</td>
<td>NTLM</td>
<td>Active Directory server using NTLM</td>
</tr>
</tbody>
</table>

Web Proxy deployment also affects how authentication works in each of the scenarios described in Table 20-1. For more information, see How Web Proxy Deployment Affects Authentication, page 20-8.

**Basic versus NTLMSSP Authentication Schemes**

When you configure an Identity group to use authentication, you choose the authentication scheme, either Basic or NTLMSSP. The authentication scheme affects the user experience and the security of users’ passwords.
Table 20-2 describes the differences between Basic and NTLMSSP authentication schemes.

<table>
<thead>
<tr>
<th>Authentication Scheme</th>
<th>User Experience</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>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.</td>
<td>Credentials are sent unsecured as clear text (Base64). A packet capture between the client and Web Security appliance can reveal the user name and password. Note: You can configure the Web Security appliance so clients send authentication credentials securely. For more information, see Sending Authentication Credentials Securely, page 20-37.</td>
</tr>
</tbody>
</table>
| NTLMSSP               | The client transparently authenticates by using its Windows login credentials. The user is not prompted for credentials. However, the client prompts the user for credentials under the following circumstances:  
  • The Windows credentials failed.  
  • The client does not trust the Web Security appliance because of browser security settings. | Credentials are sent securely using a three-way handshake (digest style authentication). The password is never sent across the connection. For more information on the three-way handshake, see Explicit Forward Deployment, NTLM Authentication, page 20-12. |

How Web Proxy Deployment Affects Authentication

The Web Proxy communicates with clients and authentication servers differently depending on the type of Web Proxy deployment and the authentication protocol.
Table 20-3 lists the possible methods of authentication for the various authentication protocols and deployment type.

<table>
<thead>
<tr>
<th>Web Proxy Deployment</th>
<th>Client to Web Security Appliance</th>
<th>Web Security Appliance to Authentication Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explicit forward</td>
<td>Basic</td>
<td>LDAP or NTLM Basic</td>
</tr>
<tr>
<td>Transparent</td>
<td>Basic</td>
<td>LDAP or NTLM Basic</td>
</tr>
<tr>
<td>Explicit forward</td>
<td>NTLM</td>
<td>NTLMSSP</td>
</tr>
<tr>
<td>Transparent</td>
<td>NTLM</td>
<td>NTLMSSP</td>
</tr>
</tbody>
</table>

The following subsections describe these methods of authentication in more detail.

**Explicit Forward Deployment, Basic Authentication**

When a client explicitly sends a web page request to a Web Security appliance deployed in explicit forward mode, the Web Proxy can reply to the client with a 407 HTTP response “Proxy Authentication Required.” This status informs the client that it must supply valid authentication credentials to access web resources.

The authentication process comprises these steps:

- **Step 1** Client sends a request to the Web Proxy to connect to a web page.
- **Step 2** Web Proxy responds with a 407 HTTP response “Proxy Authentication Required.”
- **Step 3** User enters credentials, and client application resends the original request with the credentials encoded in Base64 (not encrypted) in a “Proxy-Authorization” HTTP header.
- **Step 4** Web Proxy verifies the credentials and returns the requested web page.
Table 20-4 lists advantages and disadvantages of using explicit forward Basic authentication.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>• RFC-based</td>
<td>• Password sent as clear text (Base64) for every request</td>
</tr>
<tr>
<td>• Supported by all browsers and most other applications</td>
<td>• No single sign-on</td>
</tr>
<tr>
<td>• Minimal overhead</td>
<td></td>
</tr>
<tr>
<td>• Works for HTTPS (CONNECT) requests</td>
<td></td>
</tr>
</tbody>
</table>

**Transparent Deployment, Basic Authentication**

The 407 HTTP response “Proxy Authentication Required” is allowed from proxy servers only. However, when the Web Proxy is deployed in transparent mode, its existence is hidden from client applications on the network. Therefore, the Web Proxy cannot return a 407 response.

To address this problem, the authentication process comprises these steps:

**Step 1**  
Client sends a request to a web page and the Web Proxy transparently intercepts it.

**Step 2**  
Web Proxy uses a 307 HTTP response to redirect the client to the Web Proxy which masquerades as a local web server.

**Step 3**  
Client sends a request to the redirected URL.

**Step 4**  
Web Proxy sends a 401 HTTP response “Authorization required.”

**Step 5**  
User is prompted for credentials and enters them.

**Step 6**  
Client sends the request again, but this time with the credentials in an “Authorization” HTTP header.

**Step 7**  
Web Proxy confirms the credentials, tracks the user by IP address or with a cookie, and then redirects the client to the originally requested server.

**Note**  
You can configure the Web Proxy to use either IP addresses or cookies to track authenticated users.
Step 8  
If the client requests the original web page again, the Web Proxy transparently intercepts the request, confirms the user by IP address or cookie, and returns the requested page.

Note  
If the client tries to connect to another web page and the Web Proxy tracked the user by IP address, the Web Proxy confirms the user by IP address and returns the requested page.

Table 20-5 lists advantages and disadvantages of using transparent Basic authentication and IP-based credential caching.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Works with all major browsers</td>
<td>• 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)</td>
</tr>
<tr>
<td>• With user agents that do not support authentication, users only need to authenticate first in a supported browser</td>
<td>• No single sign-on</td>
</tr>
<tr>
<td>• Relatively low overhead</td>
<td>• Password is sent as clear text (Base64)</td>
</tr>
<tr>
<td>• Works for HTTPS requests if the user has previously authenticated with an HTTP request</td>
<td></td>
</tr>
</tbody>
</table>
Table 20-6 lists advantages and disadvantages of using transparent Basic authentication and cookie-based credential caching.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Works with all major browsers</td>
<td>• Each new web domain requires the entire authentication process because</td>
</tr>
<tr>
<td>• Authentication is associated with the user rather than the host or IP</td>
<td>cookies are domain specific</td>
</tr>
<tr>
<td>address</td>
<td>• Requires cookies to be enabled</td>
</tr>
<tr>
<td></td>
<td>• Does not work for HTTPS requests</td>
</tr>
<tr>
<td></td>
<td>• No single sign-on</td>
</tr>
<tr>
<td></td>
<td>• Password is sent as clear text (Base64)</td>
</tr>
</tbody>
</table>

Explicit Forward Deployment, NTLM Authentication

The Web Proxy uses a third party challenge and response system to authenticate users on the network.

The authentication process comprises these steps:

- **Step 1** Client sends a request to the Web Proxy to connect to a web page.
- **Step 2** Web Proxy responds with a 407 HTTP response “Proxy Authentication Required.”
- **Step 3** Client repeats request and includes a “Proxy-Authorization” HTTP header with an NTLM “negotiate” message.
- **Step 4** Web Proxy responds with a 407 HTTP response and an NTLM “challenge” message based on the negotiate message from the client.
- **Step 5** Client repeats the request and includes a response to the challenge message.

**Note** The client uses an algorithm based on its password to modify the challenge and sends the challenge response to the Web Proxy.
Chapter 20  Authentication

Understanding How Authentication Works

Step 6  Web Proxy passes the authentication information to the Active Directory server. The Active Directory server then verifies that the client used the correct password based on whether or not it modified the challenge string appropriately.

Step 7  If the challenge response passes, the Web Proxy returns the requested web page.

Note  Additional requests on the same TCP connection do not need to be authenticated again with the Active Directory server.

Table 20-7 lists advantages and disadvantages of using explicit forward NTLM authentication.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Because the password is not transmitted to the authentication server, it is more secure</td>
<td>• Moderate overhead: each new connection needs to be re-authenticated</td>
</tr>
<tr>
<td>• Connection is authenticated, not the host or IP address</td>
<td>• Primarily supported on Windows only and with major browsers only</td>
</tr>
<tr>
<td>• Achieves true single sign-on in an Active Directory environment when the client applications are configured to trust the Web Security appliance</td>
<td></td>
</tr>
</tbody>
</table>

Transparent Deployment, NTLM Authentication

Transparent NTLM authentication is similar to transparent Basic authentication except that the Web Proxy communicates with clients using NTLMSSP instead of Basic. However, with transparent NTLM authentication, the authentication credentials are not sent in the clear to the authentication server.

For more information, see Transparent Deployment, Basic Authentication, page 20-10.

The advantages and disadvantages of using transparent NTLM authentication are the same as those of using transparent Basic authentication except that transparent NTLM authentication is better because the password is not sent to the authentication server and you can achieve single sign-on when the client
applications are configured to trust the Web Security appliance. For more information on the advantages and disadvantages of transparent Basic authentication, see Table 20-5 on page 11 Table 6 on page 12.

Working with Authentication Realms

An authentication realm is a set of authentication servers (or a single server) supporting a single authentication protocol with a particular configuration. You can perform any of the following tasks when configuring authentication:

- Include up to three authentication servers in a realm.
- Create zero or more LDAP realms.
- Create zero or one NTLM realm.
- Include an authentication server in multiple realms.
- Include one or more realms in an authentication sequence.
- Include realms of different protocols in a single authentication sequence.
- Assign a realm or a sequence to an Access Policy group.

You create, edit, and delete authentication realms on the Network > Authentication page under the Authentication Realms section. Figure 20-2 shows where you define authentication realms.

<table>
<thead>
<tr>
<th>Authentication Realms</th>
</tr>
</thead>
<tbody>
<tr>
<td>No authentication realms have been defined.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Global Settings</th>
<th>Authentication Type</th>
<th>Cookie</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action if Authentication Server Unavailable</td>
<td>Block all traffic if authentication fails</td>
<td></td>
</tr>
<tr>
<td>Authentication Cache (Basic Only)</td>
<td>Cache TTL: 3600 seconds</td>
<td></td>
</tr>
<tr>
<td>Cache Size</td>
<td>812 entries</td>
<td></td>
</tr>
</tbody>
</table>

Edit Global Settings...
When you create two or more realms, you can order them in an authentication sequence. For more information, see Working with Authentication Sequences, page 20-16.

Creating Authentication Realms

When you first create a realm, you choose the protocol type, either LDAP or NTLM. You can only create on NTLM realm so therefore, once an NTLM realm is defined, the appliance only allows you to create LDAP realms. After you enter the authentication settings, you can test that the parameters you entered are valid before you submit your changes. For more information about testing the authentication settings, see Testing Authentication Settings, page 20-20.

To create an authentication realm:

2. Enter a name for the authentication realm in the Realm Name field.
   
   **Note** All sequence and realm names must be unique and only contain alphanumeric characters or the space character.

3. If no NTLM realm is defined, choose the authentication protocol and scheme in the Authentication Protocol and Scheme(s) field.
4. Enter the authentication settings as necessary, depending on the protocol type.
   - For details on LDAP settings, see Table 20-12 on page 44.
   - For details on NTLM settings, see Table 20-15 on page 52.
5. You can test the parameters you entered by clicking Start Test in the Test Current Settings section.
6. Submit and commit your changes.

Editing Authentication Realms

To edit an authentication realm:
Step 1 On the Network > Authentication page, click the realm name.

Step 2 Change the name of the realm if necessary.

Step 3 Edit the authentication settings as necessary, depending on the protocol type.
   - For details on LDAP settings, see Table 20-12 on page 44.
   - For details on NTLM settings, see Table 20-15 on page 52.

Step 4 You can test the parameters you entered by clicking Start Test in the Test Current Settings section.

Step 5 Submit and commit your changes.

Deleting Authentication Realms

When you delete a realm, the Web Security appliance automatically deletes that realm from any sequence that used it. Also, any Identity policy group that depends on the deleted realm becomes disabled.

To delete an authentication realm:

Step 1 On the Network > Authentication page, click the trash can icon for the realm name.

Step 2 Confirm that you want to delete the realm by clicking Delete.

Step 3 Commit your changes.

Working with Authentication Sequences

When you create more than one realm, you can group the realms into an authentication sequence. An authentication sequence is a group of authentication realms listed in the order the Web Security appliance uses for authenticating clients.

You can perform any of the following tasks when configuring authentication sequences:
   - Create multiple authentication sequences.
   - Include one or more realms in an authentication sequence.
Include realms of different protocols in a single authentication sequence.

Assign a realm or a sequence to an Access Policy group.

You create authentication sequences on the Network > Authentication page under the Realm Sequences section. The Realm Sequences section only appears when you create two or more realms. Figure 20-3 shows where you create, edit, and delete authentication sequences Figure 20-3.

Creating Authentication Sequences

You can create an authentication sequence after you create multiple authentication realms.

To create an authentication sequence:

Step 1 On the Network > Authentication page, click Add Sequence.

The Add Realm Sequence page appears.
Working with Authentication Sequences

Step 2 Enter a name for the sequence in the Name for Realm Sequence field.

**Note** All sequence and realm names must be unique and only contain alphanumeric characters or the space character.

Step 3 In the first row of the Authentication Realm Sequence area, choose the realm name you want to include in the sequence from the Realms field.

Step 4 If you want to include more realms, click Add Row.

Step 5 Choose the realm name for any additional row you add.

**Note** You can delete a realm from the sequence by clicking the trash can icon for that row.

Step 6 When you have entered all realms in the sequence, and they are in the order you want, submit and commit your changes.

Editing Authentication Sequences

To edit an authentication sequence:

Step 1 On the Network > Authentication page, click the sequence name.

Step 2 Perform any of the following tasks as necessary:

- Change the name of the sequence.
Appliance Behavior with Multiple Authentication Realms

You can configure the Web Security appliance to attempt authenticating clients against multiple authentication servers, and against authentication servers with different authentication protocols. When you configure the appliance to authenticate against multiple authentication servers, it only requests the credentials from the clients once. This is true even when you configure the appliance to authenticate against different protocols.

You might want to configure a web policy group to authenticate against different realms if your organization acquires another organization that has its own authentication server using the same or a different authentication protocol. That way, you can create one Access Policy group for all users and assign to the policy group an authentication sequence that contains a realm for each authentication server.

Deleting Authentication Sequences

If you delete an authentication sequence, any Access Policy group that depends on the deleted sequence becomes disabled.

To delete an authentication sequence:

Step 1  On the Network > Authentication page, click the trash can icon for the sequence name.

Step 2  Confirm that you want to delete the sequence by clicking Delete.

Step 3  Commit your changes.

Appliance Behavior with Multiple Authentication Realms

You can configure the Web Security appliance to attempt authenticating clients against multiple authentication servers, and against authentication servers with different authentication protocols. When you configure the appliance to authenticate against multiple authentication servers, it only requests the credentials from the clients once. This is true even when you configure the appliance to authenticate against different protocols.

You might want to configure a web policy group to authenticate against different realms if your organization acquires another organization that has its own authentication server using the same or a different authentication protocol. That way, you can create one Access Policy group for all users and assign to the policy group an authentication sequence that contains a realm for each authentication server.

• Add a new realm by clicking Add Row.
• Delete a realm by clicking the trash can icon.
• Change the order of the realms by clicking the arrow icon in the Order column for the realm.

Step 3  Submit and commit your changes.
When you assign an authentication sequence with multiple realms to a policy group and a client sends a content request, the appliance performs the following actions:

**Step 1** The appliance gets the credentials from the client.

**Step 2** The appliance attempts to authenticate the client against the authentication server(s) defined in the first realm in the sequence.

**Step 3** If the client credentials do not match a user in the servers defined in the first realm, it tries to authenticate against the authentication server(s) in the next realm in the sequence.

**Step 4** The appliance continues trying to authenticate the client against servers in the next realms until it either succeeds or runs out of authentication realms.

**Step 5** When authentication succeeds, the appliance passes the content response to the client.

**Step 6** When the appliance fails to authenticate the client against any authentication realm in the sequence, the appliance does not allow the client to connect to the destination server. Instead, it displays an error message to the client.

**Tip:** For optimal performance, configure clients on a subnet to be authenticated in a single realm.

### Testing Authentication Settings

When you create or edit an authentication realm, you enter a lot of configuration settings to connect to the authentication server. You can test the settings you enter before submitting the changes to verify you entered the connection information correctly.

You can test authentication setting from either the CLI or the web interface:

- **Web interface.** Use **Start Test** when you create or edit an authentication realm. For more information, see Testing Authentication Settings in the Web Interface, page 20-22.

- **CLI command.** Use the **testauthconfig** command. For more information, see Testing Authentication Settings in the CLI, page 20-23.
Testing Process

When you test authentication settings, the Web Security appliance first verifies that the settings you entered for the realm are in valid formats. For example, if a field requires a string and it currently contains a numeric value, the appliance informs you of that error.

If all fields contain valid values, the appliance performs different steps, depending on the authentication protocol. If the realm contains multiple authentication servers, the appliance goes through the testing process for each server in turn.

The appliance continues testing all servers in the realm and determines as many failures as possible for each server. It reports the testing outcome of each server in the realm.

LDAP Testing

The appliance performs the following steps when you test LDAP authentication settings:

- **Step 1** It ensures that the LDAP server is listening on the specified LDAP port.
- **Step 2** If Secure LDAP is selected, the appliance ensures the LDAP server supports secure LDAP.
- **Step 3** It performs an LDAP query using the supplied Base DN, User Name Attribute, and User Filter Query.
- **Step 4** If the realm includes Bind Parameters, the appliance validates them by forming an LDAP query with the Bind Parameters.
- **Step 5** If Group Authorization is provided, the appliance ensures that the specified group attributes are valid by fetching the groups from the server.

NTLM Testing

The appliance performs the following steps when you test NTLM authentication settings:

- **Step 1** It ensures that the specified Active Directory server is reachable and responds to queries.
Testing Authentication Settings

Step 2 It ensures that a DNS lookup on the Active Directory domain is successful since the Active Directory domain must be a DNS domain name and not a WINS domain name.

Step 3 It ensures the system time of the appliance and the system time of the Active Directory server are within three minutes of each other.

Step 4 It validates the user credentials by generating a kerberos ticket.

Step 5 It validates whether the user has the proper privileges to add the Web Security appliance to the Active Directory domain.

Step 6 It validates whether you can fetch the groups within the domain.

Testing Authentication Settings in the Web Interface

You verify the authentication settings in the Test Current Settings section when you create or edit an authentication realm.

Figure 20-4 shows where you verify the authentication settings in the web interface.

After you enter all settings, click **Start Test**. The appliance uses the connection information entered to attempt to connect to the authentication server. It displays the status of the test below **Start Test**.

**Start Test** changes to **Stop Test** while the appliance tests the settings against the authentication servers. If the testing takes too much time and you already know it is going to fail, you can click **Stop Test** to stop the testing process and edit the settings.

Figure 20-5 shows the testing results for an LDAP authentication realm.
Testing Authentication Settings in the CLI

You can use the `testauthconfig` CLI command to test authentication settings defined for a given realm. The command syntax is:

```
testauthconfig [-d level] [realm name]
```

Running the command without any option causes the appliance to list the configured authentication realms from which you can make a selection.

The debug flag (`-d`) controls the level of debug information. The levels can range between 0-10. If unspecified, the appliance uses a level of 0. With level 0, the command will return success or failure. If the test settings fail, the command will list the cause of the failure.

Note

Cisco recommends you use level 0. Only use a different debug level when you need more detailed information to troubleshoot.

For more information about the `testauthconfig` command, see Web Security Appliance CLI Commands, page 27-8.

Configuring Global Authentication Settings

Some authentication settings are independent of any realm you define. For example, you can configure whether or not clients send authentication credentials to the Web Security appliance securely, even when using Basic authentication scheme. For more information, see Sending Authentication Credentials Securely, page 20-37.
Figure 20-6 shows the global authentication settings on the Network > Authentication page.

### Authentication

**Authentication Realms**

<table>
<thead>
<tr>
<th>Realm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No authentication realms have been defined.</td>
</tr>
</tbody>
</table>

**Global Authentication Settings**

- Action if Authentication Service Unavailable: Block all traffic if authentication fails
- Failed Authentication Handling: Log Guest User by IP Address
- Re-authentication: Disabled
- Basic Authentication Token TTL: 3600

**Transparent Proxy Next Authentication Settings**

- Credential Encryption: Disabled
- Redirect Hostname: is1 IronPort-01
- Credential Cache Options: Enabled
- Surrogate Timeout: 3600 seconds
- Client IP Idle Timeout: 3600 seconds
- Cache Size: 65536 entries
- User Session Restrictions: Disabled

**Secure Authentication Certificate**

- Common name: IronPort Appliance Demo Certificate
- Country: US
- Expiration Date: May 1 2027/50 00:00 GMT
- Basic Constraints: Not Critical

---

**Note**

The global authentication settings you can configure changes according to the Web Proxy deployment. You can configure more settings when it is deployed in transparent mode than in explicit forward mode.

To configure global authentication settings:

**Step 1**

On the Network > Authentication page, click **Edit Global Settings**.

The Edit Global Authentication Settings page appears with two main sections, one labeled Global Authentication Settings and the other labeled for the proxy deployment type, either transparent or forward.

Figure 20-7 on page 25 shows the Global Authentication Settings section.
Step 2 Edit the settings in the Global Authentication Settings section as defined in Table 20-8.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action if Authentication Service Unavailable</strong></td>
<td>Choose one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Permit traffic to proceed without authentication.</strong> Processing continues as if the user was authenticated.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Block all traffic if user authentication fails.</strong> Processing is discontinued and all traffic is blocked.</td>
</tr>
<tr>
<td><strong>Failed Authentication Handling</strong></td>
<td>When you grant users guest access in an Identity policy, this setting determines how the Web Proxy identifies and logs the user as a guest in the access logs. For more information on granting users guest access, see <strong>Allowing Guest Access to Users Who Fail Authentication</strong>, page 7-13.</td>
</tr>
</tbody>
</table>
The remaining authentication settings you can configure depends on how the Web Proxy is deployed, in transparent or explicit forward mode.

**Figure 20-8 on page 27** shows where you configure the global authentication settings when the Web Proxy is deployed in transparent mode.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-authentication</td>
<td>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. 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. <strong>Note:</strong> 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. For more information, see Allowing Users to Re-Authenticate, page 20-39.</td>
</tr>
<tr>
<td>Basic Authentication Token TTL</td>
<td>Controls the length of time that user credentials are stored in the cache before revalidating them with the authentication server. 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.</td>
</tr>
</tbody>
</table>
### Configuring Global Authentication Settings

<table>
<thead>
<tr>
<th>Transparent Proxy Mode Authentication Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Encryption:</td>
</tr>
<tr>
<td>HTTPS Redirect Port:</td>
</tr>
<tr>
<td>Redirect Hostname:</td>
</tr>
<tr>
<td>Credential Cache Options:</td>
</tr>
<tr>
<td>Surrogate Timeout:</td>
</tr>
<tr>
<td>Client IP Idle Timeout:</td>
</tr>
<tr>
<td>If this value is greater than the Surrogate Timeout value, this setting has no effect.</td>
</tr>
<tr>
<td>Cache Size:</td>
</tr>
<tr>
<td>User Session Redirections:</td>
</tr>
<tr>
<td>Restriction Timeout:</td>
</tr>
</tbody>
</table>

**Advanced**

- **Common name:** IronPort Appliance Deto Certificate
- **Organization:** IronPort Systems, Inc.
- **Country:** US
- **Expiration Date:** May 1, 2016 7:55:00 GMT
- **Basic Constraints:** Not Critical

**Certificate:**

**Key:**

- Private key must be unencrypted.

*Upload Files:*

Uploading a new pair of certificate and key will replace the currently used certificate and key as displayed above.

---

Cisco IronPort AsyncOS 7.1 for Web User Guide

OL-23207-01

20-27
Step 3 If the Web Proxy is deployed in transparent mode, edit the settings in Table 20-9.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Encryption</td>
<td>This setting specifies whether or not the client sends the login credentials to the Web Proxy through an encrypted HTTPS connection.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Sending Authentication Credentials Securely, page 20-37.</td>
</tr>
<tr>
<td>HTTPS Redirect Port</td>
<td>Specify a TCP port to use for redirecting requests for authenticating users over an HTTPS connection.</td>
</tr>
<tr>
<td></td>
<td>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 SaaS Access Control and SaaS users are prompted to authenticate.</td>
</tr>
</tbody>
</table>
Redirect Hostname

Enter the short hostname of the network interface on which the Web Proxy listens for incoming connections.

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.

You can enter either the following values:

- **Single word hostname.** You can enter the single word hostname that is DNS resolvable by the client and the Web Security appliance. This allows clients to achieve true single sign-on with Internet Explorer without additional browser side setup. Be sure to enter the single word hostname that is DNS resolvable by the client and the Web Security appliance.

  For example, if your clients are in domain mycompany.com and the interface on which the Web Proxy is listening has a full hostname of proxy.mycompany.com, then you should enter proxy in this field. Clients perform a lookup on proxy and they should be able to resolve proxy.mycompany.com.

- **Fully qualified domain name (FQDN).** You can also enter the FQDN or IP address in this field. However, if you do that and want true single sign-on for Internet Explorer and Firefox browsers, you must ensure that the FQDN or IP address is added to the client’s Trusted Sites list in the client browsers. The default value is the FQDN of the M1 or P1 interface, depending on which interface is used for proxy traffic.
## Configuring Global Authentication Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Cache</td>
<td>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). 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.</td>
</tr>
<tr>
<td>Options:</td>
<td></td>
</tr>
<tr>
<td>Surrogate Timeout</td>
<td></td>
</tr>
<tr>
<td>Credential Cache</td>
<td>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. 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. You might want to use this setting to reduce the vulnerability of users who leave their computers.</td>
</tr>
<tr>
<td>Options:</td>
<td></td>
</tr>
<tr>
<td>Client IP Idle Timeout</td>
<td></td>
</tr>
<tr>
<td>Credential Cache</td>
<td>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.</td>
</tr>
<tr>
<td>Options:</td>
<td></td>
</tr>
<tr>
<td>Cache Size</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Global Authentication Settings

**User Session Restrictions**

This setting specifies whether or not authenticated users are allowed to access the Internet from multiple IP addresses simultaneously.

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.

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.

You can a specific user or all users from the authentication cache using the `authcache` CLI command.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Session Restrictions</td>
<td>This setting specifies whether or not authenticated users are allowed to access the Internet from multiple IP addresses simultaneously. 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. 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. You can a specific user or all users from the authentication cache using the <code>authcache</code> CLI command.</td>
</tr>
</tbody>
</table>

**Advanced**

When using Credential Encryption or SaaS Access Control, you can choose whether the appliance uses the digital certificate and key shipped with the appliance (the IronPort Appliance Demo Certificate) or a digital certificate and key you upload here.

To upload a digital certificate and key, click **Browse** and navigate to the necessary file on your local machine. Then click **Upload Files** after you select the files you want.

For more information, see *Uploading Certificates and Keys to Use with Credential Encryption and SaaS Access Control, page 20-38.*

---

*Figure 20-9 on page 32 shows where you configure the global authentication settings when the Web Proxy is deployed in explicit forward mode.*
### Configuring Global Authentication Settings

#### Forward Proxy Node Authentication Settings

<table>
<thead>
<tr>
<th>Credential Encryption:</th>
<th>SSL Proxy (No Encryption)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS Redirect Port:</td>
<td>443</td>
</tr>
</tbody>
</table>

**Redirect Hostname:** To achieve true single sign-on for Internet Explorer, use the short hostname or NetBIOS name instead of the fully qualified domain name.
```
http://myftp.ironport.com
```

**Credential Cache Options:**

| Surrogate Timeout: | 3000 seconds |
| Client IP Idle Timeout: | 300 seconds |

If this value is greater than the Surrogate Timeout value, this setting has no effect.

**Cache Size:** 1000 number of entries

**User Session Restrictions:**

- Prohibit an unauthenticated user from accessing the Internet from a different IP address

- **Restriction Timeout:** 100 seconds

### Advanced

**Common Name:** IronPort Appliance Demo Certificate

**Organization:** IronPort Systems, Inc.

**Organizational Unit:**

**Country:** US

**Expiration Date:** May 12 23:59:59 2016 GMT

**Basic Constraints:** Not Critical

**Certificate:**

**Key:**

Private key must be unencrypted.

**Upload File:**

Uploading a new pair of certificate and key will replace the currently used certificate and key as displayed above.
Step 4  If the Web Proxy is deployed in explicit forward mode, edit the settings in Table 20-10.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Encryption</td>
<td>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. 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. For more information, see Sending Authentication Credentials Securely, page 20-37.</td>
</tr>
<tr>
<td>HTTPS Redirect Port</td>
<td>Specify a TCP port to use for redirecting requests for authenticating users over an HTTPS connection. 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 SaaS Access Control and SaaS users are prompted to authenticate.</td>
</tr>
</tbody>
</table>
Redirect Hostname

Enter the short hostname of the network interface on which the Web Proxy listens for incoming connections.

When you enable Authentication Mode above, the Web Proxy uses this hostname in the redirection URL sent to clients for authenticating users.

You can enter either of the following values:

- **Single word hostname.** You can enter the single word hostname that is DNS resolvable by the client and the Web Security appliance. This allows clients to achieve true single sign-on with Internet Explorer without additional browser side setup.
  
  Be sure to enter the single word hostname that is DNS resolvable by the client and the Web Security appliance.
  
  For example, if your clients are in domain mycompany.com and the interface on which the Web Proxy is listening has a full hostname of proxy.mycompany.com, then you should enter proxy in this field. Clients perform a lookup on proxy and they should be able to resolve proxy.mycompany.com.

- **Fully qualified domain name (FQDN).** You can also enter the FQDN or IP address in this field. However, if you do that and want true single sign-on for Internet Explorer and Firefox browsers, you must ensure that the FQDN or IP address is added to the client’s Trusted Sites list in the client browsers.
  
  The default value is the FQDN of the M1 or P1 interface, depending on which interface is used for proxy traffic.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect Hostname</td>
<td>Enter the short hostname of the network interface on which the Web Proxy listens for incoming connections.</td>
</tr>
<tr>
<td></td>
<td>When you enable Authentication Mode above, the Web Proxy uses this hostname in the redirection URL sent to clients for authenticating users.</td>
</tr>
<tr>
<td></td>
<td>You can enter either of the following values:</td>
</tr>
<tr>
<td></td>
<td><strong>Single word hostname.</strong> You can enter the single word hostname that is DNS resolvable by the client and the Web Security appliance. This allows</td>
</tr>
<tr>
<td></td>
<td>clients to achieve true single sign-on with Internet Explorer without additional browser side setup.</td>
</tr>
<tr>
<td></td>
<td>Be sure to enter the single word hostname that is DNS resolvable by the client and the Web Security appliance.</td>
</tr>
<tr>
<td></td>
<td>For example, if your clients are in domain mycompany.com and the interface on which the Web Proxy is listening has a full hostname of proxy.</td>
</tr>
<tr>
<td></td>
<td>proxy.mycompany.com, then you should enter proxy in this field. Clients perform a lookup on proxy and they should be able to resolve proxy.</td>
</tr>
<tr>
<td></td>
<td><strong>Fully qualified domain name (FQDN).</strong> You can also enter the FQDN or IP address in this field.</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>is added to the client’s Trusted Sites list in the client browsers.</td>
</tr>
<tr>
<td></td>
<td>The default value is the FQDN of the M1 or P1 interface, depending on which interface is used for proxy traffic.</td>
</tr>
</tbody>
</table>
### Configuring Global Authentication Settings

#### Credential Cache Options:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surrogate Timeout</td>
<td>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). 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.</td>
</tr>
<tr>
<td>Client IP Idle Timeout</td>
<td>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. 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. You might want to use this setting to reduce the vulnerability of users who leave their computers.</td>
</tr>
<tr>
<td>Cache Size</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Configuring Global Authentication Settings

#### User Session Restrictions

This setting specifies whether or not authenticated users are allowed to access the Internet from multiple IP addresses simultaneously.

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.

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.

You can a specific user or all users from the authentication cache using the `authcache CLI command`.

#### Advanced

When using Credential Encryption or SaaS Access Control, you can choose whether the appliance uses the digital certificate and key shipped with the appliance (the IronPort Appliance Demo Certificate) or a digital certificate and key you upload here.

To upload a digital certificate and key, click `Browse` and navigate to the necessary file on your local machine. Then click `Upload Files` after you select the files you want.

For more information, see Uploading Certificates and Keys to Use with Credential Encryption and SaaS Access Control, page 20-38.

---

**Step 5**  
Submit and commit your changes.
Sending Authentication Credentials Securely

When authentication is used to identify clients using the Web, the client applications send the authentication credentials to the Web Proxy, which in turn passes them to the authentication server. How the credentials are passed from the clients to the Web Proxy depends on the authentication scheme used:

- **NTLMSSP.** The credentials are always passed to the Web Proxy securely. They are encrypted using a key specified by the Active Directory server and sent over HTTP.

- **Basic.** By default, the credentials are passed to the Web Proxy insecurely. They are encoded, but not encrypted, and sent over HTTP. However, you can configure the Web Security appliance so clients send authentication credentials securely. This works for both LDAP and NTLM Basic authentication.

When you configure the appliance to use credential encryption for Basic authentication, the Web Proxy redirects the client back to the Web Proxy, but this time using an encrypted connection using HTTPS. The client application makes either a GET or a CONNECT request depending on how the requests are forwarded to the appliance (explicitly or transparently) and how the client application is configured to forward HTTPS requests, either using the Web Proxy or not.

Then, using the secure HTTPS connection, the clients send the authentication credentials. The appliance uses its own certificate and private key to create an HTTPS connection with the client by default. Most browsers will warn users that the certificate is not valid. To prevent users from seeing the invalid certificate message, you can upload a certificate and key pair your organization uses. When you upload a certificate and key, the private key must be unencrypted. For information about uploading a certificate and key, see Uploading Certificates and Keys to Use with Credential Encryption and SaaS Access Control, page 20-38.

To configure the appliance to use credential encryption, enable the Credential Encryption setting in the global authentication settings. For more information, see Configuring Global Authentication Settings, page 20-23. You can also use the `advancedproxyconfig > authentication` CLI command. For more information, see Advanced Proxy Configuration, page 5-30.
Uploading Certificates and Keys to Use with Credential Encryption and SaaS Access Control

When credential encryption is enabled or when using SaaS Access Control, the appliance uses a digital certificate to securely establish a connection with the client application. By default, the Web Security appliance uses the “IronPort Appliance Demo Certificate” that comes installed. However, client applications are not programmed to recognize this certificate, so you can upload a digital certificate to the appliance that your applications recognize automatically.

Use the Advanced section on the Network > Authentication page to upload the certificate and key.

For more information on obtaining a certificate and private key pair to upload, see Obtaining Certificates, page 26-33.

Note

Any certificate and key you upload on the Network > Authentication page is only used for establishing secure connections with clients for credential encryption and authenticating SaaS users using SaaS Access Control. The certificate and key are not used for establishing secure HTTPS sessions when connecting to the Web Security appliance web interface. For more information on uploading a certificate and key pair for HTTPS connections to the web interface, see Installing a Server Digital Certificate, page 26-32.

For more information on SaaS Access Control, see Authenticating SaaS Users, page 14-4.

Accessing HTTPS and FTP Sites with Credential Encryption Enabled

Credential encryption works because the Web Proxy redirects clients to the Web Proxy itself for authentication using an HTTPS connection. After successful authentication, the Web Proxy redirects clients back to the original web site. 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 when the client accesses HTTPS sites or FTP servers using FTP over HTTP does not work.

- **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.

Because of this, you should configure the appliance to use IP addresses as the surrogate when credential encryption is enabled.

**Note** Authentication does not work with HTTPS and FTP over HTTP requests when credential encryption is enabled and configured to use cookies as the surrogate type. Therefore, with this configuration setup, HTTPS and FTP over HTTP requests only match Access Policies that do not require authentication. Typically, they often match the global Access Policy since it never requires authentication.

---

## Allowing Users to Re-Authenticate

AsyncOS for Web can block users from accessing different categories of websites depending on who is trying to access a website. In these cases, users successfully authenticate, but they are not authorized to access certain websites due to configured URL filtering in the applicable Access Policy. You can allow these authenticated users another opportunity to access the web if they fail authorization.

**Note** Only authenticated users are allowed to re-authenticate, not unauthenticated users.

You might want to do this for shared workstations that have multiple users, but the default account has limited access. If the default account on the workstation is blocked from a website due to restrictive URL filtering, the user can enter different authentication credentials that allow broader, more privileged access.

To do this, enable the “Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction” global authentication setting. The user sees a block page that includes a link that allows them to enter new authentication credentials. The Web Proxy evaluates those credentials against the
authentication realms defined in the applicable Identity group, and if the new credentials allow greater access, the requested page appears in the browser. For more information, see Configuring Global Authentication Settings, page 20-23.

**Note**
The Web Proxy evaluates the new credentials against the authentication realms defined in the applicable Identity group only. It does not compare them against all other Identity groups.

When a more privileged user authenticates and gets access, the Web Proxy caches the privileged 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.** The Web Proxy requests authentication for every new connection, but most browsers will cache the privileged user credentials and authenticate without prompting the user until the browser is closed. However, because the Web Proxy requests authentication for every new connection, there is an increased impact on the authentication server when using NTLMSSP.

**Note**
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. For more information, see Working with User Defined End-User Notification Pages, page 15-14.

### Using Re-Authentication with Internet Explorer

When you enable re-authentication and clients use Microsoft Internet Explorer, you need to verify certain settings to ensure re-authentication works properly with Internet Explorer. Due to a known issue with Internet Explorer, re-authentication does not work properly under the following circumstances:

- Internet Explorer is configured to use the Web Security appliance as a proxy.
• The Web Security appliance uses NTLMSSP authentication.
• The Web Security appliance uses cookies for authentication surrogates, but is not configured for credential encryption.
• The Web Proxy is deployed in explicit forward mode, or it is deployed in transparent mode and the “Apply same surrogate settings to explicit forward requests” option is enabled in the applicable Identity group.

Problems occur when authentication is required to access the site, and may occur either when initially requesting the site or when re-authenticating to try to access the site.

To work around these problems, enable credential encryption on the Network > Authentication page.

### Using Re-Authentication with PAC Files

When you enable re-authentication and configure client applications to use a PAC file, you may need to verify certain settings to ensure re-authentication works properly with the PAC file.

Re-authentication does not work properly under the following circumstances:

• Client browsers are configured to use a PAC file, and the PAC file is designed to bypass the Web Proxy for internal web servers. Instead of instructing the browser to explicitly send requests to the Web Proxy, it instructs the browser to directly send the request to the destination server.
• The Web Security appliance uses IP addresses for authentication surrogates or no surrogates, and credential encryption is not enabled.
• The Web Proxy is deployed in explicit forward mode, or it is deployed in transparent mode and the “Apply same surrogate settings to explicit forward requests” option is enabled for the applicable Identity group.

Problems occur because re-authentication requires clients to be redirected to the Web Proxy for authentication, but the PAC file bypasses all requests to internal web servers, including the Web Security appliance.

To work around these problems, edit the PAC file so that the function FindProxyForURL() returns “PROXY x.x.x.x:80” when the host IP address is x.x.x.x. The port number you specify in the return should be the same port configured for other destinations.
Note

If the Web Security appliance uses cookies for authentication surrogates, Cisco recommends enabling credential encryption. For more information, see Using Re-Authentication with Internet Explorer, page 20-40.

## Tracking Authenticated Users

Table 20-11 describes which authentication surrogates are supported with other configurations and different types of requests (explicitly forwarded and transparently redirected).

<table>
<thead>
<tr>
<th>Surrogate Types</th>
<th>Explicit Requests</th>
<th>Transparent Requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Encryption:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disabled</td>
<td>HTTPS &amp; FTP over HTTP</td>
<td>HTTPS &amp; FTP over HTTP</td>
</tr>
<tr>
<td>Enabled</td>
<td>HTTP</td>
<td>HTTP</td>
</tr>
<tr>
<td>Protocol:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Surrogate</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IP-based</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cookie-based</td>
<td>Yes</td>
<td>Yes***</td>
</tr>
</tbody>
</table>

* Works after the client makes a request to an HTTP site and is authenticated, or when the client makes a request to an HTTPS site and the Identity is configured to decrypt the first HTTPS request for authentication purposes. When the HTTPS Proxy is configured to deny the first HTTPS request, all requests to HTTPS sites before authentication happens for a previous request are dropped.

** When cookie-based authentication is used, the Web Proxy cannot authenticate the user for HTTPS and FTP over HTTP transactions. Due to this limitation, all HTTPS and FTP over HTTP requests bypass authentication, so authentication is not requested at all. For more information on how HTTPS requests are assigned Identity and non-Identity policy groups, see Understanding How Authentication Affects HTTPS and FTP over HTTP Requests, page 7-6.
*** No surrogate is used in this case even though cookie-based surrogate is configured.

**LDAP Authentication**

The Lightweight Directory Access Protocol (LDAP) server database is a repository for employee directories. These directories include the names of employees along with various types of personal data such as a phone number, email address, and other information that is exclusive to the individual employee. The LDAP database is composed of objects containing attributes and values. Each object name is referred to as a distinguished name (DN). The location on the LDAP server where a search begins is called the Base Distinguished Name or base DN.

The appliance supports standard LDAP server authentication and Secure LDAP authentication. Support for LDAP allows established installations to continue using their LDAP server database to authenticate users.

For Secure LDAP, the appliance supports LDAP connections over SSL. The SSL protocol is an industry standard for ensuring confidentiality. SSL uses key encryption algorithms along with Certificate Authority (CA) signed certificates to provide the LDAP servers a way to verify the identity of the appliance.

**Note**

AsyncOS for Web only supports 7-bit ASCII characters for passwords when using the Basic authentication scheme. Basic authentication fails when the password contains characters that are not 7-bit ASCII.

**Changing Active Directory Passwords**

After Active Directory LDAP users change their account passwords, the Active Directory LDAP server authenticates them with their current or previous password, depending on the Active Directory server configuration.

If you want users to only be able to authenticate with their new password, you can reboot the Active Directory server or, you can wait for the Active Directory server to time out the old passwords.
Table 20-12 describes the authentication settings you define when you choose LDAP authentication.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Version</td>
<td>Choose the version of LDAP, and choose whether or not to use Secure LDAP. The appliance supports LDAP version 2, and LDAP version 3 software. Secure LDAP requires LDAP version 3. Choose whether or not this LDAP server support Novell eDirectory to use with transparent user identification. For more information, see Identifying Users Transparently, page 7-16.</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>Enter the LDAP server IP address or hostname and its port number. You can specify up to three servers. The hostname must be a fully-qualified domain name. For example, ldap.example.com. An IP address is required only if the DNS servers configured on the appliance cannot resolve the LDAP server hostname. The default port number for Standard LDAP is 389. The default number for Secure LDAP is 636. 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. Note: When you configure multiple authentication servers in the realm, the appliance attempts to authorize with up to three authentication servers before failing to authenticate the transaction within that realm.</td>
</tr>
</tbody>
</table>
### LDAP Persistent Connections

(under the Advanced section)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Persistent Connections</td>
<td>Choose one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Use persistent connections (unlimited)</strong>. Use existing connections. If no connections are available a new connection is opened.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Use persistent connections</strong>. Use existing connections to service the number of requests specified. When the maximum is reached, establish a new connection to the LDAP server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Do not use persistent connections</strong>. Always create a new connection to the LDAP server.</td>
</tr>
</tbody>
</table>
User Authentication

Enter values for the following fields:

**Base Distinguished Name (Base DN)**

The LDAP database is a tree-type directory structure and the appliance uses the Base DN to navigate to the correct location in the LDAP directory tree to begin a search. A valid Base DN filter string is composed of one or more components of the form `object-value`. For example `dc=companyname, dc=com`.

**User Name Attribute**

Choose one of the following values:

- `uid`, `cn`, and `sAMAccountName`. Unique identifiers in the LDAP directory that specify a username.
- `custom`. A custom identifier such as `UserAccount`.

**User Filter Query**

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.

Choose one of the following values:

- `none`. Filters any user.
- `custom`. Filters a particular group of users.
You can use the user group membership information stored in an LDAP directory to apply a policy group to a group of users. To do this, enable group authorization in an LDAP authentication realm and group users by one of the following LDAP object types:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Credentials</td>
<td>Choose whether or not the authentication server accepts anonymous queries.</td>
</tr>
<tr>
<td></td>
<td>If the authentication server does accept anonymous queries, choose Server Accepts Anonymous Queries.</td>
</tr>
<tr>
<td></td>
<td>If the authentication server does not accept anonymous queries, choose Use Bind DN and then enter the following information:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bind DN.</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Password.</strong> The password associated with the user you enter in the Bind DN field.</td>
</tr>
<tr>
<td>Group Authorization</td>
<td>Choose whether or not to enable LDAP group authorization. When you enable LDAP group authorization, you can group users by group object or user object.</td>
</tr>
<tr>
<td></td>
<td>For more information on configuring this section, see LDAP Group Authorization, page 20-47.</td>
</tr>
</tbody>
</table>

**LDAP Group Authorization**

You can use the user group membership information stored in an LDAP directory to apply a policy group to a group of users. To do this, enable group authorization in an LDAP authentication realm and group users by one of the following LDAP object types:
Group object. Sometimes, group membership information is stored in the group object, which has an attribute (such as “member”) to list all users that belong to the group. Define authorized users by group object when the group object contains all users you need to define. For more information on how to define authorized users by group object, see Table 20-13 on page 49.

User object. Sometimes, group membership information is stored in the user object, which has an attribute (such as “memberOf”) that lists all groups to which a user belongs. You might want to define authorized users by user object when the authentication server does not store the member information in the group object or if it does not have a group object. For more information on how to define authorized users by user object, see Table 20-14 on page 50.

Note The user object must not contain any special character.

When you configure group authorization in an LDAP authentication realm, be sure you uniquely identify a group object in the LDAP server. If the search for a group DN returns multiple entries, the Web Security appliance only uses the first entry returned. You uniquely identify a group object using the following fields:

- Base DN
- Attribute that contains the group name
- Query string to determine if object is a group

When you create an LDAP authentication realm with user object based group authorization against an Active Directory server, the user object does not contain the primary group that the user is a member of, for example “Domain Users.” It only contains the other defined groups. Therefore, policy groups might not match these users under the following conditions:

- An Identity policy group specifies an LDAP realm with user attribute based group authentication.
- A non-Identity policy group uses the Identity policy group and the primary group is configured as an authorized group in the Active Directory server.
Table 20-13 describes the group object settings.

<table>
<thead>
<tr>
<th>Group Object Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Membership Attribute Within Group Object</td>
<td>Choose the LDAP attribute which lists all users that belong to this group.</td>
</tr>
<tr>
<td></td>
<td>Choose one of the following values:</td>
</tr>
<tr>
<td></td>
<td>•  <strong>member</strong> and <strong>uniquemember</strong>. Unique identifiers in the LDAP directory that specify group members.</td>
</tr>
<tr>
<td></td>
<td>•  <strong>custom</strong>. A custom identifier such as <strong>UserInGroup</strong>.</td>
</tr>
<tr>
<td>Attribute that Contains the Group Name</td>
<td>Choose the LDAP attribute which specifies the group name that can be used in the policy group configuration.</td>
</tr>
<tr>
<td></td>
<td>Choose one of the following values:</td>
</tr>
<tr>
<td></td>
<td>•  <strong>cn</strong>. A unique identifier in the LDAP directory that specifies the name of a group.</td>
</tr>
<tr>
<td></td>
<td>•  <strong>custom</strong>. A custom identifier such as <strong>FinanceGroup</strong>.</td>
</tr>
<tr>
<td>Query String to Determine if Object is a Group</td>
<td>Choose an LDAP search filter that determines if an LDAP object represents a user group.</td>
</tr>
<tr>
<td></td>
<td>Choose one of the following values:</td>
</tr>
<tr>
<td></td>
<td>•  <strong>objectclass=groupofnames</strong></td>
</tr>
<tr>
<td></td>
<td>•  <strong>objectclass=groupofuniquenames</strong></td>
</tr>
<tr>
<td></td>
<td>•  <strong>objectclass=group</strong></td>
</tr>
<tr>
<td></td>
<td>•  <strong>custom</strong>. A custom filter such as <strong>objectclass=person</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The query defines the set of authentication groups which can be used in policy groups.</td>
</tr>
</tbody>
</table>
Table 20-14 describes the user object settings.

<table>
<thead>
<tr>
<th>User Object Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Membership</td>
<td>Choose the attribute which list all the groups that this user belongs to.</td>
</tr>
<tr>
<td>Attribute Within User Object</td>
<td>Choose one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>memberof</strong>. Unique identifiers in the LDAP directory that specify user members.</td>
</tr>
<tr>
<td></td>
<td>• <strong>custom</strong>. A custom identifier such as <code>UserInGroup</code>.</td>
</tr>
<tr>
<td>Group Membership</td>
<td>Specify whether the group membership attribute is a distinguished name (DN) which refers to an LDAP object. For Active Directory servers, enable this option. When this is enabled, you must configure the subsequent settings.</td>
</tr>
<tr>
<td>Attribute is a DN</td>
<td></td>
</tr>
<tr>
<td>Attribute that</td>
<td>When the group membership attribute is a DN, this specifies the attribute that can be used as group name in policy group configurations.</td>
</tr>
<tr>
<td>Contains the Group</td>
<td>Choose one of the following values:</td>
</tr>
<tr>
<td>Name</td>
<td>• <strong>cn</strong>. A unique identifier in the LDAP directory that specifies the name of a group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>custom</strong>. A custom identifier such as <code>FinanceGroup</code>.</td>
</tr>
<tr>
<td>Query String to</td>
<td>Choose an LDAP search filter that determines if an LDAP object represents a user group.</td>
</tr>
<tr>
<td>Determine if Object</td>
<td>Choose one of the following values:</td>
</tr>
<tr>
<td>is a Group</td>
<td>• <strong>objectclass=groupofnames</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>objectclass=groupofuniquenames</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>objectclass=group</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>custom</strong>. A custom filter such as <code>objectclass=person</code>.</td>
</tr>
<tr>
<td>Note:</td>
<td>The query defines the set of authentication groups which can be used in Web Security Manager policies.</td>
</tr>
</tbody>
</table>
NTLM Authentication

The NT Lan Manager (NTLM) authenticates users with an encrypted challenge-response sequence that occurs between the appliance and a Microsoft Windows domain controller. The NTLM challenge-response handshake occurs when a web browser attempts to connect to the appliance and before data is delivered.

When you configure an NTLM authentication realm, you do not specify the authentication scheme. Instead, you choose the scheme at the Access Policy group level when you configure the policy member definition. This allows you to choose different schemes for different policy groups. When you create or edit the policy group, you can choose one of the following schemes:

- Use NTLMSSP
- Use Basic or NTLMSSP
- Use Basic

Note
AsyncOS for Web only supports 7-bit ASCII characters for passwords when using the Basic authentication scheme. Basic authentication fails when the password contains characters that are not 7-bit ASCII.

Working with Multiple Active Directory Domains

AsyncOS allows you to create only one NTLM authentication realm. If your organization has multiple Active Directory domains, you can authenticate users in all domains if the following conditions exist:

- All Active Directory domains must exist in a single forest.
- There must be a trust relationship among all domains in the forest.

When you define policy group membership by group name, the web interface only displays Active Directory groups in the domain where AsyncOS created a computer account when joining the domain. To create a policy group for users in a different domain in the forest, manually enter the domain and group name in the web interface.
NTLM Authentication Settings

Table 20-15 describes the authentication settings you define when you choose NTLM authentication.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Server</td>
<td>Enter the Active Directory server IP address or hostname. You can specify up to three servers. The hostname must be a fully-qualified domain name. For 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. Note: 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.</td>
</tr>
</tbody>
</table>
| Active Directory Account | Enter the following Active Directory account information:  
  - Active Directory server domain name.  
  - NetBIOS domain name. You only need to enter the NetBIOS domain name if the network uses NetBIOS. This field only appears when the NTLM security mode is set to “domain” using the setntlmsecuritymode CLI command.  
  - Computer account location.  
  Note: You must click **Join Domain** to enter an Active Directory username and password.  
  For more information about entering the Active Directory account information, see **Joining the Active Directory Domain**, page 20-53. |
When you configure an NTLM realm, you must enter information to join the Active Directory domain to set up a computer account in the domain. An Active Directory computer account is an account that uniquely identifies the computer on the domain. It is also referred to as a machine trust account.

After you enter the Active Directory account information in the authentication realm, click the **Join Domain** button to set up a computer account. Use the Location field to define the organizational directory where AsyncOS should create the computer account in the Active Directory domain.

**Figure 20-10 on page 54** shows where you join an Active Directory domain.

### Joining the Active Directory Domain

When you configure an NTLM realm, you must enter information to join the Active Directory domain to set up a computer account in the domain. An Active Directory computer account is an account that uniquely identifies the computer on the domain. It is also referred to as a machine trust account.

After you enter the Active Directory account information in the authentication realm, click the **Join Domain** button to set up a computer account. Use the Location field to define the organizational directory where AsyncOS should create the computer account in the Active Directory domain.

**Figure 20-10 on page 54** shows where you join an Active Directory domain.
Joining an Active Directory Domain

When you click **Join Domain**, you are prompted to enter login credentials for the Active Directory server. The login information is used only to create the Active Directory computer account and is not saved. Enter the login information and click **Create Account**.

**Note**
You must enter the sAMAccountName user name for the Active Directory user. Also, verify that users enter their sAMAccountName user name when they log in to their computers.

Once an account is created, the status of the account creation is displayed below the Join Domain button. If the account creation fails, the status and reason for error is displayed.
Also, when you view all realms on the Network > Authentication page, the appliance displays warning text in red saying that the domain was not joined for any realm that did not create a computer account.

### Authentication

<table>
<thead>
<tr>
<th>Authentication Realm</th>
<th>Protocol</th>
<th>Schema(s)</th>
<th>Servers</th>
<th>Base DN or NetBIOS Domain</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTLM</td>
<td>NTLM</td>
<td>NTLMSSP or Basic</td>
<td>example.com</td>
<td>Domain not joined</td>
<td>![ ]</td>
</tr>
</tbody>
</table>

Red text indicates that the domain was not joined and no computer account was created.

AsyncOS only creates an Active Directory computer account when you edit the authentication realm Active Directory information or when the appliance reboots.

**Note**

To successfully join the Active Directory domain, the time difference between the Web Security appliance and the Active Directory server should be less than the time specified in the “Maximum tolerance for computer clock synchronization” option on the Active Directory server. When you use Network Time Protocol (NTP) to specify the current time on the Web Security appliance, remember that the default time server is time.ironport.com. This may affect the time difference between the appliance and the Active Directory server.

Some Active Directory environments automatically delete computer objects at particular intervals for accounts that appear in active in order to clean up old computer objects. However, AsyncOS does not automatically change the password for the computer account it creates in an Active Directory server, so the computer account may appear inactive over time. Therefore, if the Active Directory environment automatically deletes computer objects at particular intervals, make sure the Web Security appliance computer account is created in a container that is exempt from this cleanup process.
Supported Authentication Characters

This section lists the characters the Web Security appliance supports when it communicates with LDAP and Active Directory servers. For authentication to work properly, verify that your authentication servers only use the supported characters listed in this section.

For example, according to Table 20-16, the appliance can validate users with the following Active Directory user name:

`jsmith#123`

And according to Table 20-16, the appliance cannot validate users with the following Active Directory user name:

`jsmith+`

Active Directory Server Supported Characters

Table 20-16 lists the characters the Web Security appliance supports for the User Name field for Active Directory servers.

<table>
<thead>
<tr>
<th>Supported Characters</th>
<th>Characters Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>A...Z a...z</td>
<td>/ \ [ ] ; ;</td>
</tr>
<tr>
<td>0 1 2 3 4 5 6 7 8 9</td>
<td></td>
</tr>
<tr>
<td>` ~ ! # $ % ^ &amp; ( ) _ - { } ' . @ space</td>
<td></td>
</tr>
</tbody>
</table>

Note

The Web Security appliance supports the percent (%) character for end users browsing the web. However, you cannot use a user name with the percent (%) character to join the Active Directory domain when you create an NTLM authentication realm.
Table 20-17 lists the characters the Web Security appliance supports for the Password field for Active Directory servers.

### Table 20-17 Supported Active Directory Server Characters — Password Field

<table>
<thead>
<tr>
<th>Supported Characters</th>
<th>Characters Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>A...Z a...z</td>
<td>N/A</td>
</tr>
<tr>
<td>0 1 2 3 4 5 6 7 8 9</td>
<td></td>
</tr>
<tr>
<td>` ~ ! # $ ^ &amp; ( ) _ - { } ' . / [ ] :</td>
<td>* ? @ + \ , ; &quot; = &lt; &gt; space</td>
</tr>
</tbody>
</table>

Table 20-18 lists the characters the Web Security appliance supports for the Location field for Active Directory servers. You enter the location string in the Location field when you configure an NTLM authentication realm.

### Table 20-18 Supported Active Directory Server Characters — Location Field

<table>
<thead>
<tr>
<th>Supported Characters</th>
<th>Characters Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>A...Z a...z</td>
<td>+ \ , ; &quot; = &lt; &gt;</td>
</tr>
<tr>
<td>0 1 2 3 4 5 6 7 8 9</td>
<td></td>
</tr>
<tr>
<td>` ~ ! # $ ^ &amp; ( ) _ - { } ' . / [ ] :</td>
<td>* ? @ space</td>
</tr>
</tbody>
</table>

**Note:** The appliance does not support these characters even when they are escaped with a backslash (\) character.

Table 20-19 lists the characters the Web Security appliance supports for the Group field for Active Directory servers.

### Table 20-19 Supported Active Directory Server Characters — Group Field

<table>
<thead>
<tr>
<th>Supported Characters</th>
<th>Characters Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>A...Z a...z</td>
<td>/ \ { } ;</td>
</tr>
<tr>
<td>0 1 2 3 4 5 6 7 8 9</td>
<td>space</td>
</tr>
</tbody>
</table>

` ~ ! # $ % ^ & ( ) _ - { } ' . / [ ] : | * ? @ space`
Note: You can only use the backslash (\) character as a separator between the domain name and a user or group name, or as a separator between organizational units (OU) in the location string for an Active Directory server. You cannot use it as part of a domain name, user name, group name, or location name.

### LDAP Server Supported Characters

Table 20-20 lists the characters the Web Security appliance supports for the User Name field for LDAP servers.

**Table 20-20  Supported LDAP Server Characters — User Name Field**

<table>
<thead>
<tr>
<th>Supported Characters</th>
<th>Characters Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>A...Z a...z</td>
<td>/ \ { } : ;</td>
</tr>
<tr>
<td>0 1 2 3 4 5 6 7 8 9</td>
<td></td>
</tr>
<tr>
<td>` ~ ! # $ % ^ &amp; ( ) - ( ) ' . @</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The appliance only supports the ‘(’ and ‘)’ characters when they are escaped with a backslash (\) character.

Table 20-21 lists the characters the Web Security appliance supports for the Password field for LDAP servers.

**Table 20-21  Supported LDAP Server Characters — Password Field**

<table>
<thead>
<tr>
<th>Supported Characters</th>
<th>Characters Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>A...Z a...z</td>
<td>N/A</td>
</tr>
<tr>
<td>0 1 2 3 4 5 6 7 8 9</td>
<td></td>
</tr>
<tr>
<td>` ~ ! # $ % ^ &amp; ( ) - ( ) @</td>
<td></td>
</tr>
<tr>
<td>' , / \ [ ] : ;</td>
<td>= * ? &lt; &gt; * , ; +</td>
</tr>
<tr>
<td>space</td>
<td></td>
</tr>
</tbody>
</table>
Table 20-22 lists the characters the Web Security appliance supports for the Group field for LDAP servers.

Table 20-22       Supported LDAP Server Characters — Group Field

<table>
<thead>
<tr>
<th>Supported Characters</th>
<th>Characters Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>A...Z a...z</td>
<td>, ; +</td>
</tr>
<tr>
<td>0 1 2 3 4 5 6 7 8 9</td>
<td></td>
</tr>
<tr>
<td>` ~ ! $ % ^ &amp; ( ) _ - { } @ ' . / [ ]</td>
<td></td>
</tr>
<tr>
<td>:</td>
<td>= * ? &lt; &gt; &quot;</td>
</tr>
<tr>
<td>space</td>
<td></td>
</tr>
</tbody>
</table>

Note: The appliance only supports the ‘(’ and ‘)’ characters when they are escaped with a backslash (\) character.

Table 20-23 lists the characters the Web Security appliance supports for the Custom User Filter Query Field field for LDAP servers.

Table 20-23       Supported LDAP Server Characters — Custom User Filter Query Field

<table>
<thead>
<tr>
<th>Supported Characters</th>
<th>Characters Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>A...Z a...z</td>
<td></td>
</tr>
<tr>
<td>0 1 2 3 4 5 6 7 8 9</td>
<td></td>
</tr>
</tbody>
</table>
| ` ~ ! $ % ^ & ( ) _ - { } @ ' . / \
[ ] : | = * ? < > "          |
| space                 |                          |

Table 20-24 lists the characters the Web Security appliance supports for the Custom Group Filter Query Field field for LDAP servers.

Table 20-24       Supported LDAP Server Characters — Custom Group Filter Query Field

<table>
<thead>
<tr>
<th>Supported Characters</th>
<th>Characters Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>A...Z a...z</td>
<td></td>
</tr>
<tr>
<td>0 1 2 3 4 5 6 7 8 9</td>
<td></td>
</tr>
<tr>
<td>` ~ ! $ % ^ &amp; ( ) _ - { } @ ' . / [ ] :</td>
<td>= * ? &lt; &gt; &quot;</td>
</tr>
<tr>
<td>space</td>
<td></td>
</tr>
</tbody>
</table>
L4 Traffic Monitor

This chapter contains the following information:

- About L4 Traffic Monitor, page 21-1
- How the L4 Traffic Monitor Works, page 21-1
- Configuring the L4 Traffic Monitor, page 21-3
- Viewing L4 Traffic Monitor Activity, page 21-9

About L4 Traffic Monitor

The Web Security appliance has an integrated Layer-4 Traffic Monitor that detects rogue traffic across all network ports and stops malware attempts to bypass port 80. Additionally, when internal clients are infected with malware and attempt to phone-home across non-standard ports and protocols, the L4 Traffic Monitor prevents phone-home activity from going outside the corporate network.

How the L4 Traffic Monitor Works

The L4 Traffic Monitor listens to network traffic that comes in over all ports on the appliance and matches domain names, and IP addresses against entries in its own database tables to determine whether to allow incoming and outgoing traffic. All web destinations fall under one of the following categories:
How the L4 Traffic Monitor Works

- **Known allowed address.** Any IP address or hostname listed in the Allow List property. These addresses appear in the log files as “whitelist” addresses.

- **Unlisted address.** Any IP address that is not known to be a malware site nor is a known allowed address. They are not listed on the Allow List or Additional Suspected Malware Addresses properties, nor are they listed in the L4 Traffic Monitor Database as a known malware site. These addresses do not appear in the log files.

- **Ambiguous address.** These addresses appear in the log files as “greylist” addresses. They include any of the following addresses:
  - Any IP address that is associated with both an unlisted hostname and a known malware hostname.
  - Any IP address that is associated with both an unlisted hostname and a hostname from the Additional Suspected Malware Addresses property.

- **Known malware address.** These addresses appear in the log files as “blacklist” addresses. They include any of the following addresses:
  - Any IP address or hostname that the L4 Traffic Monitor Database determines to be a known malware site and not listed in the Allow List.
  - Any IP address that is listed in the Additional Suspected Malware Addresses property and not listed in the Allow List and not determined to be ambiguous.

---

**Note**

You can define the Allow List and the Additional Suspected Malware Addresses properties on the Web Security Manager > L4 Traffic Monitor Policies page.

The L4 Traffic Monitor listens to and monitors network ports for rogue activity. It performs one of the following actions on all traffic on your network:

- **Allow.** It always allows traffic to and from known allowed and unlisted addresses.

- **Monitor.** It monitors traffic under the following circumstances:
  - When the Action for Suspected Malware Addresses option is set to Monitor, it always monitors all traffic that is not to or from a known allowed address.
  - When the Action for Suspected Malware Addresses option is set to Block, it monitors traffic to and from ambiguous addresses.
• **Block.** When the Action for Suspected Malware Addresses option is set to Block, it blocks traffic to and from known malware addresses.

### The L4 Traffic Monitor Database

The L4 Traffic Monitor uses and maintains its own internal database. This database is continuously updated with matched results for IP addresses and domain names. Additionally, the database table receives periodic updates from the IronPort update server at the following location:

https://update-manifests.ironport.com

For information about update intervals and the IronPort update server, see Manually Updating Security Service Components, page 26-51.

### Configuring the L4 Traffic Monitor

The L4 Traffic Monitor can be enabled as part of an initial system setup using the System Setup Wizard. By default, the L4 Traffic Monitor is enabled and set to monitor traffic on all ports. This includes DNS and other services.

#### Note

To monitor true client IP addresses, the L4 Traffic Monitor should always be configured inside the firewall and before network address translation (NAT). For more information about deploying the L4 Traffic Monitor, see Deploying the L4 Traffic Monitor, page 3-16.

You can configure the following settings:

- **Global L4 Traffic Monitor settings.** You can enable or disable the L4 Traffic Monitor after an initial configuration and configure which TCP ports to monitor. Use the Security Services > L4 Traffic Monitor page. For more information see Configuring L4 Traffic Monitor Global Settings, page 21-4.

- **L4 Traffic Monitor policies.** When the L4 Traffic Monitor is enabled, you configure specific policies for managing traffic. Use the Web Security Manager > L4 Traffic Monitor Policies page. For more information see Configuring L4 Traffic Monitor Policies, page 21-5.
Configuring L4 Traffic Monitor Global Settings

On the Security Services > L4 Traffic Monitor page, you can configure the L4 Traffic Monitor global settings and update the L4 Traffic Monitor anti-malware rules.

**Figure 21-1 Security Services > L4 Traffic Monitor Page**

<table>
<thead>
<tr>
<th>L4 Traffic Monitor Global Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>L4 Traffic Monitor Status: Enabled</td>
</tr>
<tr>
<td>Traffic Monitored On: All Ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IronPort L4 Anti-Malware Rules Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Update</td>
</tr>
<tr>
<td>Current Version</td>
</tr>
</tbody>
</table>

To configure L4 Traffic Monitor global settings:

**Step 1** Navigate to the Security Services > L4 Traffic Monitor page.

**Step 2** Click Edit Global Settings.

**Step 3** Choose whether or not to enable the L4 Traffic Monitor.

**Step 4** When you enable the L4 Traffic Monitor, choose which ports it should monitor:

- **All ports.** Monitors all 65535 TCP ports for rogue activity.
- **All ports except proxy ports.** Monitors all TCP ports except the following ports for rogue activity:
  - Ports configured in the “HTTP Ports to Proxy” property on the Security Services > Web Proxy page (usually port 80).
  - Ports configured in the “Transparent HTTPS Ports to Proxy” property on the Security Services > HTTPS Proxy page (usually port 443).

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

**Updating L4 Traffic Monitor Anti-Malware Rules**

To update the L4 Traffic Monitor anti-malware rules:
Step 1
Navigate to the Security Services > L4 Traffic Monitor page.

Step 2
Click Update Now.

The Web Security appliance contacts the component update server and updates the L4 Traffic Monitor anti-malware rules. For more information about the component update server, see Manually Updating Security Service Components, page 26-51.

Configuring L4 Traffic Monitor Policies

When the L4 Traffic Monitor is enabled, you can configure how it should manage traffic over the configured TCP ports. It can perform the following actions on traffic over the TCP ports:

- Allow
- Monitor
- Block

For more information about how the L4 Traffic Monitor handles traffic, see How the L4 Traffic Monitor Works, page 21-1.

The actions the L4 Traffic Monitor takes depends on the L4 Traffic Monitor policies you configure.

To configure L4 Traffic Monitor policies:

Step 1
Navigate to the Web Security Manager > L4 Traffic Monitor page.

Step 2
Click Edit Settings.

Step 3
On the Edit L4 Traffic Monitor Policies page, configure the L4 Traffic Monitor policies described in Table 21-1.
Table 21-1  L4 Traffic Monitor Policies

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow List</td>
<td>Enter zero or more address to which the L4 Traffic Monitor should always allow clients to connect. Separate multiple entries with a space or comma. For a list of valid address formats you can use, see Valid Formats, page 21-8.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Entering a domain name such as example.com also matches <a href="http://www.example.com">www.example.com</a> and hostname.example.com. Connections to all destinations in this list are always allowed and the traffic is not logged. The appliance does not check the destinations against the L4 Traffic Monitor anti-malware rules or the additional suspected malware addresses listed on the same page.</td>
</tr>
<tr>
<td></td>
<td>For example, if IP address 10.1.1.1 appears in both the Allow List and the Additional Suspected Malware Addresses fields, then the L4 Traffic Monitor always allows requests for 10.1.1.1.</td>
</tr>
</tbody>
</table>
Actions for Suspected Malware Addresses

Choose whether to monitor or block traffic destined for a known malware address. For a definition of known malware address, see How the L4 Traffic Monitor Works, page 21-1.

- **Monitor.** Scans all traffic for domains and IP addresses that match entries in the L4 Traffic Monitor database. The Monitor option does not block suspicious traffic. This setting is useful for identifying infected clients without affecting the user experience.

- **Block.** Scans all traffic for domains and IP addresses that match entries in the appliance administrative lists and the block list database and then blocks any traffic it finds. This setting is useful for identifying infected clients and stopping malware attempts through non-standard ports.

When you choose to block suspected malware traffic, you can also choose whether or not to always block ambiguous addresses. By default, ambiguous addresses are monitored.

For a definition of ambiguous address, see How the L4 Traffic Monitor Works, page 21-1.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions for Suspected Malware Addresses</td>
<td>Choose whether to monitor or block traffic destined for a known malware address. For a definition of known malware address, see How the L4 Traffic Monitor Works, page 21-1.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Monitor.</strong> Scans all traffic for domains and IP addresses that match entries in the L4 Traffic Monitor database. The Monitor option does not block suspicious traffic. This setting is useful for identifying infected clients without affecting the user experience.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Block.</strong> Scans all traffic for domains and IP addresses that match entries in the appliance administrative lists and the block list database and then blocks any traffic it finds. This setting is useful for identifying infected clients and stopping malware attempts through non-standard ports.</td>
</tr>
</tbody>
</table>

When you choose to block suspected malware traffic, you can also choose whether or not to always block ambiguous addresses. By default, ambiguous addresses are monitored.

For a definition of ambiguous address, see How the L4 Traffic Monitor Works, page 21-1.
Configuring the L4 Traffic Monitor

Note

If the L4 Traffic Monitor is configured to block, the L4 Traffic Monitor and the Web Proxy must be configured on the same network. Use the Network > Routes page to confirm that all clients are accessible on routes that are configured for data traffic.

Step 4

Submit and commit your changes.

Valid Formats

When you add addresses to the Allow List or Additional Suspected Malware Addresses properties, separate multiple entries with whitespace or commas. You can enter addresses in any of the following formats:

**Table 21-1  L4 Traffic Monitor Policies**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Additional Suspected Malware Addresses (optional) | Enter zero or more known addresses that the L4 Traffic Monitor should consider as a possible malware. For a list of valid address formats you can use, see Valid Formats, page 21-8. If you choose to block suspected malware addresses, the L4 Traffic Monitor will either block or monitor these addresses depending on whether it determines them to be known malware addresses or ambiguous addresses. For definitions of ambiguous and known malware addresses, see How the L4 Traffic Monitor Works, page 21-1. If you choose to monitor suspected malware addresses, it will monitor these addresses. 

**Note:** Adding internal IP addresses to the Additional Suspected Malware Addresses list causes legitimate destination URLs to show up as malware in L4 Traffic Monitor reports. To avoid this type of erroneous reporting, do not enter internal IP addresses in the “Additional Suspected Malware Addresses” field on the Web Security Manager > L4 Traffic Monitor Policies page. |
**Viewing L4 Traffic Monitor Activity**

The S-Series appliance supports several options for generating feature specific reports and interactive displays of summary statistics.

**Monitoring Activity and Viewing Summary Statistics**

The Reporting > L4 Traffic Monitor page provides statistical summaries of monitoring activity. You can interactively update these displays by specifying a time range of hour, day, week or month. Additionally, you have the option to print these display pages and export the raw data to a file.

You can use the following displays and reporting tools to view the results of L4 Traffic Monitor activity:

<table>
<thead>
<tr>
<th>Table 21-2</th>
<th>L4 Traffic Monitor Scanning Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>To view...</td>
<td>See...</td>
</tr>
<tr>
<td>Client statistics</td>
<td>Reporting &gt; Client Activity</td>
</tr>
<tr>
<td>Malware statistics</td>
<td>Reporting &gt; L4 Traffic Monitor</td>
</tr>
<tr>
<td>Port statistics</td>
<td></td>
</tr>
<tr>
<td>L4 Traffic Monitor log files</td>
<td>System Administration &gt; Log Subscriptions</td>
</tr>
<tr>
<td></td>
<td>• trafmon_errlogs</td>
</tr>
<tr>
<td></td>
<td>• trafmonlogs</td>
</tr>
</tbody>
</table>
Note

If the Web Proxy is configured as a forward proxy and L4 Traffic Monitor is set to monitor all ports, the IP address of the proxy’s data port is recorded and displayed as a client IP address in the client activity report on the Reporting > Client Activity page. If the Web Proxy is configured as a transparent proxy, enable IP spoofing to correctly record and display the client IP addresses.

L4 Traffic Monitor Log File Entries

The L4 Traffic Monitor log file provides a detailed record of monitoring activity. For more information about the L4 Traffic Monitor log, see Traffic Monitor Log, page 24-53.
CHAPTER 22

Reporting

This chapter contains the following information:

- Reporting Overview, page 22-1
- Using the Reporting Tab, page 22-3
- Enabling Centralized Reporting, page 22-12
- Scheduling Reports, page 22-13
- On-Demand Reports, page 22-15
- Archiving Reports, page 22-16
- SNMP Monitoring, page 22-16

Reporting Overview

Reporting functionality aggregates information from individual security features and records data that can be used to monitor your web traffic patterns and security risks. You can run reports in real-time to view an interactive display of system activity over a specific period of time, or you can schedule reports and run them at regular intervals.

The Web Security appliance not only generates high-level reports, allowing you to understand what is happening on the network, but it also allows you to drill down and see traffic details for a particular domain, user, or category.

Reporting functionality also allows you to export raw data to a file. For more information see, Printing and Exporting Reports from Report Pages, page 22-10.
Working with Usernames in Reports

When you enable authentication, reports list users by their usernames when they authenticate with the Web Proxy. By default, usernames are written as they appear in the authentication server, such as jsmith. However, you can choose to make usernames unrecognizable in all reports.

Note

Administrators always see usernames in reports.

To make usernames unrecognizable in reports:

Step 1 Navigate to the Security Services > Reporting page, and click Edit Settings.

Step 2 Under Local Reporting, select Anonymize usernames in reports.

Step 3 Submit and commit your changes.

Report Pages

The Web Security appliance offers the following reports:

- Overview
- Users
- Web Sites
- URL Categories
- Application Visibility
- Anti-Malware
- Client Malware Risk
- Web Reputation Filters
• L4 Traffic Monitor
• Reports by User Location
• Web Tracking
• System Capacity
• System Status

For detailed descriptions of each of these reports, see Web Security Appliance Reports, page 23-1.

Using the Reporting Tab

The Reporting tab provides several options for viewing system data. This section describes those options and explains the information displayed on each report page.

The report pages provide a colorful overview of system activity and support multiple options for viewing system data. For example, you can update and sort data to provide real-time visibility into resource utilization and web traffic activity. You can also search each page for website and client-specific data.

You can perform the following tasks on most reports on the Reporting tab:

• Change the time range displayed in a report. For more information, see Changing the Time Range, page 22-3.
• Search for specific clients and domains. For more information, see Searching Data, page 22-5.
• Choose and sort columns. For more information, see Working with Columns on Report Pages, page 22-5.
• Export reports to external files. For more information, see Printing and Exporting Reports from Report Pages, page 22-10.

Changing the Time Range

You can update the data displayed for each security component using the Time Range field. This option allows you to generate updates for predefined time ranges, such as the last hour or week, and it allows you to define custom time ranges from a specific start time to a specific end time.
The time range you select is used throughout all of the report pages until you select a different value in the Time Range menu.

Figure 22-1 shows the Time Range field for the URL Categories report.

Figure 22-1 Selecting Data Time Range

You can choose any of the time ranges described in Table 22-1.

Table 22-1 Configurable Time Ranges

<table>
<thead>
<tr>
<th>Time Range</th>
<th>Data is returned in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hour</td>
<td>Sixty (60) complete minutes plus up to 5 additional minutes.</td>
</tr>
<tr>
<td>Day</td>
<td>One hour intervals for the last 24 hours and including the current partial hour.</td>
</tr>
<tr>
<td>Week</td>
<td>One day intervals for the last 7 days plus the current partial day.</td>
</tr>
<tr>
<td>Month (30 days)</td>
<td>One day intervals for the last 30 days plus the current partial day.</td>
</tr>
<tr>
<td>Yesterday</td>
<td>The last 24 hours (00:00 to 23:59) using the Web Security appliance defined time zone.</td>
</tr>
<tr>
<td>Custom Range</td>
<td>The custom time range defined by the user.</td>
</tr>
<tr>
<td></td>
<td>When you choose Custom Range, a dialog box appears where you can enter the start and end times.</td>
</tr>
</tbody>
</table>

Note

All reports display date and time information based on the systems configured time zone, shown as a Greenwich Mean Time (GMT) offset. However, data exports display the time in GMT to accommodate multiple systems in multiple time zones around the world.
Searching Data

Some reports include a field that allow you to search for a particular data points. For example, on the URL Categories report, you can search for a particular URL category, and on the Users report, you can search for a particular user by user name or IP address. When you search for data, the report refines the report data for the particular data set you are searching.

You can search for values that exactly match of the string you enter, or for values that start with the string you enter.

The following report pages include search fields:

- **Users.** Search for a user by user name or client IP address.
- **Web Sites.** Search for a server by domain or server IP address.
- **URL Categories.** Search for a URL category.
- **Application Visibility.** Search for an application name that the AVC engine monitors and blocks.
- **Client Malware Risk.** Search for a user by user name or client IP address.

Note: You need to configure authentication to view client user IDs as well as client IP addresses.

Figure 22-2 shows the search field for the URL Categories report.

![Figure 22-2 Searching for URL Categories](image)

Working with Columns on Report Pages

Each page has interactive column headings that can be configured to sort the data in each column specific to your needs for viewing data on that page.

Note: Not every column is available for every report page. Click the Columns link for each report page to view the available columns.
Table 22-2 describes the columns available when working with reports.

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain or Realm</td>
<td>The domain or realm of the user displayed in text format.</td>
</tr>
<tr>
<td>User ID or Client IP</td>
<td>The username or client IP address of the user displayed in text format.</td>
</tr>
<tr>
<td>Bandwidth Used</td>
<td>The amount of bandwidth that is used by a particular user or action. Bandwidth units are displayed in Bytes or percentage.</td>
</tr>
<tr>
<td>Bandwidth Saved by Blocking</td>
<td>The amount of bandwidth that has been saved due to blocking certain transactions. Bandwidth units are displayed in Bytes.</td>
</tr>
</tbody>
</table>
Using the Reporting Tab

Chapter 22      Reporting

Table 22-2    Report Column Descriptions (continued)

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Spent</td>
<td>The amount of time spent on a web page. For purposes of investigating a user, the time spent by the user on each URL category. When tracking a URL, the time spent by each user on that specific URL. To calculate the time spent, AsyncOS assigns each active user with 60 seconds of time for activity during a minute. At the end of the minute, the time spent by each user is evenly distributed among the different domains the user visited. For example, if a user goes to four different domains in an active minute, the user is considered to have spent 15 seconds at each domain. For the purposes of the time spent value, considering the following notes:</td>
</tr>
<tr>
<td></td>
<td>- An active user is defined as a username or IP address that sends HTTP traffic through the appliance and has gone to a website that AsyncOS considers to be a “page view.”</td>
</tr>
<tr>
<td></td>
<td>- AsyncOS defines a page view as an HTTP request initiated by the user, as opposed to a request initiated by the client application. AsyncOS uses a heuristic algorithm to make a best effort guess to identify user page views. Units displayed in HH:MM format.</td>
</tr>
<tr>
<td>Allowed URL Category</td>
<td>The number and type of categories that have been allowed. Units displayed in transaction type.</td>
</tr>
<tr>
<td>Monitored URL Category</td>
<td>The number and type of categories that are being monitored. Units displayed in transaction type.</td>
</tr>
<tr>
<td>Warned URL Category</td>
<td>The number and type of categories that have initiated a warning. Units displayed in transaction type.</td>
</tr>
<tr>
<td>Blocked by URL Category</td>
<td>The transaction that has been blocked due to URL Category. Units displayed in transaction type.</td>
</tr>
</tbody>
</table>
To configure the columns that appear in a report, perform the following steps:

### Step 1
On the Security Management appliance page, choose Reporting > *Report_Name*.

### Step 2
Click the **Columns** link that appears in the lower right corner of a report.

For example, *Figure 22-3* shows the Columns link for the URL Categories report.

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked by Application or Application Type</td>
<td>The application that has been blocked due to application type. Units displayed in transaction type.</td>
</tr>
<tr>
<td>Blocked by Web Reputation</td>
<td>The transaction that has been blocked due to web reputation. Units displayed in transaction type.</td>
</tr>
<tr>
<td>Blocked by Anti-Malware</td>
<td>The transactions blocked by Anti-Malware. Units displayed in transaction type.</td>
</tr>
<tr>
<td>Other Blocked Transactions</td>
<td>All other transactions that have been blocked. Units displayed in transaction type.</td>
</tr>
<tr>
<td>Transactions with Bandwidth Limit</td>
<td>The number of transactions that have a bandwidth limit.</td>
</tr>
<tr>
<td>Transactions without Bandwidth Limit</td>
<td>The number of transactions that do not have a bandwidth limit.</td>
</tr>
<tr>
<td>Transactions Blocked by Application</td>
<td>The number of transactions blocked by a specific application type.</td>
</tr>
<tr>
<td>Warned Transactions</td>
<td>All transactions that rendered a warning to the user. Units displayed in transaction type.</td>
</tr>
<tr>
<td>Transactions Completed</td>
<td>The transactions completed by a user. Units displayed in transaction type.</td>
</tr>
<tr>
<td>Transactions Blocked</td>
<td>All transactions that have been blocked. Units displayed in transaction type.</td>
</tr>
<tr>
<td>Total Transactions</td>
<td>The total number of transactions that have occurred.</td>
</tr>
</tbody>
</table>
A pop-up window appears that allows you to select the columns you want to appear in the report. For example, Figure 22-4 shows the columns you can select for the URL Categories report.

**Step 3** Select each column to display by clicking the checkbox next to each column in the pop-up window, and click **Done**.
Printing and Exporting Reports from Report Pages

You can generate a printer-friendly formatted PDF version of any of the report pages by clicking the **Printable (PDF)** link at the top-right corner of the page.

Additionally, you can export graphs and other data to comma-separated values (CSV) format by clicking the **Export** link. Most reports allow scheduling of CSV formatting. However, you cannot schedule an extended report with a CSV format.

**Note**

You can only print to PDF and export data from the Web Tracking page after the Web Tracking page returns search results. Do this using the **Printable Download** link. From this link you can choose to create a PDF that includes data displayed on the current page or up to 1,000 transactions, or you can export all data to a CSV file.

Exporting Report Data

Most reports include an **Export** link that allows you to export raw data to a comma-separated values (CSV) file. After exporting the data to a CSV file, you can access and manipulate the data in it using applications such as Microsoft Excel.

The exported CSV data displays all message tracking and reporting data in Greenwich Mean Time (GMT) regardless of what is set on the Web Security appliance. The purpose of the GMT time conversion is to allow data to be used independently from the appliance or when referencing data from appliances in multiple time zones.

The following example is an entry from a raw data export of the Anti-Malware category report, where Pacific Daylight Time (PDT) is displayed as GMT - 7 hours:

Begin Timestamp, End Timestamp, Begin Date, End Date, Name, Transactions Monitored, Transactions Blocked, Transactions Detected
Chapter 22      Reporting

Using the Reporting Tab

1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525, 2100, 2625

Table 22-3     Viewing Raw Data Entries

<table>
<thead>
<tr>
<th>Category Header</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begin Timestamp</td>
<td>1159772400.0</td>
<td>Query start time in number of seconds from epoch.</td>
</tr>
<tr>
<td>End Timestamp</td>
<td>1159858799.0</td>
<td>Query end time in number of seconds from epoch.</td>
</tr>
<tr>
<td>Begin Date</td>
<td>2006-10-02 07:00 GMT</td>
<td>Date the query began.</td>
</tr>
<tr>
<td>End Date</td>
<td>2006-10-03 06:59 GMT</td>
<td>Date the query ended.</td>
</tr>
<tr>
<td>Name</td>
<td>Adware</td>
<td>Name of the malware category.</td>
</tr>
<tr>
<td>Transactions</td>
<td>Monitored</td>
<td>Number of transactions monitored.</td>
</tr>
<tr>
<td></td>
<td>525</td>
<td></td>
</tr>
<tr>
<td>Transactions</td>
<td>Blocked</td>
<td>Number of transactions blocked.</td>
</tr>
<tr>
<td></td>
<td>2100</td>
<td></td>
</tr>
<tr>
<td>Transactions</td>
<td>Detected</td>
<td>Total number of transactions: Number of transactions detected + Number of transactions blocked.</td>
</tr>
<tr>
<td></td>
<td>2625</td>
<td></td>
</tr>
</tbody>
</table>

Note
Category headers are different for each type of report.

Note
If you export localized CSV data, the headings may not be rendered properly in some browsers. This occurs because some browsers may not use the proper character set for the localized text. To work around this problem, you can save the file to your local machine, and open the file in any web browser using File > Open. When you open the file, select the character set to display the localized text.
Enabling Centralized Reporting

When the Web Security appliance is managed by a Security Management appliance, you can choose which appliance displays reports on the web traffic that is processed by the Web Security appliance. By default, the Web Security appliance maintains the reports (Local Reporting). However, you can configure the Web Security appliance so that the Security Management appliance maintains the reports by enabling Centralized Reporting. You might want to enable Centralized Reporting when the Security Management appliance manages multiple Web Security appliances. This gives you a centralized view of web traffic across all Web Security appliances.

Note

When you enable Centralized Reporting, only the System Capacity and System Status reports are available on the Web Security appliance. To view the other reports, connect to the Security Management appliance. The Web Security appliance no longer stores data for the other reports.

To enable Centralized Reporting:

Step 1
Navigate to the Security Services > Reporting page, and click Edit Settings.

Step 2
Choose Centralized Reporting.

Step 3
Submit and commit your changes.
Scheduling Reports

You can schedule reports to run on a daily, weekly, or monthly basis. Scheduled reports can be configured to include data for the previous day, previous seven days, or previous month. Alternatively, you can include data for a custom number of days (from 2 days to 100 days) or a custom number of months (from 2 months to 12 months).

Regardless of when you run a report, the data is returned from the previous time interval (hour, day, week, or month). For example, if you schedule a daily report to run at 1AM, the report will contain data from the previous day, midnight to midnight (00:00 to 23:59).

You can schedule reports for the following types of reports:
- Overview
- Users
- Web Sites
- URL Categories
- Application Visibility
- Anti-Malware
- Client Malware Risk
- Web Reputation Filters
- L4 Traffic Monitor
- Reports by User Location
- System Capacity

For more information on the data displayed in each report, see Web Security Appliance Reports, page 23-1.

Adding a Scheduled Report

Use the Reporting > Scheduled Reports page to schedule reporting for different reports.

To create a scheduled report:
Step 1
Navigate to the Reporting > Scheduled Reports page, and click Add Scheduled Report.

**Figure 22-5 Adding a Scheduled Report**
Add Scheduled Report

<table>
<thead>
<tr>
<th>Report Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type:</td>
</tr>
<tr>
<td>Title:</td>
</tr>
<tr>
<td>Time Range To Include:</td>
</tr>
<tr>
<td>Format:</td>
</tr>
<tr>
<td>Schedule:</td>
</tr>
<tr>
<td>At time:</td>
</tr>
<tr>
<td>Email to:</td>
</tr>
</tbody>
</table>

Step 2
Select a report type.

Step 3
Enter a title for the report. To avoid creating multiple reports with the same name, consider using a descriptive title.

Step 4
Select a time range for the data included in the report.

Step 5
Choose the format for the generated report.

The default format is PDF. Most reports allow scheduling of CSV.

Step 6
Depending on the type of report you configure, you can specify different report options, such as the number of rows to include and by which column to sort the data. Configure these options as necessary.

Step 7
In the Schedule section, choose whether to run the report daily, weekly, or monthly and at what time.

Step 8
In the Email field, enter the email address to where to send the generated report.

If you do not specify an email address, the report is archived only.

Step 9
Submit and commit your changes.
Chapter 22 Reporting

Editing Scheduled Reports

To edit reports, select the report title from the list on the Reporting > Scheduled Reports page, modify settings then submit and commit your changes.

Deleting Scheduled Reports

To delete reports, go to the Reporting > Scheduled Reports page and select the check boxes corresponding to the reports that you want to delete. To remove all scheduled reports, select the All check box, Delete and Commit your changes. Note that archived versions of deleted reports are not deleted.

On-Demand Reports

The Generate Report Now option on the Reporting > Archived Reports page allows you to generate on-demand data displays for each report type. To generate a report:

**Step 1** Select Generate Report Now

**Figure 22-6 Generating an On-Demand Report**

<table>
<thead>
<tr>
<th>Generate Report</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Type</td>
<td>Select report type...</td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Time Range To Include</td>
<td>Previous 7 calendar days</td>
</tr>
<tr>
<td>Format</td>
<td>POF</td>
</tr>
<tr>
<td>CVF</td>
<td></td>
</tr>
<tr>
<td>Delivery Options</td>
<td>Archive</td>
</tr>
<tr>
<td>Email now to recipients</td>
<td></td>
</tr>
<tr>
<td>Separate multiple addresses with commas</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2** Select a report type and edit the title, if necessary. To avoid creating multiple reports with the same name, consider using a descriptive title.

**Step 3** Select a time range for the data included in the report.
Step 4  Choose the format for the generated report.  
   The default format is PDF. Most reports allow scheduling of CSV.

Step 5  Depending on the type of report you configure, you can specify different report  
   options, such as the number of rows to include and by which column to sort the  
   data. Configure these options as necessary.

Step 6  Select whether to archive the report (if so, the report will appear on the Archived  
   Reports page).

Step 7  Specify whether to email the report, and list the email addresses of the recipients.

Step 8  Click **Deliver this Report** to generate the report.

Step 9  Commit your changes.

### Archiving Reports

The Reporting > Archived Reports page lists available archived reports. Report  
   names in the Report Title column are interactive and link to a view of each report.  
   The Show menu filters the types of reports that are listed. Additionally, interactive  
   column headings can be used to sort the data in each column.

The appliance stores up to 12 instances of each scheduled report (up to 1000  
   reports). Archived reports are stored in the `/periodic_reports` directory on the  
   appliance. Archived reports are deleted automatically. As new reports are added,  
   older reports are removed to keep the number at 1000. The limit of 12 instances  
   applies to each scheduled report with the same name and time range.

### SNMP Monitoring

The IronPort AsyncOS operating system supports system status monitoring via  
   SNMP (Simple Network Management Protocol). This includes IronPort’s  
   Enterprise MIB, `asyncoswebsecurityappliance-mib.txt`. The  
   `asyncoswebsecurityappliance-mib` helps administrators better monitor system  
   health. In addition, this release implements a read-only subset of MIB-II as  
   defined in RFCs 1213 and 1907. (For more information about SNMP, see RFCs  
   1065, 1066, and 1067.) Please note:

- SNMP is **off** by default.
SNMP Monitoring

- SNMP SET operations (configuration) are not implemented.
- AsyncOS supports SNMPv1, v2, and v3.
- The use of SNMPv3 with password authentication and DES Encryption is mandatory to enable this service. (For more information on SNMPv3, see RFCs 2571-2575.) You are required to set a SNMPv3 passphrase of at least 8 characters to enable SNMP system status monitoring. The first time you enter a SNMPv3 passphrase, you must re-enter it to confirm. The `snmpconfig` command “remembers” this phrase the next time you run the command.
- The SNMPv3 username is: v3get.

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 ironport
serv.example.com
```

- If you use only SNMPv1 or SNMPv2, you must set a community string. The community string does not default to `public`.
- For SNMPv1 and SNMPv2, you must specify a network from which SNMP GET requests are accepted.
- To use traps, an SNMP manager (not included in AsyncOS) must be running and its IP address entered as the trap target. (You can use a hostname, but if you do, traps will only work if DNS is working.)

Use the `snmpconfig` command to configure SNMP system status for the appliance. After you choose and configure values for an interface, the appliance responds to SNMPv3 GET requests. These version 3 requests must include a matching password. By default, version 1 and 2 requests are rejected. If enabled, version 1 and 2 requests must have a matching community string.

### MIB Files

IronPort Systems provides “enterprise” MIBs for Email and Web Security appliances as well as a “Structure of Management Information” (SMI) file:

- `ASYNCOS-MAIL-MIB.txt` — an SNMPv2 compatible description of the Enterprise MIB for IronPort Email Security appliances.
IRONPORT-SMI.txt — defines the role of the asyncoswebsecurityappliance-mib in IronPort’s SNMP managed products. These files are available on the documentation CD included with your IronPort appliance. You can also find these files on the Cisco IronPort Customer Support site.

**Hardware Objects**

Hardware sensors conforming to the Intelligent Platform Management Interface Specification (IPMI) report temperature, fan speed, and power supply status.

Table 22-4 shows what hardware derived objects are available for monitoring on what models. The number displayed is the number of instances of that object that can be monitored. For example, you can query the RPMs for 4 fans in the S350 appliance.

<table>
<thead>
<tr>
<th>Model</th>
<th>Ambient Temp</th>
<th>Fans</th>
<th>Power Supply</th>
<th>Disk Status</th>
<th>NIC Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>S160</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>S350</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>S360</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>S650</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>S660</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

**Hardware Traps**

Table 22-5 lists the temperature and hardware conditions that cause a hardware trap to be sent:

<table>
<thead>
<tr>
<th>Model</th>
<th>High Temp (Ambient)</th>
<th>Fan Failure</th>
<th>Power Supply</th>
<th>RAID</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>S160/S350/S650/S660</td>
<td>47C</td>
<td>0 RPMs</td>
<td>Status Change</td>
<td>Status Change</td>
<td>Status Change</td>
</tr>
</tbody>
</table>
Status change traps are sent when the status changes. Fan Failure and high temperature traps are sent every 5 seconds. The other traps are failure condition alarm traps — they are sent once when the state changes (healthy to failure). It is a good idea to poll for the hardware status tables and identify possible hardware failures before they become critical. Temperatures within 10 per cent of the critical value may be a cause for concern.

Note that failure condition alarm traps represent a critical failure of the individual component, but may not cause a total system failure. For example, a single fan or power supply can fail on a S650 appliance and the appliance will continue to operate.

### SNMP Traps

SNMP provides the ability to send traps, or notifications, to advise an administration application (an SNMP management console, typically) 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 IronPort appliance). After the condition has been met, the SNMP agent then forms an SNMP packet and sends it over port 162, the standard SNMP trap port. In the example below, the trap target of 10.1.1.29 and the Trap Community string are entered. This is the host running the SNMP management console software that will receive the SNMP traps from the IronPort appliance.

You can configure SNMP traps (enable or disable specific traps) when you enable SNMP for an interface. To specify multiple trap targets: when prompted for the trap target, you may enter up to 10 comma separated IP addresses.
CLI Example

In the following example, the `snmpconfig` command is used to enable SNMP on the “PublicNet” interface on port 161. A passphrase for version 3 is entered and then re-entered for confirmation. The system is configured to service version 1 and 2 requests, and the community string `public` is entered for GET requests from those versions 1 and 2. The trap target of `10.1.1.29` is entered. Finally, system location and contact information is entered.

```bash
example.com> snmpconfig

Current SNMP settings:

SNMP Disabled.

Choose the operation you want to perform:

- SETUP - Configure SNMP.

[>] setup

Do you want to enable SNMP? [N]> y

Please choose an IP interface for SNMP requests.

1. Management (192.168.1.1/24: wsa01-vmw1-tpub.qa)

[1]>

Enter the SNMPv3 passphrase.

> 

Please enter the SNMPv3 passphrase again to confirm.
```
Which port shall the SNMP daemon listen on?

[161]>

Service SNMP V1/V2c requests? [N]> y

Enter the SNMP V1/V2c community string.

[]> public

From which network shall SNMP V1/V2c requests be allowed?

[192.168.1.1]>

Enter the Trap target as a host name, IP address or list of IP addresses separated by commas (IP address preferred). Enter "None" to disable traps.

[None]> 10.1.1.29

Enter the Trap Community string.

[]> tcomm

Enterprise Trap Status

1. CPUUtilizationExceeded  Disabled
2. RAIDStatusChange       Enabled
3. connectivityFailure  Disabled
4. fanFailure  Enabled
5. highTemperature  Enabled
6. keyExpiration  Enabled
7. linkDown  Enabled
8. linkUp  Enabled
9. memoryUtilizationExceeded  Disabled
10. powerSupplyStatusChange  Enabled
11. resourceConservationMode  Enabled
12. updateFailure  Enabled
13. upstream_proxy_failure  Enabled

Do you want to change any of these settings? [N]> y

Do you want to disable any of these traps? [Y]> n

Do you want to enable any of these traps? [Y]> y

Enter number or numbers of traps to enable. Separate multiple numbers with commas.
[]> 1,3
What threshold would you like to set for CPU utilization?

[95]>

What URL would you like to check for connectivity failure?

[http://downloads.ironport.com]>

Enterprise Trap Status

1. CPUUtilizationExceeded       Enabled
2. RAIDStatusChange             Enabled
3. connectivityFailure          Enabled
4. fanFailure                   Enabled
5. highTemperature             Enabled
6. keyExpiration                Enabled
7. linkDown                     Enabled
8. linkUp                       Enabled
9. memoryUtilizationExceeded    Disabled
10. powerSupplyStatusChange     Enabled
11. resourceConservationMode    Enabled
12. updateFailure               Enabled
13. upstream_proxy_failure      Enabled

Do you want to change any of these settings? [N]>

Cisco IronPort AsyncOS 7.1 for Web User Guide
Enter the System Location string.

[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3

Enter the System Contact string.

[snmp@localhost]> Joe Administrator, x8888

Current SNMP settings:

Listening on interface "Management" 192.168.1.1 port 161.

SNMP v3: Enabled.

SNMP v1/v2: Enabled, accepting requests from subnet 192.168.1.1.

SNMP v1/v2 Community String: public

Trap target: 10.1.1.29

Location: Network Operations Center - west; rack #30, position 3

System Contact: Joe Administrator, x8888

Choose the operation you want to perform:

- SETUP - Configure SNMP.

[ ]> example.com>
This chapter contains the following sections:

- Web Security Appliance Reports Overview, page 23-2
- Overview Page, page 23-2
- Users Page, page 23-5
- User Details Page, page 23-7
- Web Sites Page, page 23-10
- URL Categories Page, page 23-12
- Application Visibility Page, page 23-16
- Anti-Malware Page, page 23-18
- Client Malware Risk Page, page 23-22
- Web Reputation Filters Page, page 23-29
- L4 Traffic Monitor Data Page, page 23-31
- Reports by User Location Page, page 23-33
- Web Tracking Page, page 23-35
- System Capacity Page, page 23-40
- System Status Page, page 23-44
Web Security Appliance Reports Overview

This chapter discusses the report pages available in the Web Security appliance. For more information on working with reports, such as choosing report columns, exporting reports to an external file, or scheduling reports, see Reporting, page 22-1.

This chapter describes the following reports:

- Overview Page, page 23-2
- Users Page, page 23-5
- User Details Page, page 23-7
- Web Sites Page, page 23-10
- URL Categories Page, page 23-12
- Application Visibility Page, page 23-16
- Anti-Malware Page, page 23-18
- Client Malware Risk Page, page 23-22
- Web Reputation Filters Page, page 23-29
- L4 Traffic Monitor Data Page, page 23-31
- Reports by User Location Page, page 23-33
- Web Tracking Page, page 23-35
- System Capacity Page, page 23-40

Overview Page

The Reporting > Overview page provides a synopsis of the activity on your Cisco IronPort appliances. It includes graphs and summary tables for the incoming and outgoing messages.

Figure 23-1 shows the Overview page.
Figure 23-1  The Overview Page

Time Range: 30 days
03 May 2006 00:00 to 03 Jun 2006 23:59 GMT

Total Web Proxy Activity
No data was found in the selected time range.

Web Proxy Summary

<table>
<thead>
<tr>
<th>Transaction Type</th>
<th>Percentage</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious Traffic</td>
<td>99%</td>
<td>609</td>
</tr>
<tr>
<td>Total Traffic</td>
<td>57.6%</td>
<td>276</td>
</tr>
</tbody>
</table>

Traffic Source Summary

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked by Web Reputation</td>
<td>0</td>
</tr>
<tr>
<td>Blocked by Application</td>
<td>0</td>
</tr>
<tr>
<td>Blocked by URL</td>
<td>0</td>
</tr>
</tbody>
</table>

Top URL Categories by Total Transactions

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference</td>
<td>291</td>
</tr>
<tr>
<td>Unification</td>
<td>20</td>
</tr>
<tr>
<td>Entertainment</td>
<td>10</td>
</tr>
<tr>
<td>Business and Industry</td>
<td>8</td>
</tr>
<tr>
<td>Health and Nutrition</td>
<td>6</td>
</tr>
<tr>
<td>Travel</td>
<td>5</td>
</tr>
<tr>
<td>Social Networking</td>
<td>5</td>
</tr>
</tbody>
</table>

Top Application Types by Total Transactions

<table>
<thead>
<tr>
<th>Application Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>1</td>
</tr>
<tr>
<td>Search</td>
<td>1</td>
</tr>
</tbody>
</table>

Top Threats by Detected Transactions

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious</td>
<td>20</td>
</tr>
</tbody>
</table>

Top 10 Malware Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAR</td>
<td>35</td>
</tr>
<tr>
<td>ZIP</td>
<td>20</td>
</tr>
<tr>
<td>MSI</td>
<td>10</td>
</tr>
<tr>
<td>EXE</td>
<td>5</td>
</tr>
<tr>
<td>DLL</td>
<td>3</td>
</tr>
</tbody>
</table>

Top Threats by Detection Transactions

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious</td>
<td>20</td>
</tr>
<tr>
<td>Suspicious</td>
<td>10</td>
</tr>
</tbody>
</table>

Chapter 23  Web Security Appliance Reports

Overview Page
At a high level the Overview page shows you statistics about the URL and User usage, Web Proxy activity, and various transaction summaries. The transaction summaries gives you further trending details on, for example suspect transactions, and right across from this graph, how many of those suspect transactions are blocked and in what manner they are being blocked.

The lower half of the Overview page is about usage. That is, the top URL categories being viewed, the top application types and categories that are being blocked, and the top users that are generating these blocks or warnings.

Table 23-1 describes the information on the Overview page.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range (drop-down list)</td>
<td>A menu that allows to choose the time range of the data contained in the report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td>Total Web Proxy Activity</td>
<td>This section displays the Web Proxy activity. This section displays the actual number of transactions (vertical scale) as well as the approximate date that the activity occurred (horizontal timeline).</td>
</tr>
<tr>
<td>Web Proxy Summary</td>
<td>This section allows you to view the percentage of Web Proxy activity that are suspect, or clean Web Proxy activity, including the total number of transactions.</td>
</tr>
<tr>
<td>L4 Traffic Monitor Summary</td>
<td>This section reports on traffic monitored and blocked by the L4 Traffic Monitor.</td>
</tr>
<tr>
<td>Suspect Transactions</td>
<td>This section allows you to view the web transactions that have been labeled as suspect by the various security components.</td>
</tr>
<tr>
<td></td>
<td>This section displays the actual number of transactions (vertical scale) as well as the approximate date that the activity occurred (horizontal timeline).</td>
</tr>
<tr>
<td>Suspect Transactions Summary</td>
<td>This section allows you to view the percentage of blocked or warned transactions that are suspect. Additionally, you can see the type of transactions that have been detected and blocked, and the actual number of times that this transaction was blocked.</td>
</tr>
</tbody>
</table>
Chapter 23  Web Security Appliance Reports

Users Page

Table 23-1  Overview Report Page Components (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top URL Categories by Total Transactions</td>
<td>This section displays the top 10 URL categories that have been blocked. (URL category on the vertical scale by the number of times requests in that category were blocked on the horizontal scale.)</td>
</tr>
<tr>
<td>Top Application Types by Total Transactions</td>
<td>This section displays the top application types that have been blocked by the AVC engine. (The application type on the vertical scale by the number of times requests for applications in that type were blocked on the horizontal scale.)</td>
</tr>
<tr>
<td>Top Malware Categories Detected</td>
<td>This section displays all malware categories that have been detected.</td>
</tr>
<tr>
<td>Top Users Blocked or Warned Transactions</td>
<td>This section displays the users that are generating the blocked or warned transactions. Authenticated users are displayed username and unauthenticated users are displayed by IP address.</td>
</tr>
<tr>
<td></td>
<td>You can choose to make usernames unrecognizable in reports. For more information on how to do this, see the “Working with Usernames in Reports” section on page 22-2.</td>
</tr>
</tbody>
</table>

Users Page

The Reporting > Users page provides several links that allows you to view web traffic information for individual users. You can view how much time users on the network have spent on the Internet or on a particular website or URL, and how much bandwidth users have used.

Figure 23-2 shows the Users page.
Table 23-2 describes the information on the Users page.

**Table 23-2 Users Report Page Components**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Range (drop-down list)</strong></td>
<td>A menu that allows to choose the time range of the data contained in the report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td><strong>Top Users by Transactions Blocked</strong></td>
<td>This section lists the users (vertical scale) that have the greatest number of blocked transactions (horizontal scale). Authenticated users are displayed username and unauthenticated users are displayed by IP address. You can choose to make usernames unrecognizable in reports. For more information on how to do this, see the “Working with Usernames in Reports” section on page 22-2.</td>
</tr>
</tbody>
</table>
The User Details page allows you to investigate individual user’s activity on the network. You might want to view this information if you need to run user-level investigations and need to find out, for example, what sites users are visiting, what malware threats they are encountering, what URL categories they are accessing, and how much time each user spends at these sites.

To display the User Details page for a user, click on the user from the User Table on the Reporting > Users page and the following page appears:
## Figure 23-3  User Details Page

**Users > 10.251.60.24**

<table>
<thead>
<tr>
<th>User Category</th>
<th>Bandwidth Used</th>
<th>Time Spent (Min)</th>
<th>Blocked SSL Category</th>
<th>Transactions Completed</th>
<th>Total Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Engines and Portal</td>
<td>107</td>
<td>0.71</td>
<td>0</td>
<td>0</td>
<td>107</td>
</tr>
<tr>
<td>Business and Finance</td>
<td>93</td>
<td>0.59</td>
<td>0</td>
<td>0</td>
<td>93</td>
</tr>
<tr>
<td>Computers and Internet</td>
<td>46</td>
<td>0.41</td>
<td>0</td>
<td>0</td>
<td>46</td>
</tr>
<tr>
<td>Advertising</td>
<td>36</td>
<td>0.32</td>
<td>0</td>
<td>0</td>
<td>36</td>
</tr>
<tr>
<td>Games</td>
<td>25</td>
<td>0.24</td>
<td>0</td>
<td>0</td>
<td>25</td>
</tr>
<tr>
<td>Email</td>
<td>14</td>
<td>0.21</td>
<td>0</td>
<td>0</td>
<td>14</td>
</tr>
<tr>
<td>Other</td>
<td>11</td>
<td>0.19</td>
<td>0</td>
<td>0</td>
<td>11</td>
</tr>
</tbody>
</table>

**User Details**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Bandwidth Used</th>
<th>Time Spent (Min)</th>
<th>Transactions Completed</th>
<th>Total Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.com</td>
<td>107</td>
<td>0.71</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>yahoo.com</td>
<td>93</td>
<td>0.59</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>hotmail.com</td>
<td>46</td>
<td>0.41</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>aol.com</td>
<td>36</td>
<td>0.32</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>msn.com</td>
<td>25</td>
<td>0.24</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>comcast.com</td>
<td>14</td>
<td>0.21</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>usa.com</td>
<td>11</td>
<td>0.19</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Recent Searches**

<table>
<thead>
<tr>
<th>Search Term</th>
<th>Transactions Completed</th>
<th>Total Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.com</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>yahoo.com</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>hotmail.com</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>aol.com</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>msn.com</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>comcast.com</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>usa.com</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Recent Unblocked**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Bandwidth Used</th>
<th>Time Spent (Min)</th>
<th>Transactions Completed</th>
<th>Total Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.com</td>
<td>107</td>
<td>0.71</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>yahoo.com</td>
<td>93</td>
<td>0.59</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>hotmail.com</td>
<td>46</td>
<td>0.41</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>aol.com</td>
<td>36</td>
<td>0.32</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>msn.com</td>
<td>25</td>
<td>0.24</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>comcast.com</td>
<td>14</td>
<td>0.21</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>usa.com</td>
<td>11</td>
<td>0.19</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Recent Blocked**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Bandwidth Used</th>
<th>Time Spent (Min)</th>
<th>Transactions Completed</th>
<th>Total Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.com</td>
<td>107</td>
<td>0.71</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>yahoo.com</td>
<td>93</td>
<td>0.59</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>hotmail.com</td>
<td>46</td>
<td>0.41</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>aol.com</td>
<td>36</td>
<td>0.32</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>msn.com</td>
<td>25</td>
<td>0.24</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>comcast.com</td>
<td>14</td>
<td>0.21</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>usa.com</td>
<td>11</td>
<td>0.19</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Table 23-3 describes the information on the User Details page.

### Table 23-3  User > User Details Report Page Components

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Range (drop-down list)</strong></td>
<td>A menu that allows to choose the time range of the data contained in the report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td><strong>URL Categories by Total Transactions</strong></td>
<td>This section lists the specific URL categories that a specific user is using.</td>
</tr>
<tr>
<td><strong>Trend by Total Transaction</strong></td>
<td>This graph displays at what times the user accessed the web. For example, this graph will indicate if there is a large spike in web traffic during certain hours of the day, and when those spikes occur. Using the Time Range drop-down list, you can expand this graph to see a more or less granular span of time that this user was on the web.</td>
</tr>
<tr>
<td><strong>URL Categories Matched</strong></td>
<td>This section shows all matched URL categories during a specified time range for both completed and blocked transactions. You can use column headings to sort data. When the section contains more than 10 categories, you can use the Items Displayed menu to configure the number of URL categories to display. From this section you can also search for data that applies to a specific URL category in the Find URL Category field. For more information, see Searching Data, page 22-5.</td>
</tr>
<tr>
<td><strong>Domains Matched</strong></td>
<td>From this section you can find out about a specific Domain or IP address that this user has accessed. You can also see the time spent on those categories, and various other information that you have set from the column view. In the text field at the bottom of the section enter the Domain or IP address and click Find Domain or IP. The domain or IP address does not need to be an exact match.</td>
</tr>
</tbody>
</table>
The Reporting > Web Sites page is an overall aggregation of the activity that is happening on the Web Security appliance. From this page you can monitor high-risk web sites accessed during a specific time range.

Figure 23-4 shows the Web Sites page:
Table 23-4 describes the information on the Web Sites page:

### Table 23-4  Web Sites Report Page Components

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Range (drop-down list)</strong></td>
<td>A menu that allows to choose the time range of the data contained in the report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td><strong>Top Domains by Total Transactions</strong></td>
<td>This section lists the top domains that are being visited on the site in a graph format.</td>
</tr>
</tbody>
</table>
The Reporting > URL Categories page can be used to view the URL categories that are being visited by users on the network.

Figure 23-5 shows the URL Categories page.
Figure 23-5  URL Categories Page

URL Categories

Table 23-5 describes the information on the URL Categories page.

Table 23-5  URL Categories Report Page Components

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Range (drop-down list)</strong></td>
<td>A menu that allows to choose the time range of the data contained in the report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td><strong>Top URL Categories by Total Transactions</strong></td>
<td>This section lists the top URL categories that are being visited on the site in a graph format.</td>
</tr>
</tbody>
</table>
Table 23-5  URL Categories Report Page Components (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top URL Categories by Blocked and Warned</td>
<td>This section lists the top URL that triggered a block or warning action to occur per transaction in a graph format. For example, a user went to a certain URL and because of a specific policy that is in place, this triggered a block action or a warning. This URL then gets listed in this graph as a transaction blocked or warning.</td>
</tr>
</tbody>
</table>
Chapter 23  Web Security Appliance Reports

URL Categories Page

Table 23-5  URL Categories Report Page Components (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| URL Categories Matched | The URL Categories Matched section shows all the URL categories during a specified time range for both completed, warned and blocked transactions. This is an interactive table with interactive column headings that you can use to sort data as you need. The Items Displayed menu changes the number of URL categories displayed in the list. You can use column headings to sort data, and you can choose which columns to display. For more information, see the “Working with Columns on Report Pages” section on page 22-5. When the section contains more than 10 URL categories, you can use the Items Displayed menu to configure the number of URL categories to display. From this section you can also search for data that applies to a specific URL category in the Find URL Category field. For more information, see Searching Data, page 22-5. The percentage of uncategorized URLs on the URL Categories page is typically around 15-20%. If the percentage of uncategorized URLs is higher than that, consider the following options:  
  • For specific localized URLs, you can create custom URL categories and apply them to specific users or group policies. For more information, see the “Custom URL Categories” section on page 16-16.  
  • You can report misclassified and uncategorized URLs to the Cisco IronPort Customer Support site at the following URL:  
    These get evaluated for subsequent rule updates.  
  • Verify Web Reputation Filtering and Anti-Malware Filtering are enabled. Often times, the correlation between malware and URLs with suspect content is high and it is likely that they may get caught by subsequent filters. The system pipeline is set up to catch malicious traffic with other downstream filters if URL filtering does not have a verdict. |
Using The URL Categories Page in Conjunction with Other Reporting Pages

One of the advantages of the URL Categories page is that it can be used in conjunction with the Application Visibility Page and the Users Page to investigate a particular user, but also what types of applications or websites that a particular user is trying to access.

For example, from the URL Categories Page you can generate a high level report for Human Resources which details all the URL categories that are visited by the site. From the same page, you can gather further details in the URL Categories interactive table about the URL category ‘Streaming Media’. By clicking on the Streaming Media category link, you can view the specific URL Categories report page. This page not only displays the top users that are visiting streaming media sites (in the Top Users by Category for Total Transactions section), but also displays the domains that are visited (in the Domains Matched interactive table) such as YouTube.com or QuickPlay.com.

At this point, you are getting more and more granular information for a particular user. Now, let’s say this particular user stands out because of their usage, and you want to find out exactly what they are accessing. From here you can click on the user in the Users table. This action takes you to the User Details Page, where you can view the user trends for that user, and find out exactly what they have been doing on the web.

If you wanted to go further, you can now get down to web tracking details by clicking on Transactions Completed link in the interactive table. This brings up the Web Tracking Page where you can see the actual details about what dates the user accessed the sites, the full URL, the time spent on that URL, etc.

Application Visibility Page

The Reporting > Application Visibility page shows the applications and application types used and blocked as detected by the Application Visibility and Control engine.

Figure 23-6 shows the Application Visibility page.
Table 23-6 describes the information on the Application Visibility page.

**Table 23-6 Application Visibility Report Page Components**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Range (drop-down list)</strong></td>
<td>A menu that allows to choose the time range of the data contained in the report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td><strong>Top Application Types by Total Transactions</strong></td>
<td>This section lists the top application types that are being visited on the site in a graph format. For example, Instant Messaging tools such as Yahoo Instant Messenger, and Presentation application types.</td>
</tr>
</tbody>
</table>
Table 23-6  Application Visibility Report Page Components (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Applications by Blocked Transactions</td>
<td>This section lists the top application types that triggered a block action to occur per transaction in a graph format. For example, a user has tried to start a certain application, such as Google Talk, and because of a configured policy, this triggered a block action. This application then gets listed in this graph as a transaction blocked or warning.</td>
</tr>
<tr>
<td>Application Types Matched</td>
<td>The Application Types Matched table allows you to view granular details about the application types listed in the Top Applications Type by Total Transactions graph. From the Applications column you can click on an application to view details.</td>
</tr>
<tr>
<td>Applications Matched</td>
<td>The Applications Matched section shows all the application during a specified time range. You can sort the table by clicking the column headers, and choose which columns of data to display. For more information, see Working with Columns on Report Pages, page 22-5. When the section contains more than 10 applications, you can use the Items Displayed menu to configure the number of applications to display. You can search for data on a specific application in the Find Application field. For more information, see Searching Data, page 22-5.</td>
</tr>
</tbody>
</table>

Anti-Malware Page

The Reporting > Anti-Malware page allows you to monitor and identify malware detected by the IronPort DVS engine. Figure 23-7 shows the Anti-Malware page.
Table 23-7 describes the information on the Anti-Malware page.

### Table 23-7  Anti-Malware Report Page Components

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Range (drop-down list)</strong></td>
<td>A menu that allows to choose the time range of the data contained in the report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td><strong>Top Malware Categories Detected</strong></td>
<td>This section displays the top malware categories detected by the DVS engine. This information is displayed in graph format.</td>
</tr>
<tr>
<td><strong>Top Malware Threats Detected</strong></td>
<td>This section displays the top malware threats detected by the DVS engine. This information is displayed in graph format.</td>
</tr>
</tbody>
</table>
The Malware Category Report page allows you to view detailed information on an individual Malware Category and what it is doing on your network.

To access the Malware Category report page, perform the following:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Navigate to the <strong>Reporting &gt; Anti-Malware</strong> page.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Anti-Malware page appears.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>In the Malware Categories interactive table, click on a category in the Malware Category column.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Malware Category report page appears.</td>
</tr>
</tbody>
</table>
Malware Threat Report Page

The Malware Threat Report page report shows clients at risk for a particular threat, displays a list of potentially infected clients, and links to the Client Detail page. The trend graph at the top of the report shows monitored and blocked transactions for a threat during the specified time range. The table at the bottom shows the actual number of monitored and blocked transactions for a threat during the specified time range.

To access the Malware Threat report page, perform the following:

**Step 1** Navigate to the Reporting > Anti-Malware page.
The Anti-Malware page appears.

**Step 2** In the Malware Threat table, click on a category in the Malware Category column.
The Malware Threat report page appears.
The Reporting > Client Malware Risk page is a security-related reporting page that can be used to monitor client malware risk activity.

From the Client Malware Risk page, a system administrator can see which of their users are encountering the most blocks or warnings. Given the information gathered from this page, the administrator can click on the user link to view what this user doing on the web that makes them run into so many blocks or warnings and setting off more detections than the rest of the users on the network.

Additionally, from the Client Malware Risk page you can see L4TM activity for a specific IP address.

Figure 23-10 shows the Client Malware Risk page.
# Chapter 23   Web Security Appliance Reports

## Client Malware Risk Page

### Figure 23-10   Client Malware Risk Page

#### Client Malware Risk

Time Range: Day

15 Nov 2009 09:00 to 16 Nov 2009 09:30 (GMT -0800)

**Web Proxy: Top Clients by Malware Risk**

<table>
<thead>
<tr>
<th>User ID / Client IP Address</th>
<th>Malware Transactions Monitored</th>
<th>Malware Transactions Blocked</th>
<th>Total Malware Transactions Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>173.37.10.103</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>173.37.16.45</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>173.37.10.99</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>173.37.11.230</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>173.37.10.118</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>173.37.10.76</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>10.21.126.102</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10.21.140.253</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10.21.69.104</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10.254.40.15</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**L4 Traffic Monitor: Top Clients by Malware Risk**

<table>
<thead>
<tr>
<th>Client IP Address</th>
<th>Suspicious Malware Connections Monitored</th>
<th>Suspicious Malware Connections Blocked</th>
<th>Total Suspicious Malware Connections Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>173.37.8.153</td>
<td>490</td>
<td>0</td>
<td>490</td>
</tr>
<tr>
<td>173.37.8.46</td>
<td>422</td>
<td>0</td>
<td>422</td>
</tr>
<tr>
<td>173.37.8.21</td>
<td>364</td>
<td>0</td>
<td>364</td>
</tr>
<tr>
<td>173.37.8.47</td>
<td>396</td>
<td>0</td>
<td>396</td>
</tr>
<tr>
<td>173.37.8.41</td>
<td>276</td>
<td>0</td>
<td>276</td>
</tr>
<tr>
<td>173.37.8.128</td>
<td>102</td>
<td>0</td>
<td>102</td>
</tr>
<tr>
<td>173.37.8.146</td>
<td>86</td>
<td>0</td>
<td>86</td>
</tr>
<tr>
<td>173.37.9.38</td>
<td>25</td>
<td>0</td>
<td>25</td>
</tr>
<tr>
<td>173.37.9.5</td>
<td>25</td>
<td>0</td>
<td>25</td>
</tr>
<tr>
<td>173.37.9.6</td>
<td>25</td>
<td>0</td>
<td>25</td>
</tr>
</tbody>
</table>

---

Cisco IronPort AsyncOS 7.1 for Web User Guide

OL-23207-01

23-23
Table 23-8 describes the information on the Client Malware Risk page.

Table 23-8  Client Malware Risk Report Page Components

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range (drop-down list)</td>
<td>A menu that allows to choose the time range of the data contained in the report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td>Web Proxy: Top Clients by Malware Risk</td>
<td>This section displays the top ten users that have encountered a malware risk. This information is displayed in graph format.</td>
</tr>
<tr>
<td>L4 Traffic Monitor: Top Clients by Malware Risk</td>
<td>This section displays the top ten users that have encountered a L4 Traffic Monitoring risk. This information is displayed in graph format.</td>
</tr>
<tr>
<td>Web Proxy: Clients by Malware Risk</td>
<td>The Web Proxy: Clients by Malware Risk table shows detailed information about particular clients that are displayed in the Web Proxy: Top Clients by Malware Risk section. You can click each user in this table to open the Client Detail Page that provides detailed information for each user. For more information, see the “Client Detail Page” section on page 23-24. Clicking on any of the links in the table allows you to view more granular details about individual users and what activity they are performing that is triggering the malware risk. For example, clicking on the link in the “User ID / Client IP Address” column takes you to a User page for that user.</td>
</tr>
<tr>
<td>L4 Traffic Monitor: Clients by Malware Risk</td>
<td>The Web Proxy: Clients Malware Risk interactive table shows detailed information about individual users and what activity they are performing that is triggering the L4 Traffic Monitoring malware risk. Clicking on the link in the User/IP address column will take you to a User page for that IP address.</td>
</tr>
</tbody>
</table>

**Client Detail Page**

The Client Details page shows all the web activity and malware risk data for a particular client during the specified time range.

To access the Client Details page, perform the following:
Step 1  Navigate to the Reporting > Client Malware Risk page.
The Client Malware Risk page appears.

Step 2  In the Web Proxy: Clients by Malware Risk section, click on a user in the “User ID / Client IP Address” column.
The Client Details page appears.
You can sort each table on the **Client Details** page by clicking the column headers, and choose which columns of data to display. For more information, see Working with Columns on Report Pages, page 22-5.
Table 23-9 describes the information on the Client Details page.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range (drop-down list)</td>
<td>A menu that allows to choose the time range of the data contained in the report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td>URL Categories by Total Transactions</td>
<td>This section lists the specific URL Categories that a specific user is using.</td>
</tr>
<tr>
<td>Trend by Total Transaction</td>
<td>This graph displays at what times the user accessed the web. For example, this graph will indicate if there is a large spike in web traffic during certain hours of the day, and when those spikes occur. Using the Time Range drop-down list, you can expand this graph to see a more or less granular span of time that this user was on the web.</td>
</tr>
<tr>
<td>URL Categories Matched</td>
<td>The URL Categories Matched section shows all matched categories that could potentially be a malware risk during a specified time range for both completed and blocked transactions.</td>
</tr>
<tr>
<td></td>
<td>You can sort the table by clicking the column headers, and choose which columns of data to display. For more information, see Working with Columns on Report Pages, page 22-5.</td>
</tr>
<tr>
<td></td>
<td>When the section contains more than 10 categories, you can use the Items Displayed menu to configure the number of categories to display.</td>
</tr>
<tr>
<td></td>
<td>You can search for data on a specific URL category in the Find URL Category field. For more information, see Searching Data, page 22-5.</td>
</tr>
<tr>
<td>Domains Matched</td>
<td>From the Domains Matched section you can find out about a specific Domain or IP address that this user has accessed that could potentially be a malware risk. You can also see the time spent on those domains, and various other information that you have set from the column view. You can search for data on a specific domain in the Find Domain or IP field. For more information, see Searching Data, page 22-5.</td>
</tr>
</tbody>
</table>
Chapter 23 Web Security Appliance Reports

Table 23-9 Client Malware Risk > Client Details Report Page Components

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications Matched</td>
<td>From this section you can find a specific application that a specific user is using that could potentially be a Malware risk. For example, if a user is accessing a site that requires use of a lot of Flash video, you will see the application type in the Application column. As a system administrator, you might have decided that anything with Flash video poses a malware risk. Therefore, this application will show up in the Applications Matched section. You can search for data on a specific application in the Find Application field. For more information, see Searching Data, page 22-5.</td>
</tr>
<tr>
<td>Malware Threats Detected</td>
<td>From this table you can see the top malware threats that a specific user is triggering that could potentially be a malware risk. You can search for data on a specific malware threat name in the Find Malware Threat field. For more information, see Searching Data, page 22-5.</td>
</tr>
<tr>
<td>Policies Matched</td>
<td>From this section you can find the policy groups that applied to this user when accessing the web. You can search for policy group names in the Find Policy field. For more information, see Searching Data, page 22-5.</td>
</tr>
</tbody>
</table>

Note The client reports sometimes show a user with an asterisk (*) at the end of the username. For example, the Client report might show an entry for both “jsmith” and “jsmith**”. Usernames listed with an asterisk (*) indicate the username provided by the user, but not confirmed by the authentication server. This happens when the authentication server was not available at the time and the appliance is configured to permit traffic when authentication service is unavailable.
Web Reputation Filters Page

The **Reporting > Web Reputation Filters** page is a security-related reporting page that allows you to view the results of your set Web Reputation Filters for transactions during a specified time range.

*Figure 23-12* shows the Web Reputation Filters page.
### Web Reputation Filter Page

#### Figure 23-12

**Web Reputation Filters**

<table>
<thead>
<tr>
<th>Time Range</th>
<th>Start Date</th>
<th>End Date</th>
<th>Filter</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 2006</td>
<td>22:00</td>
<td>15 Mar 2006</td>
<td>22:00</td>
<td>(GMT)</td>
</tr>
</tbody>
</table>

#### Web Reputation Actions (Total)

<table>
<thead>
<tr>
<th>Action</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>0</td>
</tr>
<tr>
<td>Scan Failure: Malware</td>
<td>0</td>
</tr>
<tr>
<td>Scan Failure: Class</td>
<td>0</td>
</tr>
<tr>
<td>Allow</td>
<td>14</td>
</tr>
<tr>
<td>Total</td>
<td>14</td>
</tr>
</tbody>
</table>

#### Web Reputation Threat Types by Blocked Transactions

- Threat Type - Transactions
- Score - Message

#### Web Reputation Actions (Total by Score)

<table>
<thead>
<tr>
<th>Score</th>
<th>Block</th>
<th>Scan Failure: Malware</th>
<th>Scan Failure: Class</th>
<th>Allow</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Web Reputation Threat Types by Allowed Transactions

- Threat Type - Transactions
- Score - Message

#### Web Reputation Actions (Total by Score)

<table>
<thead>
<tr>
<th>Score</th>
<th>Block</th>
<th>Scan Failure: Malware</th>
<th>Scan Failure: Class</th>
<th>Allow</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Table 23-10 describes the information on the Web Reputation Filters page.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range (drop-down list)</td>
<td>A menu that allows to choose the time range of the data contained in the report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td>Web Reputation Actions (Trend)</td>
<td>This section, in graph format, displays the total number of web reputation actions (vertical) against the time specified (horizontal timeline). From this you can see potential trends over time for web reputation actions.</td>
</tr>
<tr>
<td>Web Reputation Actions (Volume)</td>
<td>This section displays the web reputation action volume in percentages by transactions.</td>
</tr>
<tr>
<td>Web Reputation Threat Types by Blocked Transactions</td>
<td>This section displays the threat types that were blocked due to a low reputation score.</td>
</tr>
<tr>
<td>Web Reputation Threat Types by Scanned Further Transactions</td>
<td>This section displays the threat types that resulted in a reputation score that indicated to scan the transaction. It shows both monitored and blocked transactions.</td>
</tr>
<tr>
<td>Web Reputation Actions (Breakdown by Score)</td>
<td>This interactive table displays the web reputation scores broken down for each action.</td>
</tr>
</tbody>
</table>

**L4 Traffic Monitor Data Page**

The **Reporting> L4 Traffic Monitor** page is a security-related reporting page that displays information about malware ports and malware sites that the L4 Traffic Monitor has detected during the specified time range.

The L4 Traffic Monitor listens to network traffic that comes in over all ports on the appliance and matches domain names, and IP addresses against entries in its own database tables to determine whether to allow incoming and outgoing traffic.

The upper part of the report displays the number of connections for each of the top malware ports and web sites. The lower part of the report displays malware ports and sites detected.

Figure 23-13 shows the L4 Traffic Monitor Data page.
Table 23-11 describes the information on the L4 Traffic Monitor page.

### Table 23-11  L4 Traffic Monitor Report Page Components

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Range (drop-down list)</strong></td>
<td>A menu that allows to choose the time range of the data contained in the report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td><strong>Top Malware Ports Detected</strong></td>
<td>This section displays, in graph format, the top malware ports detected by the L4 Traffic Monitor.</td>
</tr>
</tbody>
</table>
Reports by User Location Page

The Reporting > Reports by User Location page allows you to find out what activities your local and remote users are conducting. For more information on remote and local users, see Working with Remote Users, page 13-2.

Activities include:

- URL categories that are being accessed by the local and remote users.
- Anti-Malware activity that is being triggered by sites the local and remote users are accessing.
- Web Reputation of the sites being accessed by the local and remote users.
- Applications that are being accessed by the local and remote users.
- Users (local and remote).
- Domains accessed by local and remote users.

Figure 23-14 shows the Reports by User Location page.
Figure 23-14  Reports by User Location Page

Reports by User Location

[ Summary | URL Category | Anti-Malware | Web Reputation | Applications | Users | Domains ]

Printable (PDF)

Time Range: 31 days
02 Jun 2010 00:00 to 02 Jul 2010 22:44 (GMT +01:00)

Total Web Proxy Activity - Remote Users

No data was found in the selected time range

Web Proxy Summary

All data was found in the selected time range

Total Web Proxy Activity - Local Users

Web Proxy Summary

<table>
<thead>
<tr>
<th>Web Proxy</th>
<th>%</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Suspect</td>
<td>100.0%</td>
<td>7</td>
</tr>
</tbody>
</table>

Total Transactions: 7

Export...

Suspect Transactions Detected - Remote Users

No data was found in the selected time range

Suspect Transactions Summary

No data was found in the selected time range

Suspect Transactions Detected - Local Users

Web Proxy Summary

<table>
<thead>
<tr>
<th>Web Proxy</th>
<th>%</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked or Warned by URL Category</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Blocked by Application</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Blocked by Web Reputation Filters</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Transactions Detected by Anti-Malware</td>
<td>0.0%</td>
<td>0</td>
</tr>
<tr>
<td>Other Blocked Transactions</td>
<td>100.0%</td>
<td>7</td>
</tr>
</tbody>
</table>

Total Transactions: 7

Export...
Table 23-12 describes the information on the Reports by User Location page.

### Table 23-12 Reports by User Location Report Page Components

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range (drop-down list)</td>
<td>A menu that allows to choose the time range of the data contained in the report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td><strong>Total Web Proxy Activity: Remote Users</strong></td>
<td>This section displays, in graph format, the activity of your remote users (vertical) over the specified time (horizontal).</td>
</tr>
<tr>
<td><strong>Web Proxy Summary</strong></td>
<td>This section displays a summary of the activities of the local and remote users on the network.</td>
</tr>
<tr>
<td><strong>Total Web Proxy Activity: Local Users</strong></td>
<td>This section displays, in graph format, the activity of your remote users (vertical) over the specified time (horizontal).</td>
</tr>
<tr>
<td><strong>Suspect Transactions Detected: Remote Users</strong></td>
<td>This section displays, in graph format, the suspect transactions that have been detected due to Access Policies defined for remote users (vertical) over the specified time (horizontal).</td>
</tr>
<tr>
<td><strong>Suspect Transactions Summary</strong></td>
<td>This section displays a summary of suspected transactions of the remote users on the network.</td>
</tr>
<tr>
<td><strong>Suspect Transactions Detected: Local Users</strong></td>
<td>This section displays, in graph format, the suspect transactions that have been detected due to Access Policies defined for your remote users (vertical) over the specified time (horizontal).</td>
</tr>
<tr>
<td><strong>Suspect Transactions Summary</strong></td>
<td>This section displays a summary of suspected transactions of the local users on the network.</td>
</tr>
</tbody>
</table>

From the Reports by User Location page you can generate reports showing the activity of local and remote users. This allows you to easily compare local and remote activities of your users.

### Web Tracking Page

You can use the Reporting > Web Tracking page to track and report on web usage for a particular user or all users. Web tracking aggregates information from individual security components as well as acceptable use enforcement components and records data that can be used to monitor your web traffic patterns and security risks.
The Web Tracking page returns results for individual transactions and the results include the hostname and domain in the URL (such as mail.google.com) instead of just the domain name (such as google.com).

You might want to use it to assist the following roles:

- **HR or Legal manager.** Run an investigative report for an employee during a specific time period.

- **Network security administrator.** Examine whether the company network is being exposed to malware threats through employees’ smartphones.

You can view search results for the type of transactions logged (blocked, monitored, warned, and completed) during a particular time period. You can also filter the data results using several criteria, such as URL category, malware threat, and application.

After you search for a set of transactions, you can choose which columns to display, and you can sort the data by a column. For more information, see the “Working with Columns on Report Pages” section on page 22-5.

**Figure 23-15** shows the Web Tracking page.
To track web usage for one user or all users, perform the following steps:

**Step 1** Navigate to the Reporting > Web Tracking page.

The Web Tracking page appears.
Step 2
Configure the fields defined in Table 23-13.

Table 23-13 Web Tracking Page Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range</td>
<td>Choose the time range on which to report. For more information, see the “Changing the Time Range” section on page 22-3.</td>
</tr>
<tr>
<td>User/Client IP</td>
<td>Optionally, enter an authentication username as it appears in reports or a client IP address that you want to track. When you leave this field empty, the Web Tracking page returns results for all users.</td>
</tr>
<tr>
<td>Website</td>
<td>Optionally, enter a website that you want to track. When you leave this field empty, the Web Tracking page returns results for all websites.</td>
</tr>
<tr>
<td>Transaction Type</td>
<td>Choose the type of transactions that you want to track, either All Transactions, Completed, Blocked, Monitored, or Warned.</td>
</tr>
</tbody>
</table>

Step 3
Optionally, expand the Advanced section and configure the fields defined in Table 23-14 to filter the web tracking results with more advanced criteria.

Table 23-14 Web Tracking Page Advanced Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Category</td>
<td>To filter by a URL category, select Filter by URL Category and choose a URL category by which to filter.</td>
</tr>
<tr>
<td>Application</td>
<td>To filter by an application, select Filter by Application and choose an application by which to filter.</td>
</tr>
<tr>
<td></td>
<td>To filter by an application type, select Filter by Application Type and choose an application type by which to filter.</td>
</tr>
<tr>
<td>Policy</td>
<td>To filter by a policy group, select Filter by Policy and enter a policy group name by which to filter.</td>
</tr>
</tbody>
</table>
Step 4  Click Search.

Results are sorted by time stamp, with the most recent result at the top.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Threat</td>
<td>To filter by a particular malware threat, select Filter by Malware Threat and enter a malware threat name by which to filter.</td>
</tr>
<tr>
<td></td>
<td>To filter by a malware category, select Filter by Malware Category and choose a malware category by which to filter.</td>
</tr>
<tr>
<td>WBRS</td>
<td>In the WBRS section, you can filter by web reputation score and by a particular web reputation threat.</td>
</tr>
<tr>
<td></td>
<td>• To filter by web reputation score, select Score Range and select the upper and lower values by which to filter. Or, you can filter for websites that have no score by selecting No Score.</td>
</tr>
<tr>
<td></td>
<td>• To filter by web reputation threat, select Filter by Reputation Threat and enter a web reputation threat by which to filter.</td>
</tr>
<tr>
<td>Mobile User Security</td>
<td>To filter by the location of users (either remote or local), select Filter by User Location and choose a user type by which to filter.</td>
</tr>
<tr>
<td>User Request</td>
<td>To filter by transactions that were initiated by the client, select Filter by User-Requested Transactions.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When you enable this filter, the Web Tracking results include some “best guess” transactions.</td>
</tr>
</tbody>
</table>
System Capacity Page

The Reporting > System Capacity page displays current and historical information about resource usage on the Web Security appliance.

You might want to use the System Capacity report to accomplish any of the following tasks:

- Learn when the Web Security appliance is exceeding the recommended capacity to help determine when to upgrade or obtain additional appliances.
- Identify historical trends in system behavior which point to upcoming capacity issues which require planning.
- Identify which part of the system is using the most resources to assist with troubleshooting.

Figure 23-17 shows the first four graphs on the System Capacity page.
Figure 23-17  System Capacity Page—Upper Graphs

System Capacity

| Time Range: Day | 24/02/2010 11:00 to 25/02/2010 23:45 (GMT) |

Overall CPU Usage

<table>
<thead>
<tr>
<th>Time</th>
<th>0%</th>
<th>10%</th>
<th>20%</th>
<th>30%</th>
<th>40%</th>
<th>50%</th>
<th>60%</th>
<th>70%</th>
<th>80%</th>
<th>90%</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>03:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>04:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>07:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CPU Usage by Function

<table>
<thead>
<tr>
<th>Time</th>
<th>Web-Filter</th>
<th>Web-Categorization</th>
<th>Logging</th>
<th>Reporting</th>
<th>Web-Replicating</th>
<th>Web-AllClear</th>
<th>Web-Alerts</th>
<th>Scada</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>03:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>04:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>07:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Response Time/Latency (milliseconds)

<table>
<thead>
<tr>
<th>Time</th>
<th>0.00</th>
<th>2.00</th>
<th>4.00</th>
<th>6.00</th>
<th>8.00</th>
<th>10.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>03:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>04:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>06:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>07:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>09:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Transactions Per Second

<table>
<thead>
<tr>
<th>Time</th>
<th>0.00</th>
<th>2.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>01:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>02:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>03:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>04:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>05:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>07:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>08:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>09:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Figure 23-18 shows the last three graphs on the System Capacity page.

The System Capacity report includes graphs that show the overall CPU usage on the appliance. AsyncOS for Web is optimized to use idle CPU resources to improve message throughput. High CPU usage may not indicate a system capacity problem. The CPU Usage by Function graph that displays the percentage of CPU cycles used by different functions, such as the Web Proxy and Logging. The CPU Usage by Function graph can indicate which appliance components use the most resources. If you need to optimize your appliance, this graph can help you determine which functions may need to be tuned.
Chapter 23      Web Security Appliance Reports

The Response Time/Latency and Transactions Per Second graphs shows the overall response time (in milliseconds), and transactions per second for the date range specified in the Time Range drop-down menu.

The lower three graphs on the System Capacity report show the outgoing connections, the bandwidth the appliance uses connecting out to upstream servers, and the size of the Web Proxy memory buffer.

How to Interpret the Data You See on System Capacity Page

When choosing time ranges for viewing data on the System Capacity page, the following is important to remember:

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

- **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.

The “Maximum” value indicator on the System Capacity page is the highest value seen for the specified period. The “Average” value is the average of all values for the specified period. The period of aggregation depends on the interval selected for that report. For example, you can choose to see the Average and Maximum values for each day if the chart is for a month period.
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. Table 23-15 describes each section.

Table 23-15  System Status Report Page Components

<table>
<thead>
<tr>
<th>This Section...</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Security Appliance Status</td>
<td>• System uptime</td>
</tr>
<tr>
<td></td>
<td>• System resource utilization — CPU usage, RAM usage, and percentage of disk space used for reporting and logging.</td>
</tr>
<tr>
<td>Proxy Traffic Characteristics</td>
<td>• Transactions per second</td>
</tr>
<tr>
<td></td>
<td>• Bandwidth</td>
</tr>
<tr>
<td></td>
<td>• Response time</td>
</tr>
<tr>
<td></td>
<td>• Cache hit rate</td>
</tr>
<tr>
<td></td>
<td>• Connections</td>
</tr>
<tr>
<td>Current Configuration</td>
<td>Web Proxy settings:</td>
</tr>
<tr>
<td></td>
<td>• Web Proxy Status — enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td>• Deployment Topology</td>
</tr>
<tr>
<td></td>
<td>• Web Proxy Mode — forward or transparent.</td>
</tr>
<tr>
<td></td>
<td>• IP Spoofing — enabled or disabled.</td>
</tr>
<tr>
<td>L4 Traffic Monitor settings:</td>
<td>• L4 Traffic Monitor Status — enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td>• L4 Traffic Monitor Wiring</td>
</tr>
<tr>
<td></td>
<td>• L4 Traffic Monitor Action — monitor or block.</td>
</tr>
<tr>
<td>Web Security Appliance Version Information</td>
<td>Hardware information</td>
</tr>
</tbody>
</table>
CHAPTER 24

Logging

This chapter contains the following information:

- Logging Overview, page 24-1
- Working with Log Subscriptions, page 24-9
- Access Log File, page 24-19
- W3C Compliant Access Logs, page 24-36
- Custom Formatting in Access Logs and W3C Logs, page 24-39
- Including HTTP/HTTPS Headers in Log Files, page 24-51
- Malware Scanning Verdict Values, page 24-52
- Traffic Monitor Log, page 24-53
- Troubleshooting, page 24-54

Logging Overview

You can use log files to monitor web traffic. To configure the appliance to create log files, you create log subscriptions. A log subscription is an appliance configuration that associates a log file type with a name, logging level, and other parameters, such as size and destination information. You can subscribe to a variety of log file types. For more information about log subscriptions, see Working with Log Subscriptions, page 24-9.

In typical appliance monitoring, the appliance administrator usually reads the following log files:
• **Access log.** Records all Web Proxy filtering and scanning activity. For more information about the access log, see Access Log File, page 24-19.

• **Traffic Monitor log.** Records all L4 Traffic Monitor activity. For more information about the traffic monitor log, see Traffic Monitor Log, page 24-53.

The appliance also creates other log file types, such as the system log file. You might want to read other log files to troubleshoot appliance errors. For a list of each type, see Log File Types, page 24-2.

The appliance provides several options for customizing the type of information recorded in the access log. For more information, see Custom Formatting in Access Logs and W3C Logs, page 24-39.

### Log File Types

The log file type indicates what information is recorded in the generated log, such as web traffic or system data. By default, the Web Security appliance has log subscriptions for most log file types already created. However, there are some log file types that specific to troubleshooting the Web Proxy. Those logs are not created by default. For more information on those log file types, see Web Proxy Logging, page 24-8.

Table 24-1 lists the Web Security appliance log file types created by default.

<table>
<thead>
<tr>
<th>Log File Type</th>
<th>Description</th>
<th>Supports Systlog Push?</th>
<th>Enabled by Default?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control Engine Logs</td>
<td>Records messages related to the Web Proxy ACL (access control list) evaluation engine.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Access Logs</td>
<td>Records Web Proxy client history.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication Framework Logs</td>
<td>Records authentication history and messages.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>AVC Engine Framework Logs</td>
<td>Records messages related to communication between the Web Proxy and the AVC engine.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>AVC Engine Logs</td>
<td>Records debug messages from the AVC engine.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
# Table 24-1 Default Log File Types (continued)

<table>
<thead>
<tr>
<th>Log File Type</th>
<th>Description</th>
<th>Supports Syslog Push?</th>
<th>Enabled by Default?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI Audit Logs</td>
<td>Records a historical audit of command line interface activity.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configuration Logs</td>
<td>Records messages related to the Web Proxy configuration management system.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Connection Management Logs</td>
<td>Records messages related to the Web Proxy connection management system.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Data Security Logs</td>
<td>Records client history for upload requests that are evaluated by the IronPort Data Security Filters.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>For more information on the data security log, see Logging, page 12-27.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security Module Logs</td>
<td>Records messages related to the IronPort Data Security Filters.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>DCA Engine Logs</td>
<td>Records messages related to communication between the Web Proxy and the Cisco IronPort Web Usage Controls Dynamic Content Analysis engine.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>DCA Engine Logs</td>
<td>Records messages related to the Cisco IronPort Web Usage Controls Dynamic Content Analysis engine.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Default Proxy Logs</td>
<td>Records errors related to the Web Proxy.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information about Web Proxy logging, see Web Proxy Logging, page 24-8.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Manager Logs</td>
<td>Records Web Proxy messages related to writing to the cache on disk.</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table 24-1 Default Log File Types (continued)

<table>
<thead>
<tr>
<th>Log File Type</th>
<th>Description</th>
<th>Supports Syslog Push?</th>
<th>Enabled by Default?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External Authentication Logs</strong></td>
<td>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. For more information on external authentication, see Using External Authentication, page 26-17.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Feedback Logs</td>
<td>Records the web users reporting misclassified pages.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FTP Proxy Logs</td>
<td>Records error and warning messages related to the FTP Proxy.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>FTP Server Logs</td>
<td>Records all files uploaded to and downloaded from the Web Security appliance using FTP.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GUI Logs (Graphical User Interface)</td>
<td>Records history of page refreshes in the web interface.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTPS Logs</td>
<td>Records Web Proxy messages specific to the HTTPS Proxy (when the HTTPS Proxy is enabled).</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>License Module Logs</td>
<td>Records messages related to the Web Proxy’s license and feature key handling system.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Logging Framework Logs</td>
<td>Records messages related to the Web Proxy’s logging system.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Logging Logs</td>
<td>Records errors related to log management.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>McAfee Integration Framework Logs</td>
<td>Records messages related to communication between the Web Proxy and the McAfee scanning engine.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>McAfee Logs</td>
<td>Records the status of anti-malware scanning activity from the McAfee scanning engine.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 24-1  Default Log File Types (continued)

<table>
<thead>
<tr>
<th>Log File Type</th>
<th>Description</th>
<th>Supports Syslog Push?</th>
<th>Enabled by Default?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Manager Logs</td>
<td>Records Web Proxy messages related to managing all memory including the in-memory cache for the Web Proxy process.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Miscellaneous Proxy Modules Logs</td>
<td>Records Web Proxy messages that are mostly used by developers or customer support.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Mobile User Security Daemon Logs (Secure Mobility)</td>
<td>Records the interaction between the Web Security appliance and the AnyConnect client, including the status check.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NTP Logs (Network Time Protocol)</td>
<td>Records changes to the system time made by the Network Time Protocol.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PAC File Hosting Daemon Logs</td>
<td>Records proxy auto-config (PAC) file usage by clients.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Proxy Bypass Logs</td>
<td>Records transactions that bypass the Web Proxy.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Reporting Logs</td>
<td>Records a history of report generation.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Reporting Query Logs</td>
<td>Records errors related to report generation.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| Request Debug Logs            | Records very detailed debug information on a specific HTTP transaction from all Web Proxy module log types. You might want to create this log subscription to troubleshoot a proxy issue with a particular transaction without creating all other proxy log subscriptions.  
**Note:** You can create this log subscription in the CLI only. | No                    | No                  |
| SaaS Auth Logs                | Records messages related to the SaaS Access Control feature.                                                                                                                                                     | Yes                   | Yes                 |
### Table 24-1 Default Log File Types (continued)

<table>
<thead>
<tr>
<th>Log File Type</th>
<th>Description</th>
<th>Supports Syslog Push?</th>
<th>Enabled by Default?</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHD Logs (System Health Daemon)</td>
<td>Records a history of the health of system services and a history of unexpected daemon restarts.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMP Logs</td>
<td>Records debug messages related to the SNMP network management engine.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMP Module Logs</td>
<td>Records Web Proxy messages related to interacting with the SNMP monitoring system.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Sophos Integration Framework Logs</td>
<td>Records messages related to communication between the Web Proxy and the Sophos scanning engine.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Sophos Logs</td>
<td>Records the status of anti-malware scanning activity from the Sophos scanning engine.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Status Logs</td>
<td>Records information related to the system, such as feature key downloads.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>System Logs</td>
<td>Records DNS, error, and commit activity.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Traffic Monitor Error Logs</td>
<td>Records L4TM interface and capture errors.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Traffic Monitor Logs</td>
<td>Records sites added to the L4TM block and allow lists.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>UDS Logs (User Discovery Service)</td>
<td>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 Solution as well as integrating with the Novell eDirectory server for transparent user identification. For more information, see Achieving Secure Mobility Overview, page 13-1 and Identifying Users Transparently, page 7-16.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Updater Logs</td>
<td>Records a history of WBRS and other updates.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Logging Overview

**W3C Logs**
Records Web Proxy client history in a W3C compliant format.
For more information, see [W3C Compliant Access Logs](#), page 24-36.

**WBNP Logs**
(ComposerBase Network Participation)
Records a history of SenderBase network participation uploads to the SenderBase network.

**WBRS Framework Logs**
(Web Reputation Score)
Records messages related to communication between the Web Proxy and the Web Reputation Filters.

**WCCP Module Logs**
Records Web Proxy messages related to implementing WCCP.

**Webcat Integration Framework Logs**
Records messages related to communication between the Web Proxy and the configured URL filtering engine, either IronPort URL Filters or Cisco IronPort Web Usage Controls.

**Web categorization Logs**
Records the status of the IronPort URL Filters service, such as whether or not the service is running.

**Webroot Integration Framework Logs**
Records messages related to communication between the Web Proxy and the Webroot scanning engine.

**Webroot Logs**
Records the status of anti-malware scanning activity from the Webroot scanning engine.

**Welcome Page Acknowledgement Logs**
Records a history of web clients who click the Accept button on the end-user acknowledgement page.

---

### Table 24-1 Default Log File Types (continued)

<table>
<thead>
<tr>
<th>Log File Type</th>
<th>Description</th>
<th>Supports Syslog Push?</th>
<th>Enabled by Default?</th>
</tr>
</thead>
<tbody>
<tr>
<td>W3C Logs</td>
<td>Records Web Proxy client history in a W3C compliant format. For more information, see <a href="#">W3C Compliant Access Logs</a>, page 24-36.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>WBNP Logs</td>
<td>Records a history of SenderBase network participation uploads to the SenderBase network.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WBRS Framework Logs (Web Reputation Score)</td>
<td>Records messages related to communication between the Web Proxy and the Web Reputation Filters.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>WCCP Module Logs</td>
<td>Records Web Proxy messages related to implementing WCCP.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Webcat Integration Framework Logs</td>
<td>Records messages related to communication between the Web Proxy and the configured URL filtering engine, either IronPort URL Filters or Cisco IronPort Web Usage Controls.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Web categorization Logs</td>
<td>Records the status of the IronPort URL Filters service, such as whether or not the service is running.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Webroot Integration Framework Logs</td>
<td>Records messages related to communication between the Web Proxy and the Webroot scanning engine.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Webroot Logs</td>
<td>Records the status of anti-malware scanning activity from the Webroot scanning engine.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Welcome Page Acknowledgement Logs</td>
<td>Records a history of web clients who click the Accept button on the end-user acknowledgement page.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Web Proxy Logging

By default, the Web Security appliance has one log subscription created for Web Proxy logging messages, the “Default Proxy Logs.” The Web Proxy information stored in this log covers all aspects, or modules, of the Web Proxy. 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.

If a user or administrator encounters an issue with the Web Proxy behavior, read the Default Proxy Logs first. If you see a log entry that you suspect might be the symptom of an issue, then you can create a log subscription for the relevant specific Web Proxy module. Then read that proxy log to help troubleshoot the problem.

You can create log subscriptions of these proxy module logs in web interface or in the CLI. However, you can only create the Request Debug Logs in the CLI.

The following list includes all Web Proxy module log types:

- Access Control Engine Logs
- AVC Engine Framework Logs
- Configuration Logs
- Connection Management Logs
- Data Security Module Logs
- DCA Engine Framework Logs
- Disk Manager Logs
- FTP Proxy Logs
- HTTPS Logs
- License Module Logs
- Logging Framework Logs
- McAfee Integration Framework Logs
- Memory Manager Logs
- Miscellaneous Proxy Modules Logs
- Request Debug Logs
- SNMP Module Logs
Working with Log Subscriptions

A log subscription is an appliance configuration that specifies the type of log file to create and other factors, such as the log file name and method of retrieving the log file. Use the System Administration > Log Subscriptions page to configure log file subscriptions.

Figure 24-1 shows the Log Subscriptions page where you work with log subscriptions.
Figure 24-1 Log File Subscriptions

By default, the appliance is configured with one log subscription for most log types. You can add, edit, or delete log subscriptions. You can retrieve log files from the appliance using SCP, FTP, or Syslog. You can create multiple log subscriptions for each type of log file.

The appliance includes more options when configuring the access log:

- **Include additional information in each log entry.** For more information about customizing the access log, see Custom Formatting in Access Logs and W3C Logs, page 24-39.
• **Choose the format of the information.** You can choose among the following format options:
  – Apache
  – Squid
  – Squid Details
• **Exclude entries based on HTTP status codes.** You can configure the access log to not include transactions based on particular HTTP status codes to filter out certain transactions. For example, you might want to filter out authentication failure requests that have codes of 407 or 401.

**Log File Name 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.

**Rolling Over Log Subscriptions**

AsyncOS rolls over log subscriptions based on settings you make in each log subscription. Rolling over a log subscription is an AsyncOS process that accomplishes the following tasks:
• Creates a new log file with the timestamp of the rollover and designates the file as current with the letter “c” extension.
• Renames the current log file to have a letter “s” extension signifying saved.
AsyncOS rolls over log subscriptions in the following ways:

- **Manually.** The appliance administrator can manually roll over log subscriptions on demand from either the web interface or the CLI. Use the Rollover Now button on the System Administration > Log Subscriptions page, or the rollovernow CLI command. The rollovernow command allows you to roll over all log files at once or select a specific log file from a list.

- **Automatically.** AsyncOS rolls over log subscriptions based on the first user-specified limit reached: maximum file size or maximum time. Log subscriptions based on the FTP poll retrieval method create files and store them in the FTP directory on the appliance until they are retrieved from a remote FTP client, or until the system needs to create more space for log files.

To roll over a log subscription in the web interface:

**Step 1** Navigate to the System Administration > Log Subscriptions page.

**Step 2** Click the check box under the Rollover column for each log subscription you want to roll over.

**Step 3** Click Rollover Now.

## Working with Compressed Log Files

To save disk space on the Web Security appliance, log subscriptions can compress rolled over log files before storing them on the disk. Only rolled over logs are compressed. The current active log file is not compressed.

Each log subscription has its own log compression setting, so you can choose which log subscriptions to compress. AsyncOS compresses log files using the gzip compression format.
Viewing the Most Recent Log Files

You can view the most recent version of a log file from the following locations:

- **Web interface.** On the System Administration > Log Subscriptions page, click the name of the log subscription in the Log Files column of the list of log subscriptions. When you click the link to the log subscription, AsyncOS prompts you to enter your password. Then it lists the available log files for that subscription. Click one of the log files to view it in your browser or to save it to disk.

- **Command line interface.** Use the `tail` CLI command. AsyncOS displays the configured log subscriptions and prompts you to select the log subscription to view. Use Ctrl+C to exit from the `tail` command at any time.

**Note**
If a log subscription is compressed, you must download it before you can decompress and open it.

Configuring Host Keys

Use the `logconfig -> hostkeyconfig` subcommand to manage host keys for use with SSH when pushing log files to other servers from the Web Security appliance. SSH servers must have a pair of host keys, one private and one public. The private host key resides on the SSH server and cannot be read by remote machines. The public host key is distributed to any client machine that needs to interact with the SSH server.

The `hostkeyconfig` subcommand performs the following functions:

**Table 24-2 Managing Host Keys—List of Subcommands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Add a new key.</td>
</tr>
<tr>
<td>Scan</td>
<td>Automatically download a host key.</td>
</tr>
<tr>
<td>Host</td>
<td>Display system host keys. This is the value to place in the remote system’s <code>known_hosts</code> file.</td>
</tr>
</tbody>
</table>
Adding and Editing Log Subscriptions

To add or edit a log subscription:

**Step 1** Navigate to the System Administration > Log Subscriptions page.

**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.

The New Log Subscription page or Edit Log Subscription page appears.

**Step 3** Select the type of log to associate with this subscription from the Log Type field.

**Step 4** Enter a name for the log subscription in the Log Name field.

The appliance uses this name for the directory on the appliance that will contain the log file.

**Step 5** If you are creating an access log, configure the following options:

<table>
<thead>
<tr>
<th>Access Log Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Style</td>
<td>Choose the log format to use, either Squid, Apache, or Squid Details.</td>
</tr>
<tr>
<td>Custom Fields</td>
<td>Optionally, enter the other type of information to include in each access log entry. For more information, see Custom Formatting in Access Logs and W3C Logs, page 24-39.</td>
</tr>
</tbody>
</table>
Step 6  If you are creating a W3C access log, configure the following options:

<table>
<thead>
<tr>
<th>Access Log Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Fields</td>
<td>Choose the fields you want to include in the W3C access log. Select a field in the Available Fields list, or type a field in the Custom Field box, and click Add. 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. For more information, see W3C Compliant Access Logs, page 24-36.</td>
</tr>
</tbody>
</table>

Note  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.

Step 7  Enter a name for the log file in the File Name field.

Step 8  Enter the maximum file size in bytes the log file can be in the Maximum File Size field. After the number, enter “G” to specify Gigabytes, “M” for Megabytes, or “K” for Kilobytes.

Step 9  Choose whether or not to compress log files after they have been rolled over using the Log Compression field. For more information, see Working with Compressed Log Files, page 24-12.

Step 10 If you are creating an access log or a W3C access log, you can optionally choose to exclude certain transactions based on particular HTTP status codes in the Log Exclusions field. For example, you might want to filter out authentication failure requests that have codes of 407 or 401.

Step 11 Choose the amount of detail to include in the log file in the Log Level field.
The Log Level field does not appear for access and W3C access logs subscriptions.

More detailed settings create larger log files and have a greater impact on system performance. More detailed settings include all the messages contained in less detailed settings, plus additional messages. As the level of detail increases, system performance decreases.

Table 24-3 describes the levels of detail you can choose in the Log Level field.

**Table 24-3  Logging Levels**

<table>
<thead>
<tr>
<th>Log Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>This is the least detailed setting. This level only includes errors. Using this setting will not allow you to monitor performance and other important activities. However, the log files will not reach their maximum size as quickly. This log level is equivalent to the syslog level “Alert.”</td>
</tr>
<tr>
<td>Warning</td>
<td>This level includes all errors and warnings created by the system. Using this setting will not allow you to monitor performance and other important activities. This log level is equivalent to the syslog level “Warning.”</td>
</tr>
<tr>
<td>Information</td>
<td>This level includes the detailed system operations. This is the default. This log level is equivalent to the syslog level “Info.”</td>
</tr>
<tr>
<td>Debug</td>
<td>This level 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.”</td>
</tr>
<tr>
<td>Trace</td>
<td>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.”</td>
</tr>
</tbody>
</table>

**Step 12** Choose how to retrieve the log file from the appliance in the Retrieval Method field.
Table 24-4 describes the different ways you can retrieve log files:

**Table 24-4  Log Transfer Protocols**

<table>
<thead>
<tr>
<th>Retrieval Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP on Appliance (FTP Poll)</td>
<td>This method requires a remote FTP client accessing the appliance to retrieve log files using an admin or operator user’s username and password. 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. This is the default.</td>
</tr>
</tbody>
</table>
| FTP on Remote Server (FTP Push) | This method periodically pushes log files to an FTP server on a remote computer. When you choose this method, you must enter the following information:  
  • Maximum time between file transfers  
  • FTP server hostname  
  • Directory on FTP server to store the log file  
  • Username and password of a user that has permission to connect to the FTP server  
*Note:* AsyncOS for Web only supports passive mode for remote FTP servers. It cannot push log files to an FTP server in active mode. |
### Table 24-4 Log Transfer Protocols (continued)

<table>
<thead>
<tr>
<th>Retrieval Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| SCP on Remote Server (SCP Push)   | This method periodically pushes log files using the secure copy protocol to an SCP server on a remote computer. This method requires an SSH SCP server on a remote computer using the SSH1 or 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. When you choose this method, you must enter the following information:  
  - Maximum time between file transfers  
  - Protocol to use for transmission, either SSH1 or SSH2  
  - SCP server hostname  
  - Directory on SCP server to store the log file  
  - Username of a user that has permission to connect to the SCP server  
  Choose whether or not to enable host key checking.                                                                 |
| Syslog Push                       | This method sends log messages to a remote syslog server.  
  This method conforms to RFC 3164. The appliance uses port 514.  
  When you choose this method, you must enter the following information:  
  - Syslog server hostname  
  - Protocol to use for transmission, either UDP or TCP  
  - Facility to use with the log  
  You can only choose syslog for text-based logs.                                                                 |

**Step 13** Submit and commit your changes.

**Step 14** If you chose SCP as the retrieval method, the appliance displays an SSH key to you must place on the SCP server host.
Deleting a Log Subscription

To delete a log subscription:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Navigate to the System Administration &gt; Log Subscriptions page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the icon under the Delete column for the log subscription you want to delete.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Submit and commit your changes.</td>
</tr>
</tbody>
</table>

Access Log File

The access log file 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. You can view the access log file from the System Administration > Log Subscriptions page.

**Note**
The W3C access log also records all Web Proxy filtering and scanning activity, but in a format that is W3C compliant. For more information, see W3C Compliant Access Logs, page 24-36.

The following text is an example access log file entry for a single transaction:

```
```

<table>
<thead>
<tr>
<th>Field Value</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1278096903.150</td>
<td>Timestamp since UNIX epoch.</td>
</tr>
<tr>
<td>97</td>
<td>Elapsed time (latency) in milliseconds.</td>
</tr>
</tbody>
</table>
### Table 24-5 Access Log File Entry (continued)

<table>
<thead>
<tr>
<th>Field Value</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.xx.xx.xx</td>
<td>Client IP address. <strong>Note:</strong> You can choose to mask the IP address in the access logs using the <code>advancedproxyconfig &gt; authentication</code> CLI command.</td>
</tr>
<tr>
<td>TCP_MISS/</td>
<td>Transaction result code. For more information, see Transaction Result Codes, page 24-23.</td>
</tr>
<tr>
<td>200</td>
<td>HTTP response code.</td>
</tr>
<tr>
<td>8187</td>
<td>Response size (headers + body).</td>
</tr>
<tr>
<td>GET <a href="http://my.site.com/">http://my.site.com/</a></td>
<td>First line of the request. <strong>Note:</strong> 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. The following characters are URL encoded: <code>&amp; # % + , ; = @ ^ { } [ ]</code></td>
</tr>
<tr>
<td>-</td>
<td>Authenticated username. <strong>Note:</strong> You can choose to mask the username in the access logs using the <code>advancedproxyconfig &gt; authentication</code> CLI command.</td>
</tr>
</tbody>
</table>
## Chapter 24 Logging

### Access Log File

#### Table 24-5 Access Log File Entry (continued)

<table>
<thead>
<tr>
<th>Field Value</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIRECT/my.site.com</td>
<td>Code that describes which server was contacted for the retrieving the request content.</td>
</tr>
<tr>
<td></td>
<td>Most common values include:</td>
</tr>
<tr>
<td></td>
<td>- <strong>NONE</strong>. The Web Proxy had the content, so it did not contact any other server to retrieve the content.</td>
</tr>
<tr>
<td></td>
<td>- <strong>DIRECT</strong>. The Web Proxy went to the server named in the request to get the content.</td>
</tr>
<tr>
<td></td>
<td>- <strong>DEFAULT_PARENT</strong>. The Web Proxy went to its primary parent proxy or an external DLP server to get the content.</td>
</tr>
<tr>
<td>text/plain</td>
<td>Response body MIME type.</td>
</tr>
<tr>
<td>DEFAULT_CASE_11</td>
<td>ACL decision tag.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The end of the ACL decision tag includes a dynamically generated number that the Web Proxy uses internally. You can ignore this number.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">ACL Decision Tags, page 24-24</a>.</td>
</tr>
<tr>
<td>AccessOrDecryptionPolicy</td>
<td>Access Policy or Decryption Policy group name. When the transaction matches the global Access Policy or global Decryption Policy, this value is “DefaultGroup.”</td>
</tr>
<tr>
<td></td>
<td>Any space in the policy group name is replaced with an underscore ( _ ).</td>
</tr>
<tr>
<td>Identity</td>
<td>Identity policy group name.</td>
</tr>
<tr>
<td></td>
<td>Any space in the policy group name is replaced with an underscore ( _ ).</td>
</tr>
<tr>
<td>OutboundMalwareScanning</td>
<td>Outbound Malware Scanning Policy group name.</td>
</tr>
<tr>
<td>Policy</td>
<td>Any space in the policy group name is replaced with an underscore ( _ ).</td>
</tr>
</tbody>
</table>
### Table 24-5 Access Log File Entry (continued)

<table>
<thead>
<tr>
<th>Field Value</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DataSecurityPolicy</strong></td>
<td>IronPort Data Security Policy group name. When the transaction matches the global IronPort Data Security Policy, this value is “DefaultGroup.” This policy group name only appears when 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 (_).</td>
</tr>
<tr>
<td><strong>ExternalDLPPolicy</strong></td>
<td>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 (_).</td>
</tr>
<tr>
<td><strong>RoutingPolicy</strong></td>
<td>Routing Policy group name as ProxyGroupName/ProxyServerName. 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 (_).</td>
</tr>
</tbody>
</table>

```
IW_comp,-,"Skipped","-",-,-,"-","-",-,-,"-",-,-,-,"-",-,-,-,I
W_comp,-,"-","-",-,-,Unknown,"Unknown","-","-",198
.34,0,-,"-","-"
```

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 Understanding Scanning Verdict Information, page 24-30.

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.

<table>
<thead>
<tr>
<th>Result Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP_HIT</td>
<td>The object requested was fetched from the disk cache.</td>
</tr>
<tr>
<td>TCP_IMS_HIT</td>
<td>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.</td>
</tr>
<tr>
<td>TCP_MEM_HIT</td>
<td>The object requested was fetched from the memory cache.</td>
</tr>
<tr>
<td>TCP_MISS</td>
<td>The object was not found in the cache, so it was fetched from the origin server.</td>
</tr>
<tr>
<td>TCP_REFRESH_HIT</td>
<td>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.</td>
</tr>
<tr>
<td>TCP_CLIENT_REFRESH_MISS</td>
<td>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.</td>
</tr>
<tr>
<td>TCP_DENIED</td>
<td>The client request was denied due to Access Policies.</td>
</tr>
<tr>
<td>NONE</td>
<td>There was an error in the transaction. For example, a DNS failure or gateway timeout.</td>
</tr>
</tbody>
</table>
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.

Table 24-7 describes the ACL decision tag values.

<table>
<thead>
<tr>
<th>ACL Decision Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALLOW_ADMIN</td>
<td>The Web Proxy allowed the transaction based on Applications settings for the Access Policy group.</td>
</tr>
<tr>
<td>ALLOW_ADMIN_ERROR_PAGE</td>
<td>The Web Proxy allowed the transaction to an IronPort notification page and to any logo used on that page.</td>
</tr>
<tr>
<td>ALLOW_CUSTOMCAT</td>
<td>The Web Proxy allowed the transaction based on custom URL category filtering settings for the Access Policy group.</td>
</tr>
<tr>
<td>ALLOW_WBRS</td>
<td>The Web Proxy allowed the transaction based on the Web Reputation filter settings for the Access Policy group.</td>
</tr>
<tr>
<td>BLOCK_ADMIN</td>
<td>The Web Proxy blocked the transaction based on Applications or Objects settings for the Access Policy group.</td>
</tr>
<tr>
<td>BLOCK_ADMIN_CONNECT</td>
<td>The Web Proxy blocked the transaction based on the TCP port of the destination as defined in the HTTP CONNECT Ports setting for the Access Policy group.</td>
</tr>
</tbody>
</table>
### Table 24-7  ACL Decision Tag Values (continued)

<table>
<thead>
<tr>
<th>ACL Decision Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLOCK_ADMIN_CUSTOM_USER_AGENT</td>
<td>The Web Proxy blocked the transaction based on the user agent as defined in the Block Custom User Agents setting for the Access Policy group.</td>
</tr>
<tr>
<td>BLOCK_ADMIN_DLP</td>
<td>The Web Proxy blocked the transaction based on the MIME type of the request body content as defined in the Data Security Policy group.</td>
</tr>
<tr>
<td>BLOCK_ADMIN_FILE_TYPE</td>
<td>The Web Proxy blocked the transaction based on the file type as defined in the Access Policy group.</td>
</tr>
<tr>
<td>BLOCK_ADMIN_PROTOCOL</td>
<td>The Web Proxy blocked the transaction based on the protocol as defined in the Block Protocols setting for the Access Policy group.</td>
</tr>
<tr>
<td>BLOCK_ADMIN_SIZE</td>
<td>The Web Proxy blocked the transaction based on the size of the response as defined in the Object Size settings for the Access Policy group.</td>
</tr>
<tr>
<td>BLOCK_ADMIN_SIZE_DLP</td>
<td>The Web Proxy blocked the transaction based on the size of the request body content as defined in the Data Security Policy group.</td>
</tr>
<tr>
<td>BLOCK_AMW_REQ</td>
<td>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.</td>
</tr>
<tr>
<td>BLOCK_AMW_RESP</td>
<td>The Web Proxy blocked the response based on the Anti-Malware settings for the Access Policy group.</td>
</tr>
<tr>
<td>ACL Decision Tag</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BLOCK_AMW_RESP_URL</td>
<td>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.</td>
</tr>
<tr>
<td>BLOCK_AVC</td>
<td>The Web Proxy blocked the transaction based on the configured Application settings for the Access Policy group.</td>
</tr>
<tr>
<td>BLOCKCONTENT_UNSAFE</td>
<td>The Web Proxy blocked the transaction based on the site content ratings settings for the Access Policy group. The client request was for adult content and the policy is configured to block adult content.</td>
</tr>
<tr>
<td>BLOCK_CONTINUECONTENT_UNSAFE</td>
<td>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.</td>
</tr>
<tr>
<td>BLOCK_CONTINUECUSTOMCAT</td>
<td>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.”</td>
</tr>
<tr>
<td>BLOCK_CONTINUEWEBCAT</td>
<td>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.”</td>
</tr>
<tr>
<td>BLOCKCUSTOMCAT</td>
<td>The Web Proxy blocked the transaction based on custom URL category filtering settings for the Access Policy group.</td>
</tr>
<tr>
<td>BLOCKICAP</td>
<td>The Web Proxy blocked the request based on the verdict of the external DLP system as defined in the External DLP Policy group.</td>
</tr>
</tbody>
</table>
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.

The Web Proxy blocked the transaction based on the Suspect User Agent setting for the Access Policy group.

The Web Proxy blocked the transaction based on the safe search settings for the Access Policy group. The transaction was for an unsupported search engine, and the policy is configured to block unsupported search engines.

The Web Proxy blocked the transaction based on the Web Reputation filter settings for the Access Policy group.

The Web Proxy blocked the upload request based on the Web Reputation filter settings for the Data Security Policy group.

The Web Proxy blocked the transaction based on URL category filtering settings for the Access Policy group.

The Web Proxy blocked the upload request based on the URL category filtering settings for the Data Security Policy group.

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.

The Web Proxy monitored the server response based on the Anti-Malware settings for the Access Policy group.

<table>
<thead>
<tr>
<th>ACL Decision Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLOCK_SEARCHUnsafe</td>
<td>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.</td>
</tr>
<tr>
<td>BLOCK_SUSPECT_USER_AGENT</td>
<td>The Web Proxy blocked the transaction based on the Suspect User Agent setting for the Access Policy group.</td>
</tr>
<tr>
<td>BLOCK_UNSUPPORTED_SEARCH_APP</td>
<td>The Web Proxy blocked the transaction based on the safe search settings for the Access Policy group. The transaction was for an unsupported search engine, and the policy is configured to block unsupported search engines.</td>
</tr>
<tr>
<td>BLOCK_WBRS</td>
<td>The Web Proxy blocked the transaction based on the Web Reputation filter settings for the Access Policy group.</td>
</tr>
<tr>
<td>BLOCK_WBRS_DLP</td>
<td>The Web Proxy blocked the upload request based on the Web Reputation filter settings for the Data Security Policy group.</td>
</tr>
<tr>
<td>BLOCK_WEBCAT</td>
<td>The Web Proxy blocked the transaction based on URL category filtering settings for the Access Policy group.</td>
</tr>
<tr>
<td>BLOCK_WEBCAT_DLP</td>
<td>The Web Proxy blocked the upload request based on the URL category filtering settings for the Data Security Policy group.</td>
</tr>
<tr>
<td>DEFAULT_CASE</td>
<td>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.</td>
</tr>
<tr>
<td>MONITOR_AMW_RESP</td>
<td>The Web Proxy monitored the server response based on the Anti-Malware settings for the Access Policy group.</td>
</tr>
<tr>
<td>ACL Decision Tag</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MONITOR_AMW_RESP_URL</td>
<td>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.</td>
</tr>
<tr>
<td>MONITOR_AVC</td>
<td>The Web Proxy monitored the transaction based on the Application settings for the Access Policy group.</td>
</tr>
<tr>
<td>MONITOR_CONTINUE_CONTENT_UNSFAFE</td>
<td>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.</td>
</tr>
<tr>
<td>MONITOR_CONTINUE_CUSTOMCAT</td>
<td>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.</td>
</tr>
<tr>
<td>MONITOR_CONTINUE_WEBCAT</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 24-7 ACL Decision Tag Values (continued)

<table>
<thead>
<tr>
<th>ACL Decision Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MONITOR_DLP</td>
<td>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.</td>
</tr>
<tr>
<td>MONITOR_SUSPECT_USER_AGENT</td>
<td>The Web Proxy monitored the transaction based on the Suspect User Agent setting for the Access Policy group.</td>
</tr>
<tr>
<td>MONITOR_WEBRS</td>
<td>The Web Proxy monitored the transaction based on the Web Reputation filter settings for the Access Policy group.</td>
</tr>
<tr>
<td>NO_AUTHORIZATION</td>
<td>The Web Proxy did not allow the user access to the SaaS application because the user was already authenticated against an authentication realm, but not against any authentication realm configured in the SaaS Application Authentication Policy.</td>
</tr>
<tr>
<td>NO_PASSWORD</td>
<td>The user failed authentication.</td>
</tr>
<tr>
<td>REDIRECT_CUSTOMCAT</td>
<td>The Web Proxy redirected the transaction to a different URL based on a custom URL category in the Access Policy group configured to “Redirect.”</td>
</tr>
<tr>
<td>SAAS_AUTH</td>
<td>The Web Proxy allowed the user access to the SaaS application because the user was authenticated transparently against the authentication realm configured in the SaaS Application Authentication Policy.</td>
</tr>
<tr>
<td>OTHER</td>
<td>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.</td>
</tr>
</tbody>
</table>
Understanding Scanning Verdict Information

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:

```plaintext
IW_infr,ns,"Trojan Phisher","Trojan-Phisher-Gamec",0,354385,12559,"-","-","-","-","-","-","-","-",IW_infr,,-"Trojan Phisher",-","Unknown","Unknown","-",489.73,0,[Local],"-","
```

Table 24-8 describes the different fields in the scanning verdict information section of each access log file entry.

<table>
<thead>
<tr>
<th>Field Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IW_infr</td>
<td>The URL category assigned to the transaction, abbreviated. This field shows “nc” when no category is assigned. For a list of URL category abbreviations, see URL Category Descriptions, page 16-32.</td>
</tr>
<tr>
<td>ns</td>
<td>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.</td>
</tr>
<tr>
<td>Trojan Phisher</td>
<td>The malware scanning verdict Webroot passed to the DVS engine. Applies to responses detected by Webroot only. For more information, see Malware Scanning Verdict Values, page 24-52.</td>
</tr>
<tr>
<td>Trojan-Phisher-Gamec</td>
<td>Name of the spyware that is associated with the object. Applies to responses detected by Webroot only.</td>
</tr>
</tbody>
</table>

For an example of a whole access log file entry, see Access Log File, page 24-19.
Table 24-8 Access Log File Entry — Scanning Verdict Information

<table>
<thead>
<tr>
<th>Field Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The Webroot specific value associated with the Threat Risk Threshold (TRT) value that determines the probability that malware exists. Applies to responses detected by Webroot only.</td>
</tr>
<tr>
<td>354385</td>
<td>A value that Webroot uses as a threat identifier. IronPort Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Webroot only.</td>
</tr>
<tr>
<td>12559</td>
<td>A value that Webroot uses as a trace identifier. IronPort Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Webroot only.</td>
</tr>
<tr>
<td>-</td>
<td>The malware scanning verdict McAfee passed to the DVS engine. Applies to responses detected by McAfee only. For more information, see Malware Scanning Verdict Values, page 24-52.</td>
</tr>
<tr>
<td>-</td>
<td>The name of the file McAfee scanned. Applies to responses detected by McAfee only.</td>
</tr>
<tr>
<td>-</td>
<td>A value that McAfee uses as a scan error. IronPort Customer Support may use this value when troubleshooting an issue. Applies to responses detected by McAfee only.</td>
</tr>
<tr>
<td>-</td>
<td>A value that McAfee uses as a detection type. IronPort Customer Support may use this value when troubleshooting an issue. Applies to responses detected by McAfee only.</td>
</tr>
<tr>
<td>-</td>
<td>A value that McAfee uses as a virus type. IronPort Customer Support may use this value when troubleshooting an issue. Applies to responses detected by McAfee only.</td>
</tr>
<tr>
<td>-</td>
<td>The name of the virus that McAfee scanned. Applies to responses detected by McAfee only.</td>
</tr>
<tr>
<td>-</td>
<td>The malware scanning verdict Sophos passed to the DVS engine. Applies to responses detected by Sophos only. For more information, see Malware Scanning Verdict Values, page 24-52.</td>
</tr>
</tbody>
</table>
Table 24-8  Access Log File Entry — Scanning Verdict Information

<table>
<thead>
<tr>
<th>Field Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>A value that Sophos uses as a scan return code. IronPort Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Sophos only.</td>
</tr>
<tr>
<td>-</td>
<td>The file location where Sophos found the objectionable content. For non-archive files, this value is the file name itself. For archive file, it is the object in the archive, such as archive.zip/virus.exe. Applies to responses detected by Sophos only.</td>
</tr>
<tr>
<td>-</td>
<td>A value that Sophos uses as the threat name. IronPort Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Sophos only.</td>
</tr>
</tbody>
</table>
| -           | The IronPort Data Security scan verdict based on the action in the Content column of the IronPort Data Security Policy. The following list describes the possible values for this field:  
  - 0. Allow  
  - 1. Block  
  - (hyphen). No scanning was initiated by the IronPort Data Security Filters. This value appears when the IronPort Data Security Filters is disabled or when the URL category action is set to Allow. |
| -           | The External DLP scan verdict based on the result given in the ICAP response. The following list describes the possible values for this field:  
  - 0. Allow  
  - 1. Block  
  - (hyphen). No scanning was initiated by the external DLP server. This value appears when External DLP scanning is disabled or when the content was not scanned due to an exempt URL category on the External DLP Policies > Destinations page. |
### Table 24-8  Access Log File Entry — Scanning Verdict Information

<table>
<thead>
<tr>
<th>Field Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IW_infr</td>
<td>The URL category verdict determined during request-side scanning, abbreviated. Applies to both IronPort URL Filters and Cisco IronPort Web Usage Controls URL filtering engines. This field lists a hyphen ( - ) when URL filtering is disabled. For a list of URL category abbreviations, see URL Category Descriptions, page 16-32.</td>
</tr>
<tr>
<td>-</td>
<td>The URL category verdict determined by the Dynamic Content Analysis engine during response-side scanning, abbreviated. Applies to the Cisco IronPort 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 URL Category Descriptions, page 16-32.</td>
</tr>
<tr>
<td>Trojan Phisher</td>
<td>Unified response-side anti-malware scanning verdict independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning.</td>
</tr>
<tr>
<td>-</td>
<td>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.</td>
</tr>
<tr>
<td>Unknown</td>
<td>The application name as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled.</td>
</tr>
<tr>
<td>Unknown</td>
<td>The application type as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled.</td>
</tr>
<tr>
<td>-</td>
<td>The application behavior as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled.</td>
</tr>
<tr>
<td>-</td>
<td>Safe browsing scanning verdict. This value indicates whether or not either the safe search or site content ratings feature was applied to the transaction. For a list of the possible values, see Logging Adult Content Access, page 16-22.</td>
</tr>
<tr>
<td>489.73</td>
<td>The average bandwidth consumed serving the request in Kb per second.</td>
</tr>
</tbody>
</table>
Table 24-8  Access Log File Entry — Scanning Verdict Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>A value that indicates whether or not the request was throttled due to bandwidth limit control settings. “1” indicates the request was throttled, “0” indicates it was not.</td>
</tr>
<tr>
<td>[Local]</td>
<td></td>
<td>The type of user making the request, either “local” or “remote.” Only applies when Mobile User Security is enabled. When it is not enabled, the value is a hyphen (-).</td>
</tr>
<tr>
<td>-</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>-</td>
<td></td>
<td>The threat name assigned to the client request that was blocked or monitored due to an applicable Outbound Malware Scanning Policy. This threat name is independent of which anti-malware scanning engines are enabled.</td>
</tr>
</tbody>
</table>

Web Reputation Filters Example

In the following example, the URL request was allowed because the URL’s Web Reputation score was high enough to qualify to be allowed without being scanned for malware.

```
1278100150.818 1303 172.xx.xx.xx TCP_MISS/200 46578 GET
http://www.cisco.com/- DIRECT/www.cisco.com -
ALLOW_WBRS_11-AccessPolicy-Identity-NONE-NONE-NONE-DefaultGroup
 IW_comp,6.5,",","","","","","","","","",IW_comp,",",",",Unknown",Unknown",",",",",285.97,0,"","" > -
```

In this example, “6.5” is the Web Reputation score. The hyphen “-” values indicate the request was not forwarded to the DVS engine for anti-malware scanning. The ACL decision tag “ALLOW_WBRS” indicates that the request was allowed, and therefore not forwarded for anti-malware scanning, based on this Web Reputation score.
Antimalware Request Example

In the following example, the Webroot scanning engine scanned the URL request and assigned a malware scanning verdict based on the URL request. Webroot is the only scanning engine that scans a URL request. For more information about Webroot scanning, see Webroot Scanning, page 19-7.

1278106367.381 170 172.xx.xx.xx TCP_DENIED/403 1828 GET
http://www.gator.com/ - NONE/- -
BLOCK_AMW_RESP_URL_11-AccessPolicy-Identity-OMSPolicy-NONE-NONE-NONE
<IW_busi,3.4,"Adware","GAIN - Common Components",95,37607,10,"-","-","-","-","-","-","-","-","-","-","-",IW_busi,
-,"Adware","-","Unknown","Unknown","-","-",86.02,0,-,"-","-"> 

In this example, “3.4” is the Web Reputation score, indicating to scan the website for malware. Therefore, the Web Proxy passed the request to the DVS engine for anti-malware scanning.

The “Adware” value is the malware scanning verdict that Webroot passed to the DVS engine. The “BLOCK_AMW_RESP_URL” ACL decision tag shows that Webroot’s request-side checking of the URL produced this verdict. The remainder of the fields show the malware name (“GAIN - Common Components”), threat risk rating (“95”), threat ID (“37607”), and trace ID (“10”) values, which Webroot derived from its evaluation. All of the McAfee and Sophos-related values are empty (“-”) because neither the McAfee or Sophos scanning engine scanned the URL request.

Antimalware Response Example

In the following example, the McAfee scanning engine scanned the server response, assigned a malware scanning verdict based on the server response, and blocked it from the user.

1278097193.276 51 172.xx.xx.xx TCP_DENIED/403 3122 GET
http://badsite.com/malware.exe - DIRECT/badsite.com
application/x-dosexec
BLOCK_AMW_RESP_11-AccessPol-Identity-NONE-NONE-NONE-DefaultGroup
<IW_infr,3.0,"Trojan Phisher","Trojan-Phisher-Gamec",0,354385,12559,
","-","-","-","-","-",IW_infr,","Trojan Phisher","-","Unknown","Unknown","-","-",489.73,0,[Local],"-","-"> 

OL-23207-01
Cisco IronPort AsyncOS 7.1 for Web User Guide
The following list explains the values in this access log entry that show that this transaction was blocked based on the result of the Webroot scanning engine:

- **TCP_DENIED.** The website was denied due to Access Policies.
- **BLOCK_AMW_RESP_11-AccessPol.** This transaction matched the “AccessPol” Access Policy group, and the due to the settings defined in that policy group, the server response was blocked due to detected malware.
- **3.0 in the angled brackets.** The URL received a Web Reputation Score of 3.0, which fell in the score range to scan further.
- **“Trojan Phisher” in the angled brackets.** The malware scanning verdict Webroot passed to the DVS engine.
- **“Trojan-Phisher-Gamec”.** The name of the malware that Webroot scanned.

## W3C Compliant Access Logs

The Web Security appliance provides two different log types for recording Web Proxy transaction information, the access logs and the W3C access logs. The W3C access logs are W3C compliant, and record transaction history in the W3C Extended Log File (ELF) Format.

You can create multiple W3C access log subscriptions and define the data to include in each. You might want to create one W3C access log that includes all information your organization typically needs, and other, specialized W3C access logs that can be used for troubleshooting purposes or special analysis. For example, you might want to create a W3C access log for an HR manager that only needs access to certain information.

Consider the following rules and guidelines when working with W3C access logs:

- You define what data is recorded in each W3C access log subscription.
- The 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.
When defining a W3C access log subscription, you can choose from a list of predefined log fields or enter a custom log field. For more information, see Working with Log Fields in W3C Access Logs, page 24-38.

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.

If you want to copy the log fields included in a W3C access log in their order, use the `logconfig > edit` CLI command. The CLI displays the log fields in order, from which you can copy and then paste them into a separate Web Security appliance web interface.

### 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.

Table 24-9 describes the header fields listed at the beginning of each W3C log file.

<table>
<thead>
<tr>
<th>Header Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The version of the W3C ELF format used.</td>
</tr>
<tr>
<td>Date</td>
<td>The date and time at which the entry was added.</td>
</tr>
<tr>
<td>System</td>
<td>The Web Security appliance that generated the log file in the format “Management_IP - Management_hostname.”</td>
</tr>
<tr>
<td>Software</td>
<td>The Software which generated these logs</td>
</tr>
<tr>
<td>Fields</td>
<td>The fields recorded in the log</td>
</tr>
</tbody>
</table>

For example, a W3C log file might contain the following header information:

```
#Version: 1.0
#Date: 2009-06-15 13:55:20
#System: 10.1.1.1 - wsa.qa
```
Working with Log Fields in W3C Access Logs

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. For more information, see Custom Formatting in Access Logs and W3C Logs, page 24-39.

- **User defined.** You can type a log field that is not included in the predefined list. For more information, see Including HTTP/HTTPS Headers in Log Files, page 24-51.

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.

Table 24-10 on page 38 describes the W3C log fields prefixes.

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c</td>
<td>Client</td>
<td></td>
</tr>
<tr>
<td>s</td>
<td>Server</td>
<td></td>
</tr>
<tr>
<td>cs</td>
<td>Client to server</td>
<td></td>
</tr>
<tr>
<td>sc</td>
<td>Server to client</td>
<td></td>
</tr>
<tr>
<td>x</td>
<td>Application specific identifier.</td>
<td></td>
</tr>
</tbody>
</table>

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.
Custom Formatting in Access Logs and W3C Logs

You can customize access logs and W3C access logs to include many different fields to capture comprehensive information about web traffic within the network. Access logs use format specifiers, and the W3C access logs use W3C log fields. Table 24-11 describes the W3C log fields you can include in the W3C access logs and the custom format specifiers (for the access logs) they correspond with.

Table 24-11: Log Fields in W3C Logs and Format Specifiers in Access Logs

<table>
<thead>
<tr>
<th>W3C Log Field</th>
<th>Format Specifier in Access Logs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>%B</td>
<td>Total bytes used (request size + response size, which is %q + %s)</td>
</tr>
<tr>
<td>c-ip</td>
<td>%a</td>
<td>Client IP Address</td>
</tr>
<tr>
<td>c-port</td>
<td>%F</td>
<td>Client source port</td>
</tr>
<tr>
<td>CMF</td>
<td>%M</td>
<td>Cache miss flags, CMF flags</td>
</tr>
<tr>
<td>cs(Cookie)</td>
<td>%C</td>
<td>Cookie header. This field is written with double-quotes in the access logs.</td>
</tr>
<tr>
<td>cs(Referer)</td>
<td>%&lt;Referrer:</td>
<td>Referrer</td>
</tr>
<tr>
<td>cs(User-Agent)</td>
<td>%u</td>
<td>User agent. This field is written with double-quotes in the access logs.</td>
</tr>
<tr>
<td>cs(X-Forwarded-For)</td>
<td>%f</td>
<td>X-Forwarded-For header</td>
</tr>
<tr>
<td>cs-auth-group</td>
<td>%g</td>
<td>Authorized group names. This field is written with double-quotes in the access logs.</td>
</tr>
</tbody>
</table>
### Table 24-11  Log Fields in W3C Logs and Format Specifiers in Access Logs

<table>
<thead>
<tr>
<th>W3C Log Field</th>
<th>Format Specifier in Access Logs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cs-auth-mechanism</td>
<td>%m</td>
<td>The authentication mechanism used on the transaction. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>BASIC.</strong> The user name was authenticated using the Basic authentication scheme.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>NTLMSSP.</strong> The user name was authenticated using the NTLMSSP authentication scheme.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>SSO_EDIR.</strong> The user name was obtained by matching the client IP address to an authenticated user name in Novell eDirectory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>SSO_ASA.</strong> The user is a remote user and the user name was obtained from a Cisco ASA using the Secure Mobility Solution.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>FORM_AUTH.</strong> The user entered authentication credentials in a form in the web browser when accessing a SaaS application.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>GUEST.</strong> The user failed authentication and instead was granted guest access.</td>
</tr>
<tr>
<td>cs-bytes</td>
<td>%q</td>
<td>Request size (headers + body)</td>
</tr>
<tr>
<td>cs-method</td>
<td>%y</td>
<td>Method</td>
</tr>
<tr>
<td>cs-mime-type</td>
<td>%c</td>
<td>Response body MIME type. This field is written with double-quotes in the access logs.</td>
</tr>
<tr>
<td>N/A</td>
<td>%r</td>
<td>Request first line - request method, URI, HTTP version</td>
</tr>
<tr>
<td>cs-uri</td>
<td>%U</td>
<td>Request URI</td>
</tr>
<tr>
<td>cs-url</td>
<td>%Y</td>
<td>The entire URL</td>
</tr>
<tr>
<td>cs-username</td>
<td>%A</td>
<td>Authenticated user name. This field is written with double-quotes in the access logs.</td>
</tr>
</tbody>
</table>
### Table 24-11 Log Fields in W3C Logs and Format Specifiers in Access Logs

<table>
<thead>
<tr>
<th>W3C Log Field</th>
<th>Format Specifier in Access Logs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cs-version</td>
<td>%P</td>
<td>Protocol, including the version number when applicable</td>
</tr>
<tr>
<td>date</td>
<td>%v</td>
<td>Date in YYYY-MM-DD</td>
</tr>
<tr>
<td>DCF</td>
<td>%j</td>
<td>Do not cache response code; DCF flags</td>
</tr>
<tr>
<td>s-computerName</td>
<td>%N</td>
<td>Server name or destination hostname. This field is written with double-quotes in the access logs.</td>
</tr>
<tr>
<td>s-hierarchy</td>
<td>%H</td>
<td>Hierarchy retrieval</td>
</tr>
<tr>
<td>s-hostname</td>
<td>%d</td>
<td>Data source or server IP address</td>
</tr>
<tr>
<td>s-ip</td>
<td>%k</td>
<td>Data source IP address (server IP address)</td>
</tr>
<tr>
<td>s-port</td>
<td>%p</td>
<td>Destination port number</td>
</tr>
<tr>
<td>sc(Server)</td>
<td>%&gt;Server:</td>
<td>Server header in the response</td>
</tr>
<tr>
<td>sc-body-size</td>
<td>%b</td>
<td>Bytes sent to the client from the Web Proxy for the body content.</td>
</tr>
<tr>
<td>sc-bytes</td>
<td>%s</td>
<td>Response size (header + body)</td>
</tr>
<tr>
<td>sc-http-status</td>
<td>%h</td>
<td>HTTP response code</td>
</tr>
<tr>
<td>sc-result-code</td>
<td>%w</td>
<td>Result code For example: TCP_MISS, TCP_HIT</td>
</tr>
<tr>
<td>sc-result-code-denial</td>
<td>%W</td>
<td>Result code denial</td>
</tr>
<tr>
<td>time</td>
<td>%V</td>
<td>Time in HH:MM:SS</td>
</tr>
<tr>
<td>timestamp</td>
<td>%t</td>
<td>Timestamp in UNIX epoch</td>
</tr>
</tbody>
</table>

**Note:** If you want to use a third party log analyzer tool to read and parse the W3C access logs, you might need to include the “timestamp” field. Most log analyzers only understand time in the format provided by this field.
### Table 24-11 Log Fields in W3C Logs and Format Specifiers in Access Logs

<table>
<thead>
<tr>
<th>W3C Log Field</th>
<th>Format Specifier in Access Logs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-type</td>
<td>%l</td>
<td>Type of user, either local or remote. For more information, see <em>Working with Remote Users, page 13-2.</em></td>
</tr>
<tr>
<td>x-acltag</td>
<td>%D</td>
<td>ACL decision tag</td>
</tr>
<tr>
<td>x-avc-app</td>
<td>%XO</td>
<td>The web application identified by the AVC engine.</td>
</tr>
<tr>
<td>x-avc-behavior</td>
<td>%Xb</td>
<td>The web application behavior identified by the AVC engine.</td>
</tr>
<tr>
<td>x-avc-reqbody-scanverdict</td>
<td>%XH</td>
<td>AVC request body verdict</td>
</tr>
<tr>
<td>x-avc-reqbody-scanverdict</td>
<td>%XN</td>
<td>AVC response body verdict</td>
</tr>
<tr>
<td>x-avc-reqhead-scanverdict</td>
<td>%XG</td>
<td>AVC request header verdict</td>
</tr>
<tr>
<td>x-avc-resphead-scanverdict</td>
<td>%XM</td>
<td>AVC response header verdict</td>
</tr>
<tr>
<td>x-avc-type</td>
<td>%Xu</td>
<td>The web application type identified by the AVC engine.</td>
</tr>
<tr>
<td>x-avg-bw</td>
<td>%XB</td>
<td>Average bandwidth of the user if bandwidth limits are defined by the AVC engine.</td>
</tr>
<tr>
<td>x-bw-throttled</td>
<td>%XT</td>
<td>Flag that indicates whether or not bandwidth limits were applied to the transaction.</td>
</tr>
<tr>
<td>x-elapsed-time</td>
<td>%e</td>
<td>Elapsed time</td>
</tr>
<tr>
<td>x-error-code</td>
<td>%E</td>
<td>Error type</td>
</tr>
<tr>
<td>x-hierarchy-origin</td>
<td>%H/%d</td>
<td>Code that describes which server was contacted for the retrieving the request content. (e.g. DIRECT/www.example.com)</td>
</tr>
<tr>
<td>x-icap-server</td>
<td>%i</td>
<td>IP address of the last ICAP server contacted while processing the request</td>
</tr>
<tr>
<td>x-icap-verdict</td>
<td>%Xp</td>
<td>External DLP server scanning verdict</td>
</tr>
</tbody>
</table>
### Custom Formatting in Access Logs and W3C Logs

The following table summarizes the log fields in W3C Logs and the format specifiers in Access Logs, along with the description of each field:

<table>
<thead>
<tr>
<th>W3C Log Field</th>
<th>Format Specifier in Access Logs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-ids-verdict</td>
<td>%XI</td>
<td>IronPort 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 &quot;-&quot; if no IDS policy was active for the request.</td>
</tr>
<tr>
<td>x-latency</td>
<td>%x</td>
<td>Latency</td>
</tr>
<tr>
<td>x-local_time</td>
<td>%L</td>
<td>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.</td>
</tr>
<tr>
<td>x-mcafee-av-detecttype</td>
<td>%Xg</td>
<td>McAfee specific identifier: (detect type)</td>
</tr>
<tr>
<td>x-mcafee-av-scanerror</td>
<td>%Xf</td>
<td>McAfee specific identifier: (scan error)</td>
</tr>
<tr>
<td>x-mcafee-av-virustype</td>
<td>%Xh</td>
<td>McAfee specific identifier: (virus type)</td>
</tr>
<tr>
<td>x-mcafee-filename</td>
<td>%Xe</td>
<td>McAfee specific identifier: (File name yielding verdict) This field is written with double-quotes in the access logs.</td>
</tr>
<tr>
<td>x-mcafee-scanverdict</td>
<td>%Xd</td>
<td>McAfee specific identifier: (scan verdict)</td>
</tr>
<tr>
<td>x-mcafee-virus-name</td>
<td>%Xj</td>
<td>McAfee specific identifier: (virus name). This field is written with double-quotes in the access logs.</td>
</tr>
<tr>
<td>x-req-dvs-scanverdict</td>
<td>%X2</td>
<td>Request side DVS Scan verdict</td>
</tr>
<tr>
<td>x-req-dvs-threat-name</td>
<td>%X4</td>
<td>Request side DVS threat name</td>
</tr>
<tr>
<td>x-req-dvs-verdictname</td>
<td>%X3</td>
<td>Request side DVS verdict name</td>
</tr>
<tr>
<td>x-request-rewrite</td>
<td>%XS</td>
<td>Safe browsing scanning verdict. Indicates whether or not either the safe search or site content ratings feature was applied to the transaction. For more information, see Logging Adult Content Access, page 16-22.</td>
</tr>
<tr>
<td>x-resp-dvs-scanverdict</td>
<td>%X0</td>
<td>Response side DVS scan verdict</td>
</tr>
</tbody>
</table>
Table 24-11  Log Fields in W3C Logs and Format Specifiers in Access Logs

<table>
<thead>
<tr>
<th>W3C Log Field</th>
<th>Format Specifier in Access Logs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-resp-dvs-threat-name</td>
<td>%X1</td>
<td>Response side DVS threat name. This field is written with double-quotes in the access logs.</td>
</tr>
<tr>
<td>x-resp-dvs-verdictname</td>
<td>%XZ</td>
<td>Response side DVS verdict name</td>
</tr>
<tr>
<td>x-result-code</td>
<td>%Xr</td>
<td>Result code</td>
</tr>
<tr>
<td>x-resultcode-httpstatus</td>
<td>%w/%h</td>
<td>Result code and the HTTP response code, with a slash (/) in between</td>
</tr>
<tr>
<td>x-sophos-file-name</td>
<td>%Xy</td>
<td>Sophos specific identifier: (threat location)</td>
</tr>
<tr>
<td>x-sophos-scanerror</td>
<td>%Xx</td>
<td>Sophos specific identifier: (scan return code)</td>
</tr>
<tr>
<td>x-sophos-virus-name</td>
<td>%Xz</td>
<td>Sophos specific identifier: (threat name)</td>
</tr>
<tr>
<td>x-suspect-user-agent</td>
<td>%?BLOCK_SUSPECT_USER_AGENT,</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>MONITOR_SUSPECT_USER_AGENT?%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User-Agent:%!%-%.</td>
<td></td>
</tr>
<tr>
<td>x-transaction-id</td>
<td>%I</td>
<td>Transaction ID</td>
</tr>
<tr>
<td>x-wbrs-score</td>
<td>%XW</td>
<td>Decoded WBRS score &lt;-10.0-10.0&gt;</td>
</tr>
<tr>
<td>x-wbrs-threat-reason</td>
<td>%XK</td>
<td>Web reputation threat reason</td>
</tr>
<tr>
<td>x-wbrs-threat-type</td>
<td>%Xk</td>
<td>Web reputation threat type</td>
</tr>
<tr>
<td>N/A</td>
<td>%Xw</td>
<td>Raw numeric WBRS score</td>
</tr>
<tr>
<td>N/A</td>
<td>%Xc</td>
<td>URL category code (numeric) of the URL category assigned to the transaction. Applies to both IronPort URL Filters and Cisco IronPort Web Usage Controls URL filtering engines.</td>
</tr>
<tr>
<td>x-webcat-code-abbr</td>
<td>%XC</td>
<td>URL category abbreviation for the URL category assigned to the transaction. Applies to both IronPort URL Filters and Cisco IronPort Web Usage Controls URL filtering engines.</td>
</tr>
</tbody>
</table>
### Table 24-11  
**Log Fields in W3C Logs and Format Specifiers in Access Logs**

<table>
<thead>
<tr>
<th>W3C Log Field</th>
<th>Format Specifier in Access Logs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-webcat-code-full</td>
<td>%XF</td>
<td>Full name of the URL category assigned to the transaction. This field is written with double-quotes in the access logs. Applies to both IronPort URL Filters and Cisco IronPort Web Usage Controls URL filtering engines.</td>
</tr>
<tr>
<td>N/A</td>
<td>%Xq</td>
<td>The URL category code (numeric) determined during request-side scanning. Applies to both IronPort URL Filters and Cisco IronPort Web Usage Controls URL filtering engines.</td>
</tr>
<tr>
<td>x-webcat-req-code-abbr</td>
<td>%XQ</td>
<td>The URL category verdict determined during request-side scanning, abbreviated. Applies to both IronPort URL Filters and Cisco IronPort Web Usage Controls URL filtering engines.</td>
</tr>
<tr>
<td>x-webcat-req-code-full</td>
<td>%XR</td>
<td>The URL category verdict determined during request-side scanning, full name. Applies to both IronPort URL Filters and Cisco IronPort Web Usage Controls URL filtering engines.</td>
</tr>
<tr>
<td>N/A</td>
<td>%Xa</td>
<td>The URL category code (numeric) determined during response-side scanning. Applies to the Cisco IronPort Web Usage Controls URL filtering engine only.</td>
</tr>
<tr>
<td>x-webcat-resp-code-abbr</td>
<td>%XA</td>
<td>The URL category verdict determined during response-side scanning, abbreviated. Applies to the Cisco IronPort Web Usage Controls URL filtering engine only.</td>
</tr>
</tbody>
</table>
### Table 24-11 Log Fields in W3C Logs and Format Specifiers in Access Logs

<table>
<thead>
<tr>
<th>W3C Log Field</th>
<th>Format Specifier in Access Logs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-webcat-resp-code-full</td>
<td>%XL</td>
<td>The URL category verdict determined during response-side scanning, full name. Applies to the Cisco IronPort Web Usage Controls URL filtering engine only.</td>
</tr>
<tr>
<td>x-webroot-scanverdict</td>
<td>%Xv</td>
<td>Malware scanning verdict from Webroot</td>
</tr>
<tr>
<td>x-webroot-spyid</td>
<td>%Xs</td>
<td>Webroot specific identifier: (Spy ID)</td>
</tr>
<tr>
<td>x-webroot-threat-name</td>
<td>%Xn</td>
<td>Webroot specific identifier: (Threat name) This field is written with double-quotes in the access logs.</td>
</tr>
<tr>
<td>x-webroot-trace-id</td>
<td>%Xi</td>
<td>Webroot specific scan identifier: (Trace ID)</td>
</tr>
<tr>
<td>x-webroot-trr</td>
<td>%Xt</td>
<td>Webroot specific identifier: (Threat Risk Ratio (TRR))</td>
</tr>
<tr>
<td>x-s2p-first-byte-time</td>
<td>%:&gt;1</td>
<td>Wait-time for first response byte from server</td>
</tr>
<tr>
<td>x-c2p-first-byte-time</td>
<td>%:1&lt;</td>
<td>Wait-time for first request byte from new client connection</td>
</tr>
<tr>
<td>x-p2c-first-byte-time</td>
<td>%:1&gt;</td>
<td>Wait-time for first byte written to client</td>
</tr>
<tr>
<td>x-p2p-auth-wait-time</td>
<td>%:&lt;a</td>
<td>Wait-time to receive the response from the Web Proxy authentication process, after the Web Proxy sent the request.</td>
</tr>
<tr>
<td>x-p2p-auth-svc-time</td>
<td>%:&gt;a</td>
<td>Wait-time to receive the response from the Web Proxy authentication process, including the time required for the Web Proxy to send the request.</td>
</tr>
<tr>
<td>x-p2p-avc-svc-time</td>
<td>%:A&lt;</td>
<td>Wait-time to receive the response from the AVC process, including the time required for the Web Proxy to send the request.</td>
</tr>
<tr>
<td>x-p2p-avc-wait-time</td>
<td>%:A&gt;</td>
<td>Wait-time to receive the response from the AVC process, after the Web Proxy sent the request.</td>
</tr>
</tbody>
</table>
### Custom Formatting in Access Logs and W3C Logs

<table>
<thead>
<tr>
<th>W3C Log Field</th>
<th>Format Specifier in Access Logs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-p2s-body-time</td>
<td>%:&lt;b</td>
<td>Wait-time to write request body to server after header</td>
</tr>
<tr>
<td>x-s2p-body-time</td>
<td>%:&gt;b</td>
<td>Wait-time for complete response body after header received</td>
</tr>
<tr>
<td>x-c2p-body-time</td>
<td>%:&lt;b</td>
<td>Wait-time for complete client body</td>
</tr>
<tr>
<td>x-p2c-body-time</td>
<td>%:&gt;b</td>
<td>Wait-time for complete body written to client</td>
</tr>
<tr>
<td>x-p2p-fetch-time</td>
<td>%:&gt;c</td>
<td>Time required for the Web Proxy to read a response from the disk cache.</td>
</tr>
<tr>
<td>x-p2p-dca-resp-wait-time</td>
<td>%:&lt;c</td>
<td>Wait-time to receive the response from the Dynamic Content Analysis engine, after the Web Proxy sent the request.</td>
</tr>
<tr>
<td>x-p2p-dca-resp-svc-time</td>
<td>%:&gt;c</td>
<td>Wait-time to receive the verdict from the Dynamic Content Analysis engine, including the time required for the Web Proxy to send the request.</td>
</tr>
<tr>
<td>x-p2p-dns-wait-time</td>
<td>%:&lt;d</td>
<td>Wait-time to receive the response from the Web Proxy DNS process, after the Web Proxy sent the request.</td>
</tr>
<tr>
<td>x-p2p-dns-svc-time</td>
<td>%:&gt;d</td>
<td>Wait-time to receive the response from the Web Proxy DNS process, including the time required for the Web Proxy to send the request.</td>
</tr>
<tr>
<td>x-p2s-header-time</td>
<td>%:&lt;h</td>
<td>Wait-time to write request header to server after first byte</td>
</tr>
<tr>
<td>x-s2p-header-time</td>
<td>%:&gt;h</td>
<td>Wait-time for server header after first response byte</td>
</tr>
<tr>
<td>x-c2p-header-time</td>
<td>%:&lt;h</td>
<td>Wait-time for complete client header after first byte</td>
</tr>
<tr>
<td>x-s2p-header-time</td>
<td>%:&gt;h</td>
<td>Wait-time for complete header written to client</td>
</tr>
</tbody>
</table>
### Table 24-11 Log Fields in W3C Logs and Format Specifiers in Access Logs

<table>
<thead>
<tr>
<th>W3C Log Field</th>
<th>Format Specifier in Access Logs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-p2p-mcafee-resp-svc-time</td>
<td>%:m&lt;</td>
<td>Wait-time to receive the verdict from the McAfee scanning engine, including the time required for the Web Proxy to send the request.</td>
</tr>
<tr>
<td>x-p2p-mcafee-resp-wait-time</td>
<td>%:m&gt;</td>
<td>Wait-time to receive the response from the McAfee scanning engine, after the Web Proxy sent the request.</td>
</tr>
<tr>
<td>x-p2p-sophos-resp-svc-time</td>
<td>%:p&lt;</td>
<td>Wait-time to receive the verdict from the Sophos scanning engine, including the time required for the Web Proxy to send the request.</td>
</tr>
<tr>
<td>x-p2p-sophos-resp-wait-time</td>
<td>%:p&gt;</td>
<td>Wait-time to receive the response from the Sophos scanning engine, after the Web Proxy sent the request.</td>
</tr>
<tr>
<td>x-p2p-reputation-wait-time</td>
<td>%:&lt;r</td>
<td>Wait-time to receive the response from the Web Reputation Filters, after the Web Proxy sent the request.</td>
</tr>
<tr>
<td>x-p2p-reputation-svc-time</td>
<td>%:r&gt;</td>
<td>Wait-time to receive the verdict from the Web Reputation Filters, including the time required for the Web Proxy to send the request.</td>
</tr>
<tr>
<td>x-p2p-asw-req-wait-time</td>
<td>%:&lt;s</td>
<td>Wait-time to receive the verdict from the Web Proxy anti-spyware process, after the Web Proxy sent the request.</td>
</tr>
<tr>
<td>x-p2p-asw-req-svc-time</td>
<td>%:s&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>
Configuring Custom Formatting in Access Logs

Use the System Administration > Log Subscriptions page to configure custom formatting for access log file entries. Click the access log file name to edit the access log subscription.

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

```
<format_specifier1> <format_specifier2>
```

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`, `body_bytes` is the descriptive token for `%b`, and `error_type` is the descriptive token for `%E`.

<table>
<thead>
<tr>
<th>W3C Log Field</th>
<th>Format Specifier in Access Logs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-p2p-webroot-resp-svc-time</td>
<td>%:w&lt;</td>
<td>Wait-time to receive the verdict from the Webroot scanning engine, including the time required for the Web Proxy to send the request.</td>
</tr>
<tr>
<td>x-p2p-webroot-resp-wait-time</td>
<td>%:w&gt;</td>
<td>Wait-time to receive the response from the Webroot scanning engine, after the Web Proxy sent the request.</td>
</tr>
</tbody>
</table>
**Note**

You can create a custom field for any header in a client request or a server response. For more information, see Including HTTP/HTTPS Headers in Log Files, page 24-51.

---

**Configuring Custom Formatting in W3C Logs**

Use the System Administration > Log Subscriptions page to configure custom formatting for W3C log file entries. Click the W3C log file name to edit the W3C log subscription.

*Figure 24-3 Configuring Custom Log Fields in the W3C Logs*

Enter the custom fields to add in the Custom Fields text box in the Log Fields section. You can enter multiple custom fields in the Custom Fields text box and add them simultaneously as long as each entry is separated by a new line (click Enter) before clicking Add.
You can create a custom field for any header in a client request or a server response. For more information, see Including HTTP/HTTPS Headers in Log Files, page 24-51.

Including HTTP/HTTPS Headers in Log Files

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.

Table 24-12 defines the syntax to use for access and W3C logs.

<table>
<thead>
<tr>
<th>Header Type</th>
<th>Access Log Format Specifier Syntax</th>
<th>W3C Log Custom Field Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header from the client</td>
<td>%&lt;ClientHeaderName:</td>
<td>cs(ClientHeaderName)</td>
</tr>
<tr>
<td>application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Header from the server</td>
<td>%&lt;ServerHeaderName:</td>
<td>sc(ServerHeaderName)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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)
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 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.

They are the result of proprietary calculations that associate a numerical value to the probability that either the URL request or the response content contains malware. 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.

Both the Webroot and McAfee scanning engines can return malware scanning verdicts to the DVS engine. For more information about how the DVS engine handles malware scanning verdicts, see IronPort DVS™ (Dynamic Vectoring and Streaming) Engine, page 19-4.

Table 24-13 lists the different Malware Scanning Verdict Values and each malware category with which they correspond.

<table>
<thead>
<tr>
<th>Malware Scanning Verdict Value</th>
<th>Malware Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>Not set</td>
</tr>
<tr>
<td>0</td>
<td>Unknown</td>
</tr>
<tr>
<td>1</td>
<td>Not Scanned or Skipped</td>
</tr>
<tr>
<td>2</td>
<td>Timeout</td>
</tr>
<tr>
<td>3</td>
<td>Unscannable</td>
</tr>
<tr>
<td>4</td>
<td>Unscannable</td>
</tr>
<tr>
<td>5</td>
<td>Freelist Exhaustion</td>
</tr>
<tr>
<td>6</td>
<td>Bad verdict</td>
</tr>
<tr>
<td>7</td>
<td>No Launch Method</td>
</tr>
<tr>
<td>10</td>
<td>Other Malware</td>
</tr>
<tr>
<td>12</td>
<td>Browser Helper Object</td>
</tr>
<tr>
<td>13</td>
<td>Adware</td>
</tr>
<tr>
<td>14</td>
<td>System Monitor</td>
</tr>
</tbody>
</table>

Table 24-13 Malware Scanning Verdict Values
The L4 Traffic Monitor log file provides a detailed record of monitoring activity. You can view L4 Traffic Monitor log file entries and track updates to firewall block lists and firewall allow lists. Consider the following example log entries:

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 L4 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.

<table>
<thead>
<tr>
<th>Malware Scanning Verdict Value</th>
<th>Malware Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>Commercial System Monitor</td>
</tr>
<tr>
<td>19</td>
<td>Dialer</td>
</tr>
<tr>
<td>20</td>
<td>Hijacker</td>
</tr>
<tr>
<td>21</td>
<td>Phishing URL</td>
</tr>
<tr>
<td>22</td>
<td>Trojan Downloader</td>
</tr>
<tr>
<td>23</td>
<td>Trojan Horse</td>
</tr>
<tr>
<td>24</td>
<td>Trojan Phisher</td>
</tr>
<tr>
<td>25</td>
<td>Worm</td>
</tr>
<tr>
<td>26</td>
<td>Encrypted File</td>
</tr>
<tr>
<td>27</td>
<td>Virus</td>
</tr>
<tr>
<td>28</td>
<td>Too Many Outstanding requests</td>
</tr>
<tr>
<td>33</td>
<td>Other Malware</td>
</tr>
<tr>
<td>34</td>
<td>PUA</td>
</tr>
</tbody>
</table>
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 L4 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 L4 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 L4 Traffic Monitor is set to monitor, not block.

Troubleshooting

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 IronPort Customer Support to verify whether or not you need additional Web Security appliance capacity.
This chapter contains the following information:

- Changing the System Hostname, page 25-1
- Configuring Network Interfaces, page 25-2
- Configuring TCP/IP Traffic Routes, page 25-7
- Virtual Local Area Networks (VLANs), page 25-9
- Configuring Transparent Redirection, page 25-17
- Configuring SMTP Relay Hosts, page 25-26
- Configuring DNS Server(s), page 25-28

### Changing the System Hostname

The hostname parameter is used to identify the system at the CLI prompt. You must enter a fully-qualified hostname for the system. The hostname parameter is also used in end-user notification pages, end-user acknowledgement pages, and to form the machine NetBIOS name when the Web Security appliance joins an Active Directory domain. It has no direct relationship with the hostname configured for the interface.
Use the `sethostname` command to change the name of the Web Security appliance:

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

---

### Configuring Network Interfaces

You can configure the appliance network interfaces by modifying IP address, subnet, and hostname information for the Management, Data, and L4 Traffic Monitor interfaces. *Table 25-1* describes the network interface settings you can configure.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>M1</td>
<td>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.</td>
</tr>
</tbody>
</table>
Configuring Network Interfaces

Table 25-1 Web Security Appliance Network Interface Settings (continued)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>P1 and P2 (proxy)</td>
<td>The Data interfaces are used for Web Proxy monitoring and L4 Traffic Monitor blocking (optional). You can also configure these interfaces to support outbound services such as DNS, software upgrades, NTP, and traceroute data traffic. For more information about configuring the Data interfaces, see Configuring the Data Interfaces, page 25-3.</td>
</tr>
</tbody>
</table>
| L4 Traffic Monitor | T1 and T2   | The L4 Traffic Monitor interfaces are used to configure a duplex or simplex wiring type.  
- **Duplex.** The T1 interface receives incoming and outgoing traffic.  
- **Simplex.** T1 receives outgoing traffic and T2 receives incoming traffic. |

Note

If the Management and Data interfaces are all configured, each must be assigned IP addresses on different subnets.

You can manage the network interfaces using the following methods:

- **Web interface.** Use the Network > Interfaces page. For more information, see Configuring the Network Interfaces from the Web Interface, page 25-5.
- **Command line interface.** Use the `ifconfig` CLI command to create, edit, and delete network interfaces.

Configuring the Data Interfaces

You can configure the Web Security appliance to use any of the following combinations of network interfaces for data traffic:

- M1 only
M1 and P1
M1, P1, and P2
P1 only
P1 and P2

You can enable the M1 and P1 ports during or after System Setup. However, you can only enable the P2 port after System Setup in the web interface or using the ifconfig CLI command.

The Web Proxy listens for client web requests on different network interfaces depending on how you configure the Web Security appliance:

- **M1.** The Web Proxy listens for requests on this interface when it is not configured to be restricted to appliance management services only.
- **P1.** The Web Proxy listens for requests on this interface when it is enabled.
- **P2.** By default, the Web Proxy does not listen for requests on this interface, even when enabled. However, you can configure it to listen for requests on P2 using the advancedproxyconfig > miscellaneous CLI command.

To configure the appliance to use P2 as a second data interface:

---

**Step 1** Configure the appliance to use P1 as the interface for data traffic. You can do this during System Setup or after initial setup on the Network > Interfaces page.

**Step 2** Enable P2 in the web interface (see Configuring the Network Interfaces from the Web Interface, page 25-5) or using the ifconfig CLI command.

---

**Note** If the Management and Data interfaces are all configured, each must be assigned IP addresses on different subnets.

**Step 3** In the web interface, go to the Network > Routes page. Change the Default Route for data traffic to specify the next IP address that the P2 interface is connected to.

---

**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.
Chapter 25   Configuring Network Settings

Configuring the Network Interfaces from the Web Interface

To configure the network interfaces from the web interface:

Step 1   Navigate to the Network > Interfaces page. Click **Edit Settings**.

The Edit Interfaces page appears.

**Figure 25-1   Editing Network Interfaces**

![Edit Interfaces](image)

**Step 2** Configure interface settings as necessary.

**Table 25-2** describes the interface settings you can define for each interface.

<table>
<thead>
<tr>
<th>Interface Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address to use to manage the Web Security appliance. Enter an IP address that exists on your management network.</td>
</tr>
</tbody>
</table>
Step 3 Specify whether or not to have separate routing for the Management Services using the “Restrict M1 port to appliance management services only” field.

If this checkbox is selected, the M1 port is used for appliance management services only and is not used for the data (Web Proxy) traffic. You will need to configure another port for data traffic as well as separate routes for management and data traffic. For more information about configuring routes, see Configuring TCP/IP Traffic Routes, page 25-7.

Step 4 Configure Appliance Management Services.

Choose whether or not to use HTTP or HTTPS to administer AsyncOS through the web interface. You must specify the port to access AsyncOS with each protocol you configure.

You can also choose to redirect HTTP requests to HTTPS. When you do this, AsyncOS automatically enables both HTTP and HTTPS.

Step 5 Choose the type of wired connections plugged into the “T” network interfaces:

- **Duplex TAP.** Choose Duplex TAP when the T1 port receives both incoming and outgoing traffic. You can use half- or full-duplex Ethernet connections.

- **Simplex TAP.** Choose Simplex TAP when you connect the T1 port to the internal network (traffic flows from the clients to the Internet) and you connect the T2 port to the external network (traffic flows from the Internet to the clients).

**Note** Cisco recommends using simplex when possible because it can increase performance and security.

Step 6 Submit and commit your changes.
Configuring TCP/IP Traffic Routes

You can administer routes for data and management traffic, add static routes, load your IP routing tables, and modify the default gateway using the Network > Routes page or the `routeconfig` command.

The number of sections on this page is determined by how the “Restrict M1 port to appliance management services only” check box is configured on the Network > Interfaces page:

- **Separate route configuration sections for Management and Data traffic.** When you use the Management interface for management traffic only (“Restrict M1 port” is enabled), then this page includes two sections to enter route table information, one for management traffic and one for data traffic. AsyncOS uses the management route information for management traffic only, and data route information for data traffic. Figure 25-3 on page 9 shows the Routes page when the option is enabled.

- **One route configuration section for all traffic (Management and Data).** When you use the Management interface for both management and data traffic (“Restrict M1 port” is disabled), then this page includes one section to enter route table information 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.

Modifying the Default Route

You can modify the default gateway in the web interface or in the CLI using the `setgateway` CLI command.

**Note**
The Web Proxy sends out transactions on the data interface that is on the same network as the default gateway configured for data traffic.

To modify the default gateway in the web interface:
Chapter 25  Configuring Network Settings

Configuring TCP/IP Traffic Routes

Step 1  Navigate to the Network > Routes page, and click on Default Route in the corresponding table.

Figure 25-2  Editing the Default Route

Edit Default Route for Management and Data (Interface M1: 10.1.1.1, Interface P1: 10.1.2.1)

<table>
<thead>
<tr>
<th>Default Gateway Settings</th>
<th>Destination Network</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Route</td>
<td>All Others (Including External)</td>
<td>10.5.5.1</td>
</tr>
</tbody>
</table>

Step 2  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 3  Submit and commit your changes.

Working With Routing Tables

You can save your current routing table to a file. You can load a previously saved route table. You can add new routes or delete existing ones.

To save a route table, click Save Route Table and specify where to save the file.

To load a previously saved route table, click Load Route Table, navigate to the file, and then 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.

To add a route:

Step 1  Navigate to the Network > Routes page.
Step 2  Click the **Add Route** button corresponding to the interface for which you are creating the route. The Add Route page is displayed.

Step 3  Enter a Name, Destination Network, and Gateway.

Step 4  Submit and commit your changes.

### Virtual Local Area Networks (VLANs)

VLANs are virtual local area networks bound to physical data ports. You can configure one or more VLANs to increase the number of networks the IronPort appliance can connect to beyond the number of physical interfaces included. For example, a Web Security appliance has two data interfaces available for VLANs: P1 and Management. VLANs allow more networks to be defined on separate “ports” on existing interfaces. Figure 25-4 provides an example of configuring several VLANs on the P1 interface.
Virtual Local Area Networks (VLANs)

Figure 25-4 Using VLANs to Increase the Number of Networks Available on the Appliance

VLANs can be used to segment networks for security purposes, to ease administration, or increase bandwidth. For example, create multiple VLANs on the P1 interface and then apply different policies to each. 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. Duplicate VLAN IDs are not allowed on an IronPort appliance.
VLANs and Physical Ports

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.

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. Remember to commit all changes.

Creating a New VLAN via the etherconfig Command

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.

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

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

- **NEW** - Create a new VLAN.

[]> new

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

[]> 34

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

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

[]> 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.
Choose the operation you want to perform:

- NEW - Create a new VLAN.

[1]> new

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

[1]> 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.
[1]> new

VLAN ID for the interface (Ex: "34"):  
[1]> 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.

[1]>
Creating an IP Interface on a VLAN via the interfaceconfig Command

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.

```
example.com> interfaceconfig

Currently configured interfaces:

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

Choose the operation you want to perform:

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

[]> new

IP Address (Ex: 10.10.10.10):

[]> 10.10.31.10

Ethernet interface:

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

[1]> 4

Netmask (Ex: "255.255.255.0" or "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.

[]>
Configuring Transparent Redirection

When you configure the Web Security appliance web proxy service in transparent mode, you must connect the appliance to an L4 switch or a WCCP v2 router, and you must configure the appliance so it knows to which device it is connected. You configure the device on the Network > Transparent Redirection page.

Figure 25-5  Network > Transparent Redirection Page

On this page, you can choose the device that transparently redirects traffic to the appliance, either an L4 switch or a WCCP router. When you choose an L4 switch as the device, there is nothing else to configure on this page.

However, when you choose a WCCP router as the device, you must create at least one WCCP service.

Working with 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.

You can create WCCP services that use the following service types:
• **Standard service.** The standard service is also known as a well known service because the characteristics of it are known by both WCCP routers and the appliance. It redirects traffic on port 80. It is identified as the “web-cache” service.

• **Dynamic service.** Dynamic services are any other service a web proxy creates, but the web proxy must describe the components of the service group to the router. AsyncOS supports the creation of any dynamic service you choose to define. To create a dynamic service, you must provide the service ID number, port numbers, and specify whether to redirect packets based on the destination or source port and whether to distribute packets based on the client or server address.

The Web Cache Communication Protocol allows 257 different service IDs. AsyncOS allows you to create a dynamic WCCP service for each possible service ID. However, in typical usage, most users create one or two WCCP services, where one is a standard service and the other a dynamic service.

When you create a WCCP service of any type, you must also specify the following information:

• **Assignment method.** For more information, see *Working with the Assignment Method, page 25-18.*

• **Forwarding and Return method.** For more information, see *Working with the Forwarding and Return Method, page 25-19.*

If you enable IP spoofing on the appliance, you must create two WCCP services. For more information, see *IP Spoofing when Using WCCP, page 25-20.*

**Working with the Assignment Method**

WCCP defines the assignment method as the method by which redirected packets are distributed between web proxies. In this case, between one or more Web Security appliances. The assignment method determines how the router performs load balancing of packets among multiple Web Security appliances.

You configure the assignment method for a WCCP service in the Load-Balancing Method field under the Advanced section when you create or edit a WCCP service.

You can configure WCCP services to use either of the following assignment methods:
Chapter 25 Configuring Network Settings

Configuring Transparent Redirection

- **Mask.** This method relies on masking to make redirection decisions. WCCP routers make decisions using hardware in the router. This method can be very efficient because the hardware redirects the packets. You might want to choose mask to reduce CPU cycles on the router which can increase router performance. You can only use mask with WCCP routers that support mask assignment.

  **Note** AsyncOS chooses the mask value to use with the router. You cannot configure the mask value.

- **Hash.** This method relies on a hash function to make redirection decisions. You might want to use Hash when the WCCP router does not support masking.

You can also configure a WCCP service to allow either mask or hash load balancing. When a WCCP service allows both mask and hash, AsyncOS communicates with the router to determine whether or not the router supports mask. If the router supports mask, then AsyncOS uses masking in the service group, if the router does not support mask, then AsyncOS uses hashing in the service group.

**Working with the Forwarding and Return Method**

WCCP defines the forwarding method as the method by which redirected packets are transported from the router to the web proxy. Conversely, the return method redirects packets from the web proxy to the router.

You configure the forwarding and return methods for a WCCP service in the Forwarding Method and Return Method fields under the Advanced section when you create or edit a WCCP service.

You can configure WCCP services to use either of the following methods:

- **Layer 2 (L2).** This method redirects traffic at layer 2 by replacing the packet’s destination MAC address with the MAC address of the target web proxy. This method requires that the target web proxy be directly connected to the router at layer 2. WCCP routers only allow L2 negotiation when the appliance is directly connected to the router at layer 2. The L2 method redirects traffic at the router hardware level, and typically has better performance than Generic Routing Encapsulation (GRE). You might want to
choose L2 when the router is directly connected to the appliance and you want the performance improvement provided by the L2 method. You can only use the L2 method with WCCP routers that support L2 forwarding.

- **Generic Routing Encapsulation (GRE).** This method redirects traffic at layer 3 by encapsulating the IP packet with a GRE header and a redirect header. This method redirects traffic at the router software level, which can impact performance. You might want to choose GRE when the appliance is not directly connected to the router.

You can also configure a WCCP service to allow either the L2 or GRE methods. When a WCCP service allows both L2 and GRE, 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.

**Note** If the router is not directly connected to the appliance, you must choose GRE.

### IP Spoofing when Using WCCP

You can configure the Web Proxy to do IP spoofing. When enabled, requests originating from a client retain the client’s source address and appear to originate from the client instead of the Web Proxy.

When you enable IP spoofing, you must create two WCCP services. One WCCP service must redirect traffic based on the destination port, and another based on the source port for the return path. The service based on the destination port can be the standard web-cache service. However, you must still create at least one dynamic service.

The two WCCP services you define for IP spoofing must have the same values for the following settings:

- Port numbers
- Router IP addresses
- Router security and password

**Note** IronPort suggests using a service ID number from 90 to 97 for the WCCP service used for the return path (based on the source port).
For more information about creating WCCP services, see Adding and Editing a WCCP Service, page 25-21.

Adding and Editing a WCCP Service

You must create at least one WCCP service when you configure the transparent redirection device as a WCCP router. If IP spoofing is enabled on the appliance, you must create two WCCP services. For more information about IP spoofing, see IP Spoofing when Using WCCP, page 25-20.

To add or edit a WCCP service:

Step 1 Navigate to the Network > Transparent Redirection page.

Step 2 Verify the transparent redirection device is a WCCP v2 router. If it is not, click Edit Device to change it.

Step 3 To add a WCCP service, click Add Service. Or, to edit a WCCP service, click the name of the WCCP service in the Service Profile Name column.

    The Add WCCP v2 Service page or Edit WCCP v2 Service page appears.
Step 4 Configure the WCCP options.
Table 25-3 describes the WCCP options.

**Table 25-3 WCCP Service Options**

<table>
<thead>
<tr>
<th>WCCP Service Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Profile Name</td>
<td>Enter a name for the WCCP service.</td>
</tr>
<tr>
<td>Service</td>
<td>Use this section to describe the service group for the router. Choose to create either a standard (&quot;well known&quot;) or dynamic service group. If you create a dynamic service, enter the following information:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Service ID.</strong> Enter any number from 0 to 255 in the Dynamic Service ID field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Port number(s).</strong> Enter up to eight port numbers for traffic to redirect in the Port Numbers field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Redirection basis.</strong> Choose to redirect traffic based on the source or destination port. Default is destination port.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Load balancing basis.</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>For more information about well known and dynamic service groups, see Working with WCCP Services, page 25-17.</td>
</tr>
<tr>
<td>Router IP Addresses</td>
<td>Enter the IP address for one or more WCCP enabled routers. You can enter up to 32 routers to the service group. You must enter the IP address of each router. You cannot enter a multicast address.</td>
</tr>
</tbody>
</table>
### Table 25-3  WCCP Service Options (continued)

<table>
<thead>
<tr>
<th>WCCP Service Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Security</td>
<td>Choose whether or not to require a password for this service group. If required, enter the password in the password fields. The password can contain up to seven characters. When you enable security for a service group, every appliance and WCCP router that uses the service group must use the same password. Requiring a password enables you to control which routers and WCCP-enabled systems, such as the Web Security appliance, become part of the service group. WCCP uses the MD5 hash protocol to encrypt the password. <strong>Note</strong> — Each appliance or WCCP router in the service group authenticate the security component in a received WCCP packet immediately after validating the WCCP message header. Packets failing authentication are discarded.</td>
</tr>
</tbody>
</table>
Deleting a WCCP Service

To delete a WCCP service:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Navigate to the Network &gt; Transparent Redirection page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the icon in the Delete column for the WCCP service you want to delete.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Commit your changes.</td>
</tr>
</tbody>
</table>
Configuring SMTP Relay Hosts

AsyncOS periodically sends system-generated email messages, such as notifications, alerts, and IronPort 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.

You might want to configure an SMTP relay host in the following scenarios:

- You want the system-generated emails to go to a non-local email address, and port 25 is blocked to outside networks.
- Your mail servers do not allow direct port 25 traffic from internal hosts.

If no SMTP relay host is defined, AsyncOS delivers directly to the mail server for each email address.

**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. You might want to configure multiple SMTP relay hosts for redundancy in case one system becomes unavailable. 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.

You can configure the SMTP relay host from either the web interface or command line interface:

- **Web interface.** Use the Network > Internal SMTP Relay page.
- **Command line interface.** Use the `smtprelay` CLI command.

**Configuring SMTP from the Web Interface**

Use the Network > Internal SMTP Relay page.

To configure the SMTP relay host from the web interface:
Configuring Network Settings

Chapter 25      Configuring Network Settings

Configuring SMTP Relay Hosts

Step 1
Navigate to the Network > Internal SMTP Relay page, and click Edit Settings.

Step 2
Enter the information listed in Table 25-4.

Table 25-4      SMTP Relay Host Settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relay Hostname or IP Address</td>
<td>Enter the hostname or IP address to use for the SMTP relay</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port for connecting to the SMTP relay. If this property is empty, the appliance uses port 25. This property is optional.</td>
</tr>
<tr>
<td>Routing Table to Use for SMTP</td>
<td>Choose 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.</td>
</tr>
</tbody>
</table>

Step 3
Optionally, you can add more SMTP relay host information by clicking Add Row.

Step 4
Submit and commit your changes.

Configuring SMTP from the CLI

Use the smtprelay command to configure SMTP relay hosts.

For example:

```
example.com> smtprelay
No internal SMTP relay host configured.
```

Choose the operation you want to perform:
Configuring DNS Server(s)

You can configure the DNS settings for your IronPort appliance using the Network > DNS page or using the `dnsconfig` command. Before you configure DNS, consider the following:

- Whether to use the Internet’s DNS servers or your own, and which specific server(s) to use.
- Which routing table to use for DNS traffic.
  You must use the routing table associated with the interface that faces the DNS server, either Data or Management.
- The number of seconds to wait before timing out a reverse DNS lookup.
- Clearing the DNS cache.

Specifying DNS Servers

IronPort AsyncOS 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

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.
Using the Internet Root Servers

The IronPort AsyncOS DNS resolver is designed to accommodate the large number of simultaneous DNS connections.

Multiple Entries and Priority

For each DNS server you enter, you can specify a numeric priority. AsyncOS will attempt to use the DNS server with the priority closest to 0. If that DNS server is not responding AsyncOS will attempt to use the server at the next priority. If you specify multiple entries for DNS servers with the same priority, the system randomizes the list of DNS servers at that priority every time it performs a query. The system then waits a short amount of time for the first query to expire or “time out” and then increments with a slightly longer amount of time for subsequent servers. The amount of time depends on the exact number of DNS servers and priorities that have been configured. The timeout length is the same for all IP addresses at any particular priority. The first priority gets the shortest timeout, each subsequent priority gets a longer timeout. Further, the timeout period is roughly 60 seconds. If you have one priority, the timeout for each server at that priority is 60 seconds. If you have two priorities, the timeout for each server at the first priority is 15 seconds, and each server at the second priority is 45 seconds. For three priorities, the timeout increments are 5, 10, 45.

For example, four DNS servers with two configured at priority 0, one at priority 1, and one at priority 2:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Server(s)</th>
<th>Timeout (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1.2.3.4, 1.2.3.5</td>
<td>5, 5</td>
</tr>
<tr>
<td>1</td>
<td>1.2.3.6</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>1.2.3.7</td>
<td>45</td>
</tr>
</tbody>
</table>

AsyncOS randomly chooses between the two servers at priority 0. If one of the priority 0 servers is down, the other is used. If both priority 0 servers are down, the priority 1 server (1.2.3.6) is used, and finally, the priority 2 (1.2.3.7) server.

The timeout period is the same for both priority 0 servers, longer for the priority 1 server, and longer still for the priority 2 server.
DNS Alert

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.

Clearing the DNS Cache

You can use the Clear DNS Cache button on Network > DNS page, or the dnsflush command to clear all information in the DNS cache when changes have been made to your local DNS system. Using this command might cause a temporary performance degradation while the cache is repopulated.

Configuring DNS

To edit DNS Settings:

**Step 1** Navigate to the Network > DNS page.

**Step 2** Click **Edit Settings**. The Edit DNS page appears.
Step 3  Select to use the Internet’s root DNS servers or your own internal DNS server or the Internet’s root DNS servers and specify authoritative DNS servers.

Step 4  If you use your own DNS server(s), or specify authoritative DNS servers, enter the server ID, specify a priority, and use the Add Row key to repeat as necessary for each server.

Step 5  Choose the routing table associated with an appliance network interface type, either Management or Data, to use for DNS traffic.

Step 6  Enter the number of seconds to wait before cancelling a reverse DNS lookup.

Step 7  Submit and commit to save the changes.
Managing the S-Series Appliance

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
Updates to security components
System time

Saving and Loading the Appliance Configuration

All configuration settings within the Web Security appliance can be managed using a single configuration file. The file is maintained in XML (Extensible Markup Language) format.

To archive the current configuration, you can use the System Administration > Configuration Summary page to print a summary of appliance settings, and you can use the System Administration > Configuration File page to create a local copy of the system configuration file. The system configuration file can be used to import a complete configuration or to load a unique sub-section and update specific settings.

When you save the configuration file, you can choose a system-generated name or define your own file name. You can mask the user’s passwords by clicking a checkbox. Masking a password causes the original, encrypted password to be replaced with “*****” in the exported or saved file. Please note, however, that configuration files with masked passwords cannot be loaded back into AsyncOS for Web.

Use the Load Configuration section of the System Administration > Configuration File page to load new configuration information into the Web Security appliance. You can load information using any of the following methods:

- Place information in the configuration directory and upload it.
- Upload the configuration file directly from your local machine.
- Paste configuration information directly into the web interface.

To load a copy of the configuration file, paste the configuration directly into the web interface page. At the top of the configuration file you must include the following tag:

```xml
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE config SYSTEM "config.dtd"> <config> ... your configuration information in valid XML </config>
```
After loading the XML sub-section, submit and commit the update.

**Committing Changes to the Appliance Configuration**

Each time you modify settings and change appliance behavior using the S-Series web interface, you must first submit your changes and then commit them to the active configuration.

For more information about committing changes, see Committing and Clearing Changes, page 2-14.

**Support Commands**

The features in this section are useful when you upgrade the appliance or contact your support provider. You can find the following commands under the Technical Support section of the Support and Help menu:

- **Open a Support Case.** For more information, see Open a Support Case, page 26-3.
- **Remote Access.** For more information, see Remote Access, page 26-5.
- **Packet Capture.** For more information, see Packet Capture, page 26-6.

**Open a Support Case**

You can use the appliance to send an email to IronPort Customer Support asking for assistance. When the appliance sends the email, it also sends the configuration of the appliance. You can do this in the following ways:

- **CLI.** Use the `supportrequest` command.
- **Web interface.** Use the Support and Help menu > Open a Support Case page.

When you send a support request, you can enter comments describing the issue for which you need support. The appliance must be able to send mail to the Internet to send a support request.

To send a support request in the web interface:

**Step 1**

From the Support and Help menu, choose Open a Support Case.
Figure 26-1  Open a Technical Support Case Page

Open a Technical Support Case

![Open a Technical Support Case](image)

Step 2 In the Other Recipients field, enter other email addresses separated by commas if you want to send this support request to other people.

By default, the support request (including the configuration file) is sent to IronPort Customer Support (via the checkbox at the top of the form).

Step 3 Enter your contact information, such as name and email.

Step 4 From the Issue Priority field, select the priority of this support request.

Step 5 In the Issue Subject field, enter the text to use in the subject line of the email that will be sent.

Step 6 In the Issue Description field, enter a description of the issue.

Step 7 If you have a customer support ticket already for this issue, enter it.

Step 8 Click Send.

A trouble ticket is automatically created with IronPort. For additional information, see Cisco IronPort Customer Support, page 1-15.
Remote Access

Use the Support and Help menu > Remote Access page to allow IronPort Customer Support remote access to the Web Security appliance. Click **Edit Remote Access Settings** to allow IronPort Customer Support to access the appliance.

**Figure 26-2 Remote Access Page**

By enabling Remote Access you are activating a special account used by IronPort Customer Support for debugging and general access to the system. This is used by IronPort Customer Support for tasks such as assisting customers in configuring their systems, understanding configurations, and investigating problem reports. You can also use the `techsupport` command in the CLI.

When enabling the “Secure Tunnel,” the appliance creates an SSH tunnel over the specified port to the server `upgrades.ironport.com`. By default this connection is over port 443, which will work in most environments. Once a connection is made to `upgrades.ironport.com`, IronPort Customer Support is able to use the SSH tunnel to obtain access to the appliance. As long as the connection over port 443 is allowed, this will bypass most firewall restrictions. You can also use the `techsupport tunnel` command in the CLI.

In both the “Remote Access” and “Tunnel” modes, a password is required. It is important to understand that this is not the password that will be used to access the system. Once that password and the system serial number are provided to your Customer Support representative, a password used to access the appliance is generated.

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. If there are any existing connections using the tunnel after 7 days, those connections will continue to exist and work. However, once those connections are closed, they will not be able to open again because the
Packet Capture

Sometimes when you contact IronPort Customer Support with an issue, you may be asked to provide insight into the network activity going into and out of the Web Security appliance. The appliance provides the ability to intercept and display TCP/IP and other packets being transmitted or received over the network to which the appliance is attached.

You might want to run a packet capture to debug the network setup and to discover what network traffic is reaching the appliance or leaving the appliance.

The appliance saves the captured packet activity to a file and stores the file locally. You can configure the maximum packet capture file size, how long to run the packet capture, and on which network interface to run the capture. You can also use a filter to limit the number of packets seen by the packet capture which can make the output more usable on networks with a high volume of traffic. You can send any stored packet capture file using FTP to IronPort Customer Support for debugging and troubleshooting purposes.
Support Commands

The Support and Help > Packet Capture page displays the list of complete packet capture files stored on the hard drive. When a packet capture is running, the web interface shows the status of the capture in progress by showing the current statistics, such as file size and time elapsed.

You can download the packet capture files using the Download button in the web interface, or by connecting to the appliance using FTP and retrieving them from the captures directory.

In the CLI, use the packetcapture command.

In the web interface, select the Packet Capture option under the Support and Help menu.

Note

The packet capture feature is similar to the Unix tcpdump command.

Starting a Packet Capture

To start a packet capture in the CLI, run the packetcapture > start command. If you need to stop a running packet capture, run the packetcapture > stop command.

To start a packet capture in the web interface, select the Packet Capture option under the Support and Help menu, and then click Start Capture. To stop a running capture, click Stop Capture.

Note

The web interface only displays packet captures started in the web interface, not from the CLI. Similarly, the CLI only displays the status of a current packet capture run started in the CLI.

Editing Packet Capture Settings

To edit the packet capture settings in the CLI, run the packetcapture > setup command.

To edit packet capture settings in the web interface, select the Packet Capture option under the Support and Help menu, and then click Edit Settings.
Table 26-1 describes the packet capture settings you can configure.

Table 26-1 Packet Capture Configuration Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture file size limit</td>
<td>The maximum file size for all packet capture files.</td>
</tr>
<tr>
<td>Capture duration</td>
<td>Choose how long to run the packet capture:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Run Capture Until File Size Limit Reached.</strong> The packet capture runs until the file size limit is reached.</td>
</tr>
</tbody>
</table>
|                         | • **Run Capture Until Time Elapsed Reaches.** The packet capture runs until the configured time has passed. You can enter the time in seconds (s), minutes (m), or hours (h). If you enter the amount of time without specifying the units, AsyncOS uses seconds by default.  
  **Note:** If the file reaches the maximum size limit before the entire time has elapsed, the existing file is deleted (the data is discarded) and a new file starts with the current packet capture data. |
|                         | • **Run Capture Indefinitely.** The packet capture runs until you manually stop it.  
  **Note:** If the file reaches the maximum size limit before you manually stop the packet capture, the existing file is deleted (the data is discarded) and a new file starts with the current packet capture data. |
| Network interface to capture | Select the network interface on which to run the packet capture.    |
| Filters                 | Choose whether or not to apply a filter to the packet capture to reduce the amount of data stored in the packet capture.  
  You can use one of the predefined filters to filter by port, source IP address, or destination IP address, or you can create a custom filter using any syntax supported by the Unix tcpdump command. |
### 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.

Figure 26-3 on page 9 shows where you can edit the packet capture settings in the web interface.

#### Figure 26-3  Editing Packet Capture Settings in the Web Interface

<table>
<thead>
<tr>
<th>Packet Capture Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture File Size Limit</td>
<td>200 MB (Maximum size is 200MB)</td>
</tr>
<tr>
<td>Capture Duration</td>
<td>Run Capture until File Size Limit Reached</td>
</tr>
<tr>
<td></td>
<td>Run Capture until Time Elapsed Minutes (e.g., 220s, 5m 30s, 4h)</td>
</tr>
<tr>
<td></td>
<td>Run Capture Indefinitely</td>
</tr>
</tbody>
</table>

- The capture can be ended manually at any time; use the settings above to specify whether the capture should end automatically.

<table>
<thead>
<tr>
<th>Interfaces</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>T1</td>
<td></td>
</tr>
<tr>
<td>T2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Packet Capture Filters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters: All filters are optional. Fields are not mandatory.</td>
<td></td>
</tr>
<tr>
<td>No Filters</td>
<td></td>
</tr>
<tr>
<td>Predefined Filters</td>
<td></td>
</tr>
<tr>
<td>Ports: 80,3025</td>
<td></td>
</tr>
<tr>
<td>Source IP:</td>
<td></td>
</tr>
<tr>
<td>Destination IP:</td>
<td></td>
</tr>
<tr>
<td>Custom Filter:</td>
<td></td>
</tr>
</tbody>
</table>
Working with Feature Keys

Occasionally, your support team may provide a key to enable specific functionality on your system. Use the System Administration > Feature Keys page in the web interface (or the featurekey command in the CLI) to enter the key and enable the associated functionality.

Keys are specific to the serial number of your appliance and specific to the feature being enabled (you cannot re-use a key from one system on another system). If you incorrectly enter a key, an error message is generated.

Feature keys functionality is split into two pages: Feature Keys and Feature Key Settings.

Feature Keys Page

The Feature Keys page:

- Lists all active feature keys for the appliance.
- Shows any feature keys that are pending activation.
- Looks for new keys that have been issued (optional, and also can install keys).

A list of the currently enabled features is displayed. The Pending Activation section is a list of feature keys that have been issued for the appliance but have not yet been activated. Your appliance may check periodically for new keys depending on your configuration. You can click Check for New Keys to refresh the list of pending keys.
You can also use the `featurekey` CLI command to accomplish the same tasks as on the Feature Keys page.

**Feature Key Settings Page**

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.

To add a new feature key manually, paste or type the key into the Feature Key field and click **Submit Key**. An error message is displayed if the feature is not added (if the key is incorrect, etc.), otherwise the feature key is added to the display.
To activate a new feature key from the Pending Activation list, select the key (mark the “Select” checkbox) and click **Activate Selected Keys**.

You can configure your IronPort 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.

You can also use the `featurekeyconfig` CLI command to accomplish the same tasks as on the Feature Key Settings page.

### Expired Feature Keys

If the feature key for the feature you are trying to access (via the web interface) has expired, please contact your IronPort representative or support organization.

### 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. For more information, see **Managing Local Users**, page 26-13.

- **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. For information, see **Using External Authentication**, page 26-17.

You can manage local users and connections to external authentication servers using the System Administration > Users page in the web interface, or the `userconfig` command in the CLI.

*Figure 26-6* shows where you manage local users and external authentication.
Any user you define can log into the appliance using any method, such as logging into the web interface or using SSH.

Managing Local Users

You can define any number users locally on the Web Security appliance. You can add, edit, and delete local users. Consider the following rules when defining local users:

- User names can contain lowercase letters, numbers, and the dash (-) character.
- User names cannot start with a dash.
- User names cannot be longer than 16 characters.
- Passwords must be at least 6 characters long.
- User names cannot be special names that are reserved by the system, such as "operator" or "root."

The default system admin account has all administrative privileges. You can change the admin account password, but you cannot edit or delete this account.
To create a new user account, specify a user name and a full name, and then assign
the user to a group. Each group provides a different level of default permissions.
Table 26-2 lists the groups you can assign.

Table 26-2  User Groups

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>The administrators group allows full access to all system configuration settings. However, the upgradecheck and upgradeinstall commands can be issued only from the system defined “admin” account.</td>
</tr>
</tbody>
</table>
| Operator  | The operators group restricts users from creating, editing, or removing user accounts. The operators group also restricts the use of the following commands:  
|           | • resetconfig                                                                 |
|           | • upgradecheck                                                                |
|           | • upgradeinstall                                                              |
|           | • systemsetup or running the System Setup Wizard                               |
| Guest     | The guests group users can only view system status information.                 |

After assigning the user to a group, you must specify a password for the new
account. Passwords are encrypted when they are reported using the showconfig
CLI command.

Note

If you have lost the admin user password, contact your support provider.

Adding Local Users

To add a local user:

Step 1  On the System Administration > Users page, click Add User.

The Add Local User page is displayed.
Figure 26-7  Adding a Local User

Add Local User

<table>
<thead>
<tr>
<th>Local User Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name:</td>
</tr>
<tr>
<td>Full Name:</td>
</tr>
<tr>
<td>User Type:</td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>Retype Password:</td>
</tr>
</tbody>
</table>

Step 2  Enter a name for the user. Some words are reserved, such as “operator” and “root”.
Step 3  Enter a full name for the user.
Step 4  Select a user type. See Table 26-2, `User Groups,' on page 14 for more information about user types.
Step 5  Enter a password and retype it.
Step 6  Submit and commit your changes.

Deleting Users

To delete a user:

Step 1  On the System Administration > Users page, click the trash can icon corresponding to the listed user name.
Step 2  Confirm the deletion by clicking Delete in the warning dialog that appears.
Step 3  Submit and commit your changes.

Editing Users

To edit a user:

Step 1  On the System Administration > Users page, click the user name.

The Edit User page is displayed.

Step 2  Make changes to the user.
Step 3  Submit and commit your changes.
Changing Passwords

Users can change their own passwords using the Change Password option under the Options menu located on the top right-hand side of the web interface. Figure 26-8 shows where you can change the current user password.

Figure 26-8  The Change Password Option

Note
To change the password for the admin account, use the System Administration > Users page or use the password or passwd command in the CLI. Password changes take effect immediately and do not require a commit.

Monitoring Users from the CLI

The who, whoami, and last commands can be used to monitor user access to the appliance.

- The who command lists users, the time of login, idle time, and the remote host from which the user is logged in:

```
example.com> who
Username Login Time Idle Time Remote Host What
========== ========= =========== =========== ====
admin 03:27PM  0s 10.xx.xx.xx cli
```
• The `whoami` command displays the user name and group information:

```
example.com> whoami
Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

• The `last` command displays information about users who have recently logged into the appliance.

```
example.com> last
Username  Remote Host  Login Time  Logout Time  Total Time
admin    10.xx.xx.xx  Sat May 15 23:42  still logged in  15m
admin    10.xx.xx.xx  Sat May 15 22:52  Sat May 15 23:42  50m
admin    10.xx.xx.xx  Sat May 15 11:02  Sat May 15 14:14  3h 12m
admin    10.xx.xx.xx  Fri May 14 16:29  Fri May 14 17:43  1h 13m
shutdown Fri May 14 16:22
```

## Using External Authentication

If you store user information in a RADIUS directory on your network, you can configure the Web Security appliance to use the RADIUS directory to authenticate users logging in to the appliance. You can use external authentication when logging into the appliance using HTTP, HTTPS, SSH, and FTP. To set up the appliance to use an external directory for authentication, use the System Administration > Users page in the web interface or the `userconfig > external` CLI command.
Administering User Accounts

Chapter 26  System Administration

Administering User Accounts

Figure 26-9 shows where you enable external authentication on the System Administration > Users page.

Figure 26-9  Enabling External Authentication

You can configure the appliance to contact multiple external servers for authentication. You might want to define multiple external servers to allow for failover in case one server is temporarily unavailable. When you define multiple external servers, the appliance connects to the servers in the order defined on the appliance.

When external authentication is enabled and a user logs into the Web Security appliance, the appliance first determines if the user is the system defined “admin” account. If not, then the appliance checks the first configured external server to determine if the user is defined there. If the appliance cannot connect to the first external server, the appliance checks the next external server in the list. If the user fails authentication on any external server, the appliance tries to authenticate the user as a local user defined on the Web Security appliance. If the user does not exist on any external server or on the appliance, or if the user enters the wrong password, access to the appliance is denied.

Consider the following rules and guidelines when using external authentication:

- AsyncOS for Web connects to the external server over the M1 interface only.
- The Web Security appliance assigns all users in the RADIUS directory to the administrator user group. You cannot assign users to other user groups. When external authentication is enabled and a user successfully authenticates as a local user, the local user has Administrator user group privileges regardless of the configured user type.
- Any user with a valid username and password in the RADIUS directory is granted full access as an administrator on the Web Security appliance. No authorization is performed on RADIUS users.

To enable external authentication using RADIUS:

Step 1  On the System Administration > Users page, click Enable.

The Edit External Authentication page is displayed.
Step 2  Enable the **Enable External Authentication** option if it is not enabled already.

*Figure 26-10  Enabling External Authentication Using RADIUS*

**Edit External Authentication**

<table>
<thead>
<tr>
<th>External Authentication Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable External Authentication</strong></td>
</tr>
<tr>
<td><strong>Authentication Type:</strong> RADIUS</td>
</tr>
<tr>
<td><strong>RADIUS Server Information:</strong></td>
</tr>
<tr>
<td><strong>RADIUS Server Hostname:</strong></td>
</tr>
<tr>
<td><strong>Port:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>External Authentication Cache Timeout:</strong> 0 seconds</td>
</tr>
<tr>
<td><strong>Group Mapping:</strong> Administrator</td>
</tr>
</tbody>
</table>

When RADIUS external authentication is enabled, all authenticated users map to the administrator role. This includes users that have been authenticated locally due to RADIUS failures.

Step 3  Enter the hostname for the RADIUS server.

Step 4  Enter the port number for the RADIUS server. The default port number is 1812.

Step 5  Enter the Shared Secret password for the RADIUS server.

Step 6  Enter the number of seconds for the appliance to wait for a response from the server before timing out.

Step 7  Optionally, click **Add Row** to add another RADIUS server. Repeat steps 3-6 for each RADIUS server.

*Note*  You can add up to ten RADIUS servers.

Step 8  Enter the number of seconds AsyncOS stores the external authentication credentials before contacting the RADIUS server again to authenticate again in the “External Authentication Cache Timeout” field. Default is zero (0).

*Note*  If the RADIUS server uses one-time passwords, for example passwords created from a token, enter zero (0). When the value is set to zero, AsyncOS does not contact the RADIUS server again to authenticate during the current session.

Step 9  Submit and commit your changes.
Configuring Administrator Settings

You can configure the Web Security appliance to have stricter access requirements for administrators logging into the appliance. You might want to do this to meet certain organization requirements.

You configure these settings with the `adminaccessconfig` CLI command. You can configure the appliance to:

- Display user-defined text at administrator login.
- Restrict administrator access to certain machines.
- Require stronger SSL ciphers for administrator access.

Configuring Custom Text at Login

Using the `adminaccessconfig > banner` CLI command, you can configure the appliance to display any text you specify when an administrator tries to logs in. You might want to do this to display a banner that informs the user of organizational policies and conditions. The custom banner text appears when an administrator tries to access the appliance through all interfaces, such as the web interface or via FTP.

You can load the custom text by either pasting it into the CLI prompt or by copying it from a file located on the Web Security appliance. To upload the text from a file, you must first transfer the file to the configuration directory on the appliance using FTP.

Configuring IP-Based Administrator Access

Using the `adminaccessconfig > ipaccess` CLI command, you can control from which IP addresses administrators access the Web Security appliance. Administrators can access the appliance from any machine or from machines with an IP address from a list you specify.

When restrict access to an allow list, you can specify IP addresses, subnets, or CIDR addresses.
By default, when you list the addresses that can access the appliance, the IP address of your current machine is listed as the first address in the allow list. You cannot delete the IP address of your current machine from the allow list.

### Configuring the SSL Ciphers for Administrator Access

Using the `adminaccessconfig > strictssl` CLI command, you can configure the appliance so administrators log into the web interface on port 8443 using stronger SSL ciphers (greater than 56 bit encryption).

When you configure the appliance to require stronger SSL ciphers, the change only applies to administrators accessing the appliance using HTTPS to manage the appliance. It does not apply to other network traffic connected to the Web Proxy using HTTPS.

### Configuring the Return Address for Generated Messages

You can configure the return address for mail generated by AsyncOS for reports. You can specify the display, user, and domain names of the return address. You can also choose to use the Virtual Gateway domain for the domain name.

Configure the return address on the System Administration > Return Addresses page.

![Configuring Return Addresses](image)

To configure the return address for system-generated email messages:

**Step 1** Navigate to the System Administration > Return Addresses page.

**Step 2** Click Edit Settings.
Managing Alerts

Alerts are email notifications containing information about events occurring on the IronPort 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. Alerts are generated by the IronPort appliance. You can specify which alert messages are sent to which users and for which severity of event they are sent. Manage alerts using the System Administration > Alerts page in the web interface or using the `alertconfig` command in the CLI.

Note

To receive alerts and email notifications, you must configure the SMTP relay host that the appliance uses to send the email messages. For information about configuring the SMTP relay host, see Configuring SMTP Relay Hosts, page 25-26.

Alerting Overview

The alerting feature consists of two main parts:

- **Alerts** - consist of an Alert **Recipient** (email addresses for receiving alerts), and the alert notification (severity and alert type) sent to the recipient.
• **Alert Settings** - specify global behavior for the alerting feature, including alert sender (FROM:) address, seconds to wait between sending duplicate alerts, and whether to enable AutoSupport (and optionally send weekly AutoSupport reports).

### Alerts: Alert Recipients, Alert Classifications, and Severities

Alerts are email messages or notifications containing information about a specific function (or alert classification) or functions such as a hardware or anti-virus problem, sent to an alert recipient. An alert recipient is simply an email address to which the alert notifications are sent. The information contained in the notification is determined by an alert classification and a severity. You can specify which alert classifications, at which severity, are sent to any alert recipient. The alerting engine allows for granular control over which alerts are sent to which alert recipients. For example, you can configure the system to send only specific alerts to an alert recipient, configuring an alert recipient to receive notifications only when Critical (severity) information about the System (alert type) is sent. You can also configure general settings (see Configuring Alert Settings, page 26-29).

### Alert Classifications

AsyncOS sends the following alert classifications:

<table>
<thead>
<tr>
<th>Alert Classification</th>
<th>Alert Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>System</td>
</tr>
<tr>
<td>Hardware</td>
<td>Hardware</td>
</tr>
<tr>
<td>Updater</td>
<td>Updater</td>
</tr>
<tr>
<td>Web Proxy</td>
<td>Proxy</td>
</tr>
<tr>
<td>DVSTM and Anti-Malware</td>
<td>DVS</td>
</tr>
<tr>
<td>L4 Traffic Monitor</td>
<td>TrafMon</td>
</tr>
</tbody>
</table>

### 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.

**Alert Settings**

Alert settings control the general behavior and configuration of alerts, including:

- The RFC 2822 Header From: when sending alerts (enter an address or use the default “alert@<hostname>”). You can also set this via the CLI, using the `alertconfig -> from` command.
- The initial number of seconds to wait before sending a duplicate alert.
- The maximum number of seconds to wait before sending a duplicate alert.
- The status of AutoSupport (enabled or disabled).
- The sending of AutoSupport’s weekly status reports to alert recipients set to receive System alerts at the Information level.

**Sending Duplicate Alerts**

You can specify the initial number of seconds to wait before AsyncOS will send a duplicate alert. If you set this value to 0, duplicate alert summaries are not sent and instead, all duplicate alerts are sent without any delay (this can lead to a large amount of email over a short amount of time). The number of seconds to wait between sending duplicate alerts (alert interval) is increased after each alert is sent. The increase is the number of seconds to wait plus twice the last interval. So a 5 second wait would have alerts sent at 5 seconds, 15 seconds, 35 seconds, 75 seconds, 155 seconds, 315 seconds, etc.

Eventually, the interval could become quite large. 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.
IronPort AutoSupport

To allow IronPort to better support and design future system changes, the IronPort appliance can be configured to send IronPort Systems a copy of all alert messages generated by the system. This feature, called AutoSupport, is a useful way to allow our team to be proactive in supporting your needs. AutoSupport also sends weekly reports noting the uptime of the system, the output of the `status` command, and the AsyncOS version used.

By default, alert recipients set to receive Information severity level alerts for System alert types will receive a copy of every message sent to IronPort. This can be disabled if you do not want to send the weekly alert messages internally. To enable or disable this feature, see Configuring Alert Settings, page 26-29.

Alert Messages

Alert messages are standard email messages. You can configure the Header From: address, but the rest of the message is generated automatically.

Alert From Address

You can configure the Header From: address via the Edit Settings... button or via the CLI.

Alert Subject

An alert email message's subject follows this format:

```
Subject: [severity]-[hostname]: ([class]) short message
```
Example Alert Message

Date: 23 May 2007 21:10:19 +0000

To: joe@example.com

From: IronPort S650 Alert [alert@example.com]

Subject: Critical <System> example.com: Internal SMTP giving up on message to jane@company.com with...

The Critical message is:

Internal SMTP giving up on message to jane@company.com with subject 'IronPort Report: Client Web Activity (example.com)’: Unrecoverable error.

Product: IronPort S650 Web Security Appliance

Model: S650

Version: 5.1.0-225

Serial Number: XXXXXXXXXXXX-XXXXXXX

Timestamp: Tue May 10 09:39:24 2007

For more information about this error, please see

http://support.ironport.com

If you desire further information, please contact your support provider.
Managing Alert Recipients

Log in to the S-Series appliance web interface (GUI) and click the System Administration tab. Click the Alerts link in the left menu. For information about how to access the S-Series appliance web interface, see Accessing the Web Security Appliance, page 2-3.

Figure 26-13 The Alerts Page

The Alerts page lists the existing alert recipients and alert settings.

From the Alerts page, you can:

- Add, configure, or delete alert recipients
- Modify the alert settings

Adding New Alert Recipients

To add a new alert recipient:

Step 1 Click Add Recipient... on the Alerts page. The Add Alert Recipients page is displayed:
## Managing Alerts

**Figure 26-14      Adding a New Alert Recipient**

Add Alert Recipient

<table>
<thead>
<tr>
<th>Alert Recipient</th>
<th>Recipient Address</th>
<th>Alert Severities to Receive</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>Hardware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Updater</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Proxy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DDoS and Anti-Malware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lo Traffic Monitor</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 2** Enter the recipient’s email address. You can enter multiple addresses, separated by commas.

**Step 3** Select which alert severities to receive.

**Step 4** Click **Submit** to add the alert recipient.

**Step 5** Click the **Commit Changes** button, add an optional comment if necessary, then click **Commit Changes** to save the changes.

### Configuring Existing Alert Recipients

To edit an existing alert recipient:

**Step 1** Click the alert recipient in the Alert Recipients listing. The Configure Alert Recipient page is displayed.

**Step 2** Make changes to the alert recipient.

**Step 3** Click **Submit** to edit the alert recipient.

**Step 4** Click the **Commit Changes** button, add an optional comment if necessary, then click **Commit Changes** to save the changes.

### Deleting Alert Recipients

To delete an alert recipient:
Managing Alerts

**Step 1** Click the trash can icon corresponding to the alert recipient in the Alert Recipient listing.

**Step 2** Confirm the deletion by clicking Delete in the warning dialog that appears.

**Step 3** Click the Commit Changes button, add an optional comment if necessary, then click Commit Changes to save the changes.

### Configuring Alert Settings

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

### Editing Alert Settings

To edit alert settings:

**Step 1** Click Edit Settings... on the Alerts page. The Edit Alert Settings page is displayed:

**Figure 26-15 Editing Alert Settings**

![Editing Alert Settings](image)

**Step 2** Enter a Header From: address to use when sending alerts, or select Automatically Generated (“alert@<hostname>”).

**Step 3** Mark the checkbox if you want to specify the number of seconds to wait between sending duplicate alerts. For more information, see Sending Duplicate Alerts, page 26-24.
Setting System Time

To set the system time on your Web Security appliance, set the time zone used, or select an NTP server and query interface. To set the system time, use the System Administration > Time Zone or Time Settings page or use the `ntpconfig`, `settime`, and `settz` commands.

Selecting a Time Zone

To set the time zone use the System Administration > Time Zone page:

**Figure 26-16 The Time Zone Page**

<table>
<thead>
<tr>
<th>Time Zone Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone</td>
</tr>
<tr>
<td>Country:</td>
</tr>
<tr>
<td>Time Zone:</td>
</tr>
</tbody>
</table>

Select a time zone in the Time Zone area. You can configure the time zone by specifying the region and country, or by using a GMT offset.
Chapter 26  System Administration

Setting System Time

The web interface uses the POSIX-style method of indicating the time zone using a GMT offset. This may be different than the offset convention used elsewhere. The offset refers to the amount of hours that must be added or subtracted to the local time zone in order to reach GMT (Greenwich Mean Time or the Prime Meridian). Hours preceded by a minus sign ("- ") are east of the Prime Meridian. A plus sign ("+") indicates west of the Prime Meridian.

For example, if the current time in New York is 08:00, then you must add five hours to get the current time in Greenwich, England, which is 13:00. In this case, to indicate the time in New York, the GMT offset is GMT+5. The "+5" in the offset indicates that you must add five hours to the time in New York to reach Greenwich Mean Time.

Editing System Time

To edit system time, use the System Administration > Time Settings page.

Configure NTP (Network Time Protocol)

To edit NTP server settings and use an NTP server to synchronize the system clock with other computers:

Step 1  Enter an NTP server IP address and use the Add Row key to repeat as necessary for each NTP server.
Step 2  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.

Step 3  Submit and commit the changes.

**Manually Setting System Time**

To set the system time manually:

---

Step 1  Select Set Time Manually.

Step 2  Enter the month, day, year, hour, minutes, and seconds.

Step 3  Select A.M or P.M.

Step 4  Submit and commit to save the changes.

**Installing a Server Digital Certificate**

When an administrator logs into the Web Security appliance using HTTPS, the appliance uses a digital certificate to securely establish the connection with the client application. The Web Security appliance uses the “IronPort Appliance Demo Certificate” that comes installed by default. However, client applications are not programmed to recognize this certificate, so you can upload a digital certificate to the appliance that your applications recognize automatically.

**Figure 26-18** shows the warning message that is displayed in Firefox when accessing the Web Security appliance using the IronPort Appliance Demo Certificate.
Figure 26-18  IronPort Appliance Demo Certificate as an Unknown Authority

To configure the Web Security appliance to use a different digital server certificate, follow these steps:

Step 1 Obtain a certificate and private key pair to upload. For more information, see Obtaining Certificates, page 26-33.

Step 2 Upload the certificate and private key pair to the appliance. For more information, see Uploading Certificates to the Web Security Appliance, page 26-35.

Obtaining Certificates

To obtain a digital certificate to upload to the appliance, you must follow these steps:

Step 1 Generate a public-private key pair.
Step 2 Generate a Certificate Signing Requests (CSR).
Step 3 Contact a certificate authority (CA) to sign the certificate.

The certificate you upload to the appliance must meet the following requirements:

- It must use the X.509 standard.
Installing a Server Digital Certificate

- It must include a matching private key in PEM format. DER format is not supported.
- The private key must be unencrypted.

The Web Security appliance cannot generate Certificate Signing Requests (CSR). Therefore, to have a certificate created for the appliance, you must issue the signing request from another system. Save the PEM-formatted key from this system because you will need to install it on the appliance later.

You can use any UNIX machine with a recent version of OpenSSL installed. Be sure to put the appliance hostname in the CSR. Use the guidelines at the following location for information on generating a CSR using OpenSSL:

http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28

Once the CSR has been generated, submit it to a certificate authority (CA). The CA will return the certificate in PEM format.

If you are acquiring a certificate for the first time, search the Internet for “certificate authority services SSL server certificates,” and choose the service that best meets the needs of your organization. Follow the service’s instructions for obtaining an SSL certificate.

Note

You can also generate and sign your own certificate. Tools for doing this are included with OpenSSL, free software from http://www.openssl.org.

Intermediate Certificates

In addition to root certificate authority (CA) certificate verification, AsyncOS supports the use of intermediate certificate verification. Intermediate certificates are certificates issued by a trusted root CA which are then used to create additional certificates. This creates a chained line of trust. For example, a certificate may be issued by example.com who, in turn, is granted the rights to issue certificates by a trusted root CA. The certificate issued by example.com must be validated against example.com’s private key as well as the trusted root CA’s private key.
Uploading Certificates to the Web Security Appliance

To upload a digital certificate to the Web Security appliance, use the `certconfig` command.

The following example shows a certificate being uploaded. You can also add intermediate certificates from this command.

```
example.com> certconfig
```

Currently using the demo certificate/key for HTTPS management access.

Choose the operation you want to perform:

- SETUP - Configure security certificate and key.

```
[*]> setup
```

Management (HTTPS):

paste cert in PEM format (end with '.'): 

```
-----BEGIN CERTIFICATE-----
MIICLDCCAgYCAQAwDQYJKoZIhvcNAQEEBQAwgaAxCzAJBgNVBAYTAlBUMRMwEQYDVQQIEwpRdWVlbnNsYW5kMQ8wDQYDVQQKEwZMaXNlbnZvcm1hb2UxETczPINyZXR0aWN1c3MuY2VydFMBAAAwFgYDVQQDEw5EZXNlbnZvbHZpbWVudG9iZSBMaXNlbnZvcm1hb2UxETczPINyZXR0aWN1c3MuY2VydFMBAAAwCAAwHwYDVR0PEBQAwgAAMBAGC5GMIEzCANBMAowIwYDVR0TAQawIwYDVR0SAQIjAfBgNVBAsTAE1ldHJ1c3QgQ29udGFpbiB0ZXh0IEdlbGFuZ3V0cyBjbGFzczEvMCgGCCsGAQUFBwIwHhcNMTMwMDI0MjUyMjIwNHowMDAweDh0bDggMjYwTVBd

-----END CERTIFICATE-----
```

Cisco IronPort AsyncOS 7.1 for Web User Guide
Installing a Server Digital Certificate

```
-----BEGIN CERTIFICATE-----

MFAwDQYJKoZIhvcNAQEBBDADAQRSA9+mN11LqG2vGf3SWGvJY5s92xgOgH/87i
GKjJ7T4VfjQ7L657XG3lS3v6bXZyD+Jk+/8fS8Xg3+Pn

-----END CERTIFICATE-----
```

```
paste key in PEM format (end with "."): 

-----BEGIN RSA PRIVATE KEY-----

MIIBPAIBAAJBAL7+aty3S1iBA/+yxjxv4qlMUtd1k\nk
L4LYkpzz1mC5beaqXeQ2RmGMTXU+mdVugttjVHDR3DV
PK71TC5GftUCAwEAATAN

-----END RSA PRIVATE KEY-----
```

```
Do you want add an intermediate certificate? [N]>

N

Currently using custom certificate/key for HTTPS management access.

Choose the operation you want to perform:

```
- SETUP - Configure security certificate and key.
```

```
example.com>
```

```
commit
```

```
Please enter some comments describing your changes:

[>] Installed certificate and key for HTTPS management.

Do you want add an intermediate certificate? [N]>

N

Changes committed: Fri Sep 26 17:59:53 2008 GMT
```
Chapter 26

System Administration
Installing a Server Digital Certificate

Management (HTTPS):
paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE----MIICLDCCAdYCAQAwDQYJKoZIhvcNAQEEBQAwgaAxCzAJBgNVBAYTAlBUMRMwEQYD
VQQIEwpRdWVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNib2ExFzAVBgNVBAoTDk5ldXJv
bmlvLCBMZGEuMRgwFgYDVQQLEw9EZXNlbnZvbHZpbWVudG8xGzAZBgNVBAMTEmJy
dXR1cy5uZXVyb25pby5wdDEbMBkGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZpMB4X
DTk2MDkwNTAzNDI0M1oXDTk2MTAwNTAzNDI0M1owgaAxCzAJBgNVBAYTAlBUMRMw
EQYDVQQIEwpRdWVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNib2ExFzAVBgNVBAoTDk5l
dXJvbmlvLCBMZGEuMRgwFgYDVQQLEw9EZXNlbnZvbHZpbWVudG8xGzAZBgNVBAMT

Cisco IronPort AsyncOS 7.1 for Web User Guide
OL-23207-01

26-37


Installing a Server Digital Certificate

Management (HTTPS):

paste cert in PEM format (end with "."): 

-----BEGIN CERTIFICATE-----
MIICLDCCAdYCAQAwDQYJKoZIhvcNAQEEBQAwgaAxCzAJBgAJBgNVBAYTAlBUMRMwEQYDVQQIEwpRdWV1bnNsbW5kMQ8wDQYDVQQHEwZMaXNiIb2ExFzAVBgNVBAoTDk5ldXJvbmlvLCBMZGEuMRgwFgYDVQQLEw9EZXN1bnZvbHVzdG9tYWluGExGczAZBgNVBAMTEmJydXR1cy5uZXVyb25pby5wdDEbMBkGCCsGAQUFBwEBBjQwFwYDVQQKEwZMaXNiIb2ExFzAVBgNVBAMT

-----END CERTIFICATE-----
Currently using custom certificate/key for HTTPS management access.

Choose the operation you want to perform:

oudmkNziSRTYjnwjx8mCoA/JWviB3c742eO3FG4/soi1jD9A5alihEOXfUzloenr

Do you want add an intermediate certificate? [N]> N

Changes committed: Fri Sep 26 17:59:53 2008 GMT
Upgrading the System Software

Upgrading AsyncOS for Web uses the following two step process:

Step 1  Configure the update and upgrade settings. You can configure settings that affect how the Web Security appliance downloads the upgrade information. For example, you can choose from where to download the upgrade images and more. For more information, see Configuring Upgrade and Service Update Settings, page 26-42.

Step 2  Upgrade the system software. After you configure the update and upgrade settings, upgrade the software on the appliance. For more information, see Upgrading AsyncOS for Web from the Web Interface, page 26-40 and Upgrading AsyncOS for Web from the CLI, page 26-41.

Consider the following guidelines when you upgrade AsyncOS for Web:

- Before you start the upgrade, save the XML configuration file off the Web Security appliance from the System Administration > Configuration File page or by using the `saveconfig` command. For more information, see Saving and Loading the Appliance Configuration, page 26-2.
- When upgrading, do not pause for long amounts of time at the various prompts. If the TCP session times out during the download, the upgrade may fail.
- Consider saving the configuration information to an XML file after the upgrade completes, too.

Upgrading AsyncOS for Web from the Web Interface

To upgrade AsyncOS after you configure the update and upgrade settings:

Step 1  On the System Administration > Configuration File page, save the XML configuration file off the Web Security appliance.

Step 2  On the System Administration > System Upgrade page, click Available Upgrades.

The Available Upgrades page is displayed.
Chapter 26  System Administration

Upgrading the System Software

Figure 26-19  The Available Upgrades Page

Available Upgrades

Step 3  Select an upgrade from the list of available upgrades, and click Begin Upgrade to start the upgrade process. Answer the questions as they appear.

Step 4  When the upgrade is complete, click Reboot Now to reboot the Web Security appliance.

Upgrading AsyncOS for Web from the CLI

Issue the upgrade command from the CLI to show a list of available upgrades. Select the desired upgrade from the list to install it. You may be asked to confirm messages or read and agree to license agreements, etc.

Differences from Traditional Upgrading Method

Please note these differences when upgrading AsyncOS from a local server as opposed to the traditional method:

Step 1  The upgrading installs immediately while downloading.

Step 2  A banner displays for 10 seconds at the beginning of the upgrade process. While this banner is displayed, you have the option to type Control+C to exit the upgrade process before downloading starts.
Configuring Upgrade and Service Update Settings

You can configure how the Web Security appliance downloads security services updates, such as Web Reputation Filters and AsyncOS for Web upgrades. For example, you can choose which network interface to use when downloading the files, configure the update interval, or disable automatic updates.

AsyncOS periodically queries the update servers for new updates to all security service components, but not for new AsyncOS upgrades. To upgrade AsyncOS, you must manually prompt AsyncOS to query for available upgrades. You can also manually prompt AsyncOS to query for available security service updates. For more information, see Manually Updating Security Service Components, page 26-51.

When AsyncOS queries an update server for an update or upgrade, it performs the following steps:

1. Contacts the update server.

   IronPort allows the following sources for update servers:

   - **IronPort update servers.** For more information, see Updating and Upgrading from the IronPort Update Servers, page 26-43.
   - **Local server.** For more information, see Upgrading from a Local Server, page 26-44.

2. Receives an XML file that lists the available updates or AsyncOS upgrade versions. This XML file is known as the “manifest.”

3. Downloads the update or upgrade image files.

   By default, AsyncOS contacts the IronPort update servers for both update and upgrade images and the manifest XML file. However, you can choose from where to download the upgrade and update images and the manifest file. You might want to specify a local update server for the images or manifest file for any of the following reasons:

   - **You have multiple appliances to upgrade simultaneously.** If your organization has multiple Web Security appliances that need to upgrade, you can download the upgrade image to a web server inside your network and serve it to all appliances in your network.
Your firewall settings require static IP addresses for the IronPort update servers. The IronPort update servers use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location for updates and AsyncOS upgrades. For more information, see Configuring a Static Address for the IronPort Update Servers, page 26-44.

Note

Only use a local update server for upgrade images, not update images. When you specify a local update server, the local server does not automatically receive updated security service updates from IronPort, so the appliances in your network eventually become out of date. Use a local update server for upgrading AsyncOS, and then change the update and upgrade settings back to use the IronPort update servers so the security services update automatically again.

You can configure upgrade and updates settings in the web interface or the CLI. For more information, see Configuring the Update and Upgrade Settings from the Web Interface, page 26-46 and Configuring the Update and Upgrade Settings from the CLI, page 26-51.

Figure 26-20 shows where you configure upgrade and update settings in the web interface.

Figure 26-20  System Administration > Upgrade and Update Settings Page

Updating and Upgrading from the IronPort Update Servers

The Web Security appliance can connect directly to the IronPort update servers and download upgrade images and security service updates. Each IronPort appliance downloads the updates and upgrade images separately.
IronPort Systems uses a distributed update server architecture to make sure customers can quickly download updates and AsyncOS upgrades wherever in the world they are located. Because of this distributed server architecture, the IronPort update servers use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location for AsyncOS upgrades. For more information, see Configuring a Static Address for the IronPort Update Servers, page 26-44.

**Configuring a Static Address for the IronPort Update Servers**

The IronPort update servers use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location for updates and AsyncOS upgrades. If you determine that your firewall settings require a static IP address for updates, complete the following steps:

**Step 1** Contact IronPort Customer support to obtain the static URL address.

**Step 2** Navigate to the System Administration > Upgrade and Update Settings page, and click **Edit Update Settings**.

**Step 3** On the Edit Update Settings page, in the “Update Servers (images)” section, choose Local Update Servers and enter the static URL address received in step 1.

**Step 4** Verify that IronPort Update Servers is selected for the “Update Servers (list)” section.

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

**Upgrading from a Local Server**

The Web Security appliance can download AsyncOS upgrades from a server within your network instead of obtaining upgrades directly from the IronPort update servers. When you use this feature, you only download the upgrade image from IronPort one time, and then serve it to all Web Security appliances in your network.

*Figure 26-21* shows how Web Security appliances download upgrade images from local servers.
To upgrade from a local server, perform the following steps:

**Step 1** Configure a local server to retrieve and serve the upgrade files.

**Step 2** Download the upgrade zip file.

Using a browser on the local server, go to http://updates.ironport.com/fetch_manifest.html to download a zip file of an upgrade image. To download the image, enter your serial number and the version number of the IronPort appliance. You will then be presented with a list of available upgrades. Click on the upgrade version that you want to download.

**Step 3** Unzip the zip file in the root directory on the local server while keeping the directory structure intact.

**Step 4** Configure the appliance to use the local server using the System Administration > Upgrade and Update Settings page or the updateconfig command.

**Step 5** On the System Administration > System Upgrade page, click Available Upgrades or run the upgrade command.
Cisco recommends changing the update and upgrade settings to use the IronPort update servers (using dynamic or static addresses) after the upgrade is complete to ensure the security service components continue to update automatically.

### Hardware and Software Requirements for Local Upgrade Servers

For **downloading** AsyncOS upgrade files, you must have a system in your internal network that has a web browser (see **Browser Requirements**, page 2-10) and Internet access to the IronPort Systems update servers.

**Note**

If you need to configure a firewall setting to allow HTTP access to this address, you must configure it using the DNS name and not a specific IP address.

For **hosting** AsyncOS upgrade files, a server on the internal network must have a web server, such as Microsoft IIS (Internet Information Services) or the Apache open source server, which has the following features:

- Supports the display of directory or filenames in excess of 24 characters.
- Has directory browsing enabled.
- Is configured for anonymous (no authentication) or Basic (“simple”) authentication.
- Contains at least 350MB of free disk space for each AsyncOS upgrade image.

### Configuring the Update and Upgrade Settings from the Web Interface

To edit the AsyncOS update and upgrade settings:

**Step 1** Navigate to the System Administration > Upgrade and Update Settings page, and click **Edit Update Settings**. The Edit Update Settings page is displayed.

**Figure 26-22** on page 47 shows the options you can configure on the Edit Update Settings page.
### Figure 26-22  Edit Update Settings Page

#### Edit Update Settings

<table>
<thead>
<tr>
<th>Update Settings for Security Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update Servers (XML):</strong></td>
</tr>
<tr>
<td>The XML will be used to obtain the list of available updates for the following services:</td>
</tr>
<tr>
<td>- Web Reputation Engine and Rules</td>
</tr>
<tr>
<td>- URL Engine</td>
</tr>
<tr>
<td>- WebCore</td>
</tr>
<tr>
<td>- LE Traffic Monitor</td>
</tr>
<tr>
<td>- Dynamic URL Filters</td>
</tr>
<tr>
<td>- Cisco IronPort Web Usage Controls</td>
</tr>
<tr>
<td>- IronPort AsyncOS upgrades</td>
</tr>
<tr>
<td><strong>IronPort Update Servers</strong></td>
</tr>
<tr>
<td><strong>Local Update Servers</strong> (location of list of available updates file)</td>
</tr>
<tr>
<td>Full list: <a href="http://updates.example.com/irsp_updates.xml">http://updates.example.com/irsp_updates.xml</a></td>
</tr>
<tr>
<td>Authentication (optional):</td>
</tr>
<tr>
<td>Username:</td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>Retype Password:</td>
</tr>
</tbody>
</table>

| Update Servers (Images):           |
| The update servers will be used to obtain update images for the following services: |
| - Web Reputation Engine and Rules  |
| - URL Engine                        |
| - WebCore                          |
| - LE Traffic Monitor               |
| - Dynamic URL Filters              |
| - Cisco IronPort Web Usage Controls |
| - IronPort AsyncOS upgrades        |
| **Same as defined in Update Servers (list):** |
| **Local Update Servers** (location of update image file):  |
| Base URL: [http://updates.example.com](http://updates.example.com)  |
| [http://updates.example.com](http://updates.example.com)          |
| Authentication (optional):         |
| Username:                          |
| Password:                          |
| Retype Password:                   |

| Automatic Updates: **Enable automatic updates (not including IronPort AsyncOS):** |
| Update Interval: 5m |

**Routing Table:**
*Management*

| **Proxy Server (optional):** |
| If an HTTP proxy server is defined it will be used to update the following services: |
| - Web Reputation Engine and Rules |
| - URL Engine                        |
| - WebCore                          |
| - LE Traffic Monitor               |
| - Dynamic URL Filters              |
| - Cisco IronPort Web Usage Controls |
| - IronPort AsyncOS upgrades        |
| **Proxy Server:**                  |
| Port: 800 |
| Username:                          |
| Password:                          |
| Retype Password:                   |

*Support basic authentication only:*
Step 2 Configure the settings in Table 26-4.
### Table 26-4  Update and Upgrade Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Servers (list)</td>
<td>Choose whether to download the list of available upgrades and updates (the manifest XML file) from the IronPort update servers or a local web server. The default is the IronPort update servers. You might want to choose a local web server when you want to temporarily download an upgrade image stored on a local web server. After you download the image, Cisco recommends changing this setting back to the IronPort update servers so that security components continue to update automatically. When you choose a local update server, enter the full path to the manifest XML file for the list including the file name and port number for the server. If you leave the port field blank, AsyncOS uses port 80. If the server requires authentication, you can also enter a valid user name and password. For more information, see Upgrading from a Local Server, page 26-44.</td>
</tr>
</tbody>
</table>
Step 3
Submit and commit your changes.
Configuring the Update and Upgrade Settings from the CLI

The `updateconfig` command is used to configure update and upgrade settings, such as where the appliance looks for service updates and AsyncOS upgrades. The settings you configure using the `updateconfig` command are the same as you can define in the web interface. For more information on these settings, see Table 26-4 on page 49.

**Note**
You can use the `ping` command to ensure that the appliance can contact the local server. You can also use the `telnet` CLI command to telnet to port 80 of the local server to ensure the local server is listening on that port.

Manually Updating Security Service Components

By default, each security service component periodically receives updates to its database tables from the IronPort update servers. However, you can manually update the database tables.

Typically, you do not need to manually update to the database tables. In the event a manual update is required, you can modify default settings and configure an update using the options on the System Administration > Upgrade and Update Settings page.

To configure a manual update:

**Step 1** Navigate to the System Administration > Upgrade and Update Settings page.

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

The Edit Update Settings page appears.

**Step 3** Receive the update files from IronPort and install them on a local server.

**Step 4** Specify the location of the update files.

**Step 5** Initiate the update using the Update Now function key on the component page located on the Security Services tab. For example, Security Services > Web Reputation Filters page.

**Step 6** View a record of update activity in the updater log file. Subscribe to the updater log file on the System Administration > Log Subscriptions page.
Updates that are in-progress cannot be interrupted. All in-progress updates must complete before new changes can be applied.
This chapter contains the following information:

- The Command Line Interface Overview, page 27-1
- Using the Command Line Interface, page 27-1
- General Purpose CLI Commands, page 27-6
- Web Security Appliance CLI Commands, page 27-8

The Command Line Interface Overview

The IronPort AsyncOS Command Line Interface (CLI) is an interactive interface designed to allow you to configure and monitor the Web Security appliance. 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.

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.

Using the Command Line Interface

This section describes the rules and conventions of the AsyncOS Command Line Interface.
Accessing the Command Line Interface

Access to the CLI varies depending on the management connection method chosen while setting up the appliance. The factory default username and password are listed next. Initially, only the admin user account has access to the CLI. You can add other users with differing levels of permission after you have accessed the CLI for the first time using the admin account. The System Setup Wizard prompts you to change the password for the admin account.

You can also reset the admin account password at any time using the `passwd` command.

You can connect using one of the following methods:

- **Ethernet.** Start an SSH session with the IP address of the Web Security appliance. The factory default IP address is 192.168.42.42. SSH is configured to use port 22.

- **Serial connection.** Start a terminal session with the communication port on your personal computer that the serial cable is connected to.

Log in to the appliance by entering the username and password below.

- Username: `admin`
- Password: `ironport`

For example:

```text
login: admin
password: ironport
```

Working with the Command Prompt

The top-level command prompt consists of the fully qualified hostname, followed by the greater than (>) symbol, followed by a space. For example:

```text
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:
```
Using the Command Line Interface

Chapter 27      Command Line Interface

- 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 IronPort AsyncOS CLI supports command completion. You can enter the first few letters of some commands followed by the Tab key and the CLI completes the string. If the letters you entered are not unique among commands, the CLI “narrows” the set. For example:

example.com> set (type the Tab key)
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth (typing the Tab again completes the entry with sethostname)
Configuration Changes

You can make configuration changes while web operations proceed normally. Configuration changes do not take effect until you complete the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Issue the commit command at the command prompt.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Give the commit command the input required.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Receive confirmation of the commit procedure at the CLI.</td>
</tr>
</tbody>
</table>

Changes to configuration that have not been committed are recorded, but do not go into effect until you run the commit command. However, not all commands require the commit command to be run.

Exiting the CLI session, system shutdown, reboot, failure, or issuing the clear command clears changes that have not yet been committed.

General Purpose CLI Commands

This section describes the some basic commands you might use in a typical CLI session, such as committing and clearing changes. For a full list of commands, see Web Security Appliance CLI Commands, page 27-8.

Committing Configuration Changes

The commit command allows you to change configuration settings while other operations proceed normally. Changes are not actually committed until you receive confirmation and a timestamp. Exiting the CLI session, system shutdown, reboot, failure, or issuing the clear command clears changes that have not yet been committed.

Entering comments after the commit command is optional.

```
example.com> commit
```

Please enter some comments describing your changes:
Chapter 27    Command Line Interface

General Purpose CLI Commands

Note
To successfully commit changes, you must be at the top-level command prompt. Type Return at an empty prompt to move up one level in the command line hierarchy.

Clearing Configuration Changes

The clear command clears any changes made to the appliance configuration since the last commit or clear command was issued.

example.com> clear

Are you sure you want to clear all changes since the last commit? [Y]> y

Changes cleared: Wed Jan 01 12:00:01 2007

example.com>

Exiting the Command Line Interface Session

The exit command logs you out of the CLI application. Configuration changes that have not been committed are cleared.

example.com> exit

Configuration changes entered but not committed. Exiting will lose changes.

Type 'commit' at the command prompt to commit changes.

Are you sure you wish to exit? [N]> y
Seeking Help on the Command Line Interface

The `help` command lists all available CLI commands and gives a brief description of each command. The `help` command can be invoked by typing either `help` or a single question mark (?) at the command prompt.

```
example.com> help
```

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.

Table 27-1 lists the Web Security appliance Command Line Interface commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| advancedproxyconfig | Configure more advanced Web Proxy configurations, such as authentication and DNS parameters.  
                        | For more information about the `advancedproxyconfig` command, see Advanced Proxy Configuration, page 5-30. |
| adminaccessconfig   | You can configure the Web Security appliance to have stricter access requirements for administrators logging into the appliance.  
                        | For more information about the `adminaccessconfig` command, see Configuring Administrator Settings, page 26-20. |
| alertconfig        | Specify alert recipients, and set parameters for sending system alerts.    |
### Table 27-1  Web Security appliance Administrative Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authcache</td>
<td>Allows you to delete a one or all entries (users) from the authentication cache. You can also list all users currently included in the authentication cache. You might want to clear a user from the authentication cache so the user can login again from a different machine before the User session Restrictions values times out.</td>
</tr>
<tr>
<td>bwcontrol</td>
<td>Enable bandwidth control debug messages in the Default Proxy log file.</td>
</tr>
<tr>
<td>certconfig</td>
<td>Configure security certificates and keys.</td>
</tr>
<tr>
<td>clear</td>
<td>Clears pending configuration changes since last commit.</td>
</tr>
<tr>
<td>commit</td>
<td>Commits pending changes to the system configuration.</td>
</tr>
<tr>
<td>createcomputerobject</td>
<td>Creates a computer object at the location you specify.</td>
</tr>
<tr>
<td>datasecurityconfig</td>
<td>Defines a minimum request body size, below which upload requests are not scanned by the IronPort Data Security Filters. For more information, see Bypassing Upload Requests Below a Minimum Size, page 12-3.</td>
</tr>
<tr>
<td>dnsconfig</td>
<td>Configure DNS server parameters.</td>
</tr>
<tr>
<td>dnsflush</td>
<td>Flush DNS entries on the appliance.</td>
</tr>
<tr>
<td>etherconfig</td>
<td>Configure Ethernet port connections.</td>
</tr>
<tr>
<td>externaldlpconfig</td>
<td>Defines a minimum request body size, below which upload requests are not scanned by the external DLP server. For more information, see Bypassing Upload Requests Below a Minimum Size, page 12-3.</td>
</tr>
<tr>
<td>featurekey</td>
<td>Submits valid keys to activate licensed features. For more information, see Feature Keys Page, page 26-10.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>featurekeyconfig</td>
<td>Automatically check for and update feature keys. For more information, see Feature Key Settings Page, page 26-11.</td>
</tr>
<tr>
<td>grep</td>
<td>Searches named input files for lines containing a match to the give pattern.</td>
</tr>
<tr>
<td>help</td>
<td>Returns a list of commands.</td>
</tr>
<tr>
<td>iccm_message</td>
<td>Clears the message in the web interface and CLI that indicates when this Web Security appliance is managed by a Security Management appliance (M-Series).</td>
</tr>
<tr>
<td>ifconfig or interfaceconfig</td>
<td>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.</td>
</tr>
<tr>
<td>last</td>
<td>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.</td>
</tr>
<tr>
<td>loadconfig</td>
<td>Load a system configuration file.</td>
</tr>
<tr>
<td>logconfig</td>
<td>Configure access to log files.</td>
</tr>
<tr>
<td>mailconfig</td>
<td>Mail the current configuration file to the address specified.</td>
</tr>
<tr>
<td>musconfig</td>
<td>Use this command to enable Secure Mobility Solution and configure how to identify remote users, either by IP address or by integrating with one or more Cisco adaptive security appliances. For more information on enabling and configuring Secure Mobility Solution, see Enabling Secure Mobility, page 13-3.</td>
</tr>
</tbody>
</table>
Table 27-1  Web Security appliance Administrative Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| musstatus        | Use this command to display information related to Secure Mobility Solution when the Web Security appliance is integrated with an adaptive security appliance. This command displays the following information:  
- The status of the Web Security appliance connection with each adaptive security appliance.  
- The duration of the Web Security appliance connection with each adaptive security appliance in minutes.  
- The number of remote clients from each adaptive security appliance.  
- The number of remote clients being serviced, which is defined as the number of remote clients that have passed traffic through the Web Security appliance.  
- The total number of remote clients. |
| 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. For more information, see Packet Capture, page 26-6. |
| passwd           | Set the password.                                |
| pathmtudiscovery | Enables or disables Path MTU Discovery.  
You might want to disable Path MTU Discovery if you need to packet fragmentation. |
### Table 27-1  Web Security appliance Administrative Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping</td>
<td>Sends an ICMP ECHO REQUEST to the specified host or gateway.</td>
</tr>
<tr>
<td>proxyconfig</td>
<td>Enables or disables the Web Proxy.</td>
</tr>
<tr>
<td>proxystat</td>
<td>Display web proxy statistics.</td>
</tr>
<tr>
<td>quit, q, exit</td>
<td>Terminates an active process or session.</td>
</tr>
<tr>
<td>reboot</td>
<td>Flushes the file system cache to disk, halts all running processes, and restarts the system.</td>
</tr>
<tr>
<td>reportingconfig</td>
<td>Configure a reporting system.</td>
</tr>
<tr>
<td>resetconfig</td>
<td>Restores the configuration to factory defaults.</td>
</tr>
<tr>
<td>rollovernow</td>
<td>Roll over a log file.</td>
</tr>
<tr>
<td>routeconfig</td>
<td>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.</td>
</tr>
<tr>
<td>saveconfig</td>
<td>Saves a copy of the current configuration settings to a file. This file can be used to restore defaults, if necessary.</td>
</tr>
<tr>
<td>setgateway</td>
<td>Configure the default gateway for the machine.</td>
</tr>
<tr>
<td>sethostname</td>
<td>Set the hostname parameter.</td>
</tr>
<tr>
<td>setntlmsecuritymode</td>
<td>Changes the security setting for the NTLM authentication realm to either “ads” or “domain.” When the setting is “domain,” the appliance joins the Active Directory domain with a domain security trust account, and when the setting is “ads,” it joins the domain as a native Active Directory member. Default is ads.</td>
</tr>
<tr>
<td>setttime</td>
<td>Set system time.</td>
</tr>
<tr>
<td>settz</td>
<td>Displays the current time zone, and provides an operations menu to set a local time zone.</td>
</tr>
<tr>
<td>showconfig</td>
<td>Display all configuration values.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Terminates connections and shuts down the system.</td>
</tr>
</tbody>
</table>
Table 27-1   Web Security appliance Administrative Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>smtprelay</td>
<td>Configure SMTP relay hosts for internally generated email. An SMTP relay host is required to receive system generated email and alerts. For more information about configuring SMTP relay hosts, see Configuring SMTP Relay Hosts, page 25-26.</td>
</tr>
<tr>
<td>snmpconfig</td>
<td>Configure the local host to listen for SNMP queries and allow SNMP requests.</td>
</tr>
<tr>
<td>sshconfig</td>
<td>Configure hostname and host key options for trusted servers.</td>
</tr>
<tr>
<td>status</td>
<td>Displays system status.</td>
</tr>
<tr>
<td>supportrequest</td>
<td>Send the support request email to IronPort customer care. This includes system information and a copy of the master configuration. The e-mail address is “<a href="mailto:support@ironport.com">support@ironport.com</a>”.</td>
</tr>
</tbody>
</table>
| 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  |
| techsupport | Provides a temporary connection to allow IronPort Customer Care/Applications Engineering to access the system and assist in troubleshooting. |
| telnet     | Communicates with another host using the TELNET protocol. |
| testauthconfig | Tests the authentication settings for a given authentication realm against the authentication servers defined in the realm.  
For more information about testing authentication settings, see Testing Authentication Settings, page 20-20. |
| traceroute | Traces IP packets through gateways and along the path to a destination host. |
### Table 27-1 Web Security appliance Administrative Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>updateconfig</td>
<td>Configure update and upgrade settings. For more information, see Configuring Upgrade and Service Update Settings, page 26-42.</td>
</tr>
<tr>
<td>updatenow</td>
<td>Update all components.</td>
</tr>
<tr>
<td>upgrade</td>
<td>Install an AsyncOS software upgrade.</td>
</tr>
<tr>
<td>userconfig</td>
<td>Configure system administrators.</td>
</tr>
<tr>
<td>version</td>
<td>Displays general system information, installed versions of system software, and rule definitions.</td>
</tr>
<tr>
<td>webcache</td>
<td>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. For more information, see Web Proxy Cache, page 5-2.</td>
</tr>
<tr>
<td>who</td>
<td>Displays who is logged into the system.</td>
</tr>
<tr>
<td>whoami</td>
<td>Displays user information.</td>
</tr>
</tbody>
</table>
IronPort End User License Agreement

This appendix contains the following section:

- Cisco IronPort Systems, LLC Software License Agreement, page A-1

Cisco IronPort Systems, LLC Software License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”) FOR THE LICENSE OF THE SOFTWARE (AS DEFINED BELOW). BY CLICKING THE ACCEPT BUTTON OR ENTERING “Y” WHEN PROMPTED, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY, COLLECTIVELY, THE “COMPANY”) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THE FOLLOWING AGREEMENT BETWEEN CISCO IRONPORT SYSTEMS, LLC, A DELAWARE CORPORATION (“IRONPORT”) AND COMPANY (COLLECTIVELY, THE “PARTIES”). BY CLICKING THE ACCEPT BUTTON OR ENTERING “Y” WHEN PROMPTED, YOU REPRESENT THAT (A) YOU ARE DULY AUTHORIZED TO REPRESENT YOUR COMPANY AND (B) YOU ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT ON BEHALF OF YOUR COMPANY, AND AS SUCH, AN AGREEMENT IS THEN FORMED. IF YOU OR THE COMPANY YOU REPRESENT (COLLECTIVELY, “COMPANY”) DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, CLICK THE CANCEL BUTTON OR ENTER “N” WHEN PROMPTED AND PROMPTLY (BUT NO LATER THAN THIRTY (30) DAYS
OF THE DELIVERY DATE, AS DEFINED BELOW) NOTIFY IRONPORT, OR THE RESELLER FROM WHOM YOU RECEIVED THE SOFTWARE, FOR A FULL REFUND OF THE PRICE PAID FOR THE SOFTWARE.

1. DEFINITIONS

1.1 “Company Service” means the Company’s email or internet services provided to End Users for the purposes of conducting Company’s internal business and which are enabled via Company’s products as described in the purchase agreement, evaluation agreement, beta or pre-release agreement, purchase order, sales quote or other similar agreement between the Company and IronPort or its reseller (“Agreement”) and the applicable user interface and IronPort’s standard system guide documentation that outlines the system architecture and its interfaces (collectively, the “License Documentation”).

1.2 “End User” means the employee, contractor or other agent authorized by Company to access the Internet or use email services via the Company Service.

1.3 “Service(s)” means (i) the provision of the Software functionality, including Updates and Upgrades, and (ii) the provision of support by IronPort or its reseller, as the case may be.

1.4 “Software” means: (i) IronPort’s proprietary software licensed by IronPort to Company along with IronPort’s hardware products; (ii) any software provided by IronPort’s third-party licensors that is licensed to Company to be implemented for use with IronPort’s hardware products; (iii) any other IronPort software module(s) licensed by IronPort to Company along with IronPort’s hardware products; and (iv) any and all Updates and Upgrades thereto.

1.5 “Updates” means minor updates, error corrections and bug fixes that do not add significant new functions to the Software, and that are released by IronPort or its third party licensors. Updates are designated by an increase to the Software’s release number to the right of the decimal point (e.g., Software 1.0 to Software 1.1). The term Updates specifically excludes Upgrades or new software versions marketed and licensed by IronPort or its third party licensors as a separate product.

1.6 “Upgrade(s)” means revisions to the Software, which add new enhancements to existing functionality, if and when it is released by IronPort or its third party licensors, in their sole discretion. Upgrades are designated by an increase in the Software’s release number, located to the left of the decimal point (e.g., Software
1.x to Software 2.0). In no event shall Upgrades include any new versions of the Software marketed and licensed by IronPort or its third party licensors as a separate product.

2. LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

2.1 License of Software. By using the Software and the License Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, IronPort hereby grants to Company a non-exclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on IronPort’s hardware products, solely in connection with the provision of the Company Service to End Users. The duration and scope of this license(s) is further defined in the License Documentation. Except as expressly provided herein, no right, title or interest in any Software is granted to the Company by IronPort, IronPort’s resellers or their respective licensors. This license and any Services are co-terminus.

2.2 Consent and License to Use Data. Subject to Section 8 hereof, and subject to the IronPort Privacy Statement at http://www.IronPort.com/privacy.html, as the same may be amended from time to time by IronPort with notice to Company, Company hereby consents and grants to IronPort a license to collect and use the data from the Company as described in the License Documentation, as the same may be updated from time to time by IronPort (“Data”). To the extent that reports or statistics are generated using the Data, they shall be disclosed only in the aggregate and no End User identifying information may be surmised from the Data, including without limitation, user names, phone numbers, unobfuscated file names, email addresses, physical addresses and file content. Notwithstanding the foregoing, Company may terminate IronPort’s right to collect and use Data at any time upon prior written or electronic notification, provided that the Software or components of the Software may not be available to Company if such right is terminated.

3. CONFIDENTIALITY. Each Party agrees to hold in confidence all Confidential Information of the other Party to the same extent that it protects its own similar Confidential Information (and in no event using less than a reasonable degree of care) and to use such Confidential Information only as permitted under this Agreement. For purposes of this Agreement “Confidential Information” means information of a party marked “Confidential” or information reasonably considered by the disclosing Party to be of a proprietary or confidential nature; provided that the Data, the Software, information disclosed in design reviews and any pre-production releases of the Software provided by IronPort is expressly designated Confidential Information whether or not marked as such.
4. PROPRIETARY RIGHTS; OWNERSHIP. Title to and ownership of the Software and other materials and all associated Intellectual Property Rights (as defined below) related to the foregoing provided by IronPort or its reseller to Company will remain the exclusive property of IronPort and/or its superior licensors. Company and its employees and agents will not remove or alter any trademarks, or other proprietary notices, legends, symbols, or labels appearing on or in copies of the Software or other materials delivered to Company by IronPort or its reseller. Company will not modify, transfer, resell for profit, distribute, copy, enhance, adapt, translate, decompile, reverse engineer, disassemble, or otherwise determine, or attempt to derive source code for any Software or any internal data files generated by the Software or to create any derivative works based on the Software or the License Documentation, and agrees not to permit or authorize anyone else to do so. Unless otherwise agreed in writing, any programs, inventions, concepts, documentation, specifications or other written or graphical materials and media created or developed by IronPort or its superior licensors during the course of its performance of this Agreement, or any related consulting or professional service agreements, including all copyrights, database rights, patents, trade secrets, trademark, moral rights, or other intellectual property rights (“Intellectual Property Right(s)”) associated with the performance of such work shall belong exclusively to IronPort or its superior licensors and shall, in no way be considered a work made for hire for Company within the meaning of Title 17 of the United States Code (Copyright Act of 1976).

5. LIMITED WARRANTY AND WARRANTY DISCLAIMERS

5.1 Limited Warranty. IronPort warrants to Company that the Software, when properly installed and properly used, will substantially conform to the specifications in the License Documentation for a period of ninety (90) days from the delivery date or the period set forth in the License Documentation, whichever is longer (“Warranty Period”). FOR ANY BREACH OF THE WARRANTY CONTAINED IN THIS SECTION, COMPANY’S EXCLUSIVE REMEDY AND IRONPORT’S ENTIRE LIABILITY, WILL BE PROMPT CORRECTION OF ANY ERROR OR NONCONFORMITY, PROVIDED THAT THE NONCONFORMITY HAS BEEN REPORTED TO IRONPORT AND/OR ITS RESELLER BY COMPANY WITHIN THE WARRANTY PERIOD. THIS WARRANTY IS MADE SOLELY TO COMPANY AND IS NOT TRANSFERABLE TO ANY END USER OR OTHER THIRD PARTY. IronPort shall have no liability for breach of warranty under this Section or otherwise for breach of this Agreement if such breach arises directly or indirectly out of or in connection with the following: (i) any unauthorized, improper, incomplete or inadequate maintenance or calibration of the Software by Company or any third
party; (ii) any third party hardware software, services or system(s); (iii) any unauthorized modification or alteration of the Software or Services; (iv) any unauthorized or improper use or operation of the Software or Company’s failure to comply with any applicable environmental specification; or (v) a failure to install and/or use Updates, Upgrades, fixes or revisions provided by IronPort or its resellers from time to time.

5.2 WARRANTY DISCLAIMER. THE EXPRESS WARRANTIES SET FORTH IN SECTION 5.1 OF THIS AGREEMENT CONSTITUTE THE ONLY PERFORMANCE WARRANTIES WITH RESPECT TO THE SOFTWARE OR SERVICES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IRONPORT LICENSES THE SOFTWARE AND SERVICES HEREUNDER ON AN “AS IS” BASIS. EXCEPT AS SPECIFICALLY SET FORTH HEREIN, IRONPORT AND ITS SUPERIOR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY (EITHER IN FACT OR BY OPERATION OF LAW), AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NEITHER IRONPORT NOR ITS THIRD PARTY LICENSORS WARRANT THAT THE SOFTWARE OR SERVICES (1) IS FREE FROM DEFECTS, ERRORS OR BUGS, (2) THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED, OR (3) THAT ANY RESULTS OR INFORMATION THAT IS OR MAY BE DERIVED FROM THE USE OF THE SOFTWARE WILL BE ACCURATE, COMPLETE, RELIABLE AND/OR SECURE.

6. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY LOSS OF PROFITS, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS, OR FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF SUCH PARTY RECEIVED ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF EITHER PARTY ARISING UNDER ANY PROVISION OF THIS AGREEMENT, REGARDLESS OF WHETHER THE CLAIM FOR SUCH DAMAGES IS BASED IN CONTRACT, TORT, OR OTHER LEGAL THEORY, EXCEED THE TOTAL AMOUNT PAID FOR THE SOFTWARE OR SERVICES DURING THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY.
7. TERM AND TERMINATION. The term of this Agreement shall be as set forth in the License Documentation (the “Term”). If IronPort defaults in the performance of any material provision of this Agreement or the License Documentation, then Company may terminate this Agreement upon thirty (30) days written notice if the default is not cured during such thirty (30) day period. If Company defaults in the performance of any material provision of this Agreement or the License Documentation, IronPort may terminate this Agreement upon thirty (30) days written notice if the default is not cured during such thirty (30) day notice and without a refund. This Agreement may be terminated by one Party immediately at any time, without notice, upon (i) the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings or any other proceedings for the settlement of such Party’s debts, (ii) such other Party making a general assignment for the benefit of creditors, or (iii) such other Party’s dissolution. The license granted in Section 2 will immediately terminate upon this Agreement’s termination or expiration. Within thirty (30) calendar days after termination or expiration of this Agreement, Company will deliver to IronPort or its reseller or destroy all copies of the Software and any other materials or documentation provided to Company by IronPort or its reseller under this Agreement.

8. U.S. GOVERNMENT RESTRICTED RIGHTS; EXPORT CONTROL. The Software and accompanying License Documentation are deemed to be “commercial computer software” and “commercial computer software documentation,” respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying License Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Company acknowledges that the Software and License Documentation must be exported in accordance with U.S. Export Administration Regulations and diversion contrary to U.S. laws is prohibited. Company represents that neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked or denied Company export privileges. Company represents that Company will not use or transfer the Software for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S. Government by regulation or specific license. Company acknowledges it is Company’s ultimate responsibility to comply with any and all import and export restrictions, and other applicable laws, in the U.S. or elsewhere, and that IronPort or its reseller has no further responsibility after the initial sale to Company within the original country of sale.
9. MISCELLANEOUS. This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. Nothing contained herein shall be construed as creating any agency, partnership, or other form of joint enterprise between the parties. Neither party shall be liable hereunder by reason of any failure or delay in the performance of its obligations hereunder (except for the payment of money) on account of (i) any provision of any present or future law or regulation of the United States or any applicable law that applies to the subject hereof, and (ii) interruptions in the electrical supply, failure of the Internet, strikes, shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes, or any other cause which is beyond the reasonable control of such party. This Agreement and the License Documentation set forth all rights for the user of the Software and is the entire agreement between the parties and supersedes any other communications with respect to the Software and License Documentation. The terms and conditions of this Agreement will prevail, notwithstanding any variance with the License Documentation or any purchase order or other written instrument submitted by a party, whether formally rejected by the other party or not. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of IronPort, except that IronPort may modify the IronPort Privacy Statement at any time, in its discretion, via notification to Company of such modification that will be posted at http://www.IronPort.com/privacy.html. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by IronPort or a duly authorized representative of IronPort. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

10. IRONPORT CONTACT INFORMATION. If Company wants to contact IronPort for any reason, please write to IronPort Systems, Inc., 950 Elm Avenue, San Bruno, California 94066, or call or fax us at tel: 650.989.6500 and fax: 650.989.6543.
### A

- **access log file**
  - see also *W3C access logs*
- **ACL decision tags** 24-24
- **anti-malware information** 24-30
- **anti-malware request example entry** 24-35
- **anti-malware response example entry** 24-35
- **custom formatting** 24-39
- **no category (nc)** 24-30
- **no score (ns)** 24-30
- **overview** 24-19
- **result codes** 24-23
- **URL category abbreviations** 16-32
- **Web Reputation Filters example entry** 24-34
- **web reputation information** 24-30

### Access Policy groups
- see also *policy groups*

### Access Policies
- **anti-malware** 8-17
- **application filtering** 8-15
- **configuring Web Reputation** 18-5

### creating 8-7
- flow diagram 8-13
- guest users 7-13
- membership 8-4
- Monitor action 8-3
- objects 8-16
- overview 8-1
- protocol of request 8-9
- protocols and user agents 8-14
- redirecting traffic 16-23
- subnet of request 8-10
- time of request 8-10
- URL category of request 8-10
- URL filters 8-15
- user agent of request 8-11
- user location of request 8-11
- Web Reputation 8-17

- **access logs**
  - custom fields 24-51
  - variables 24-39

- **Active Directory**
  - changing passwords 20-43
Index

joining the domain 20-53
multiple domains 20-51
active mode
  enabling for FTP 5-47
adding
  log subscriptions 24-14
  WCCP service 25-21
addresses
  ambiguous address 21-2
  known allowed address 21-2
  known malware address 21-2
  unlisted address 21-2
adminaccessconfig command
  overview 26-20
administering the appliance
  connecting to the management interface 2-3
  System Setup Wizard 2-2
administrator access
  configuring for IP addresses 26-20
  configuring SSL ciphers 26-21
adult content
  filtering 16-20
  logging usage 16-22
advancedproxyconfig command
  overview 5-30
  web proxy usage agreement 5-18
alert recipient 26-22
alerts
  alert classifications 26-23
  recipients 26-22
  settings 26-23
  severities 26-23
  alert settings 26-23
All Identities
  overview 6-12
  allowing traffic
    L4 Traffic Monitor 21-2
    ambiguous address
      defined 21-2
    anonymizing
      usernames in reports 22-2
anti-malware
  access log file 19-15
  access log information 24-30
  configuring 19-10
  databases 19-5
  outbound scanning 11-1
  overview 19-1
  parameter settings 19-11
  rules for L4 Traffic Monitor 21-4
  scanning verdicts 24-52
  viewing activity 19-15
Anti-Malware report 23-18
anti-malware rules
  L4 Traffic Monitor 21-4
  anti-malware scanning
    bypassing 5-15
    outbound 11-1
AnyConnect Secure Mobility
  see Secure Mobility
application hostname
  DNS support 4-6
application behaviors
  defined 17-4
application bypass settings
  configuring 5-18
application control
  application behaviors 17-4
  applications 17-4
  application types 17-4
  bandwidth 17-11
  bypassing application scanning 5-18
  configuring 17-4, 17-9
  instant messaging traffic 17-17
  logging 17-19
  overview 17-1
  report 23-16
  reporting 17-19
  rules and guidelines 17-9
applications
  blocking 17-9
  configuring bandwidth limits 17-15
  defined 17-4
application scanning
  bypassing 5-18
application types
  configuring bandwidth limits 17-13
  defined 17-4
  overriding bandwidth limits 17-13
Application Visibility and Control
  see application control
Application Visibility and Control engine
  see AVC engine
Application Visibility report
  overview 23-16
  archiving reports 22-16
assignment method
  WCCP service 25-18
AsyncOS upgrades
  overview 26-40
authentication
  behavior with multiple realms 20-19
  compared to authorization 6-10
  configuring global settings 20-23
  configuring LDAP 20-43
  configuring NTLM 20-51
  defined 6-10
  entering the domain 20-4
  exempting user agents 6-18
  failure 20-4
  global Identity policy 7-6
  guest access 7-13
  HTTPS requests 7-6
  Identity groups 7-4
  LDAP 20-43
  MSN Messenger 7-26
Index

native FTP 5-9
NTLM 20-51
overview 20-1
realms 20-14
re-authenticating users 20-39
SaaS applications 14-4
secure LDAP 20-43
sending credentials securely 20-37
sequences 20-16
special characters 20-56
supported characters for Basic 20-51
surrogates 20-40
surrogates supported 20-42
testing settings 20-20
upstream proxies 20-3
authentication credentials
defined 20-5
invalid 20-4
SaaS Access Control 14-4
sending securely 20-37
authentication realms
behavior with multiple realms 20-19
creating 20-15
deleting 20-16
editing 20-15
overview 20-14
testing settings 20-20
authentication scheme
Identity group 7-9
authentication sequences
behavior with multiple realms 20-19
creating 20-17
deleting 20-19
editing 20-18
overview 20-16
authentication server
unavailable 20-4
authentication surrogates
supported 20-42
authorization
defined 6-10
failing 20-39
AutoSupport feature 26-25
available upgrades 26-40
AVC engine
enabling 17-3
updates 17-3

B

bandwidth
configuring overall limits 17-11
configuring user limits 17-12
limiting 17-11

bandwidth limits
configuring for applications 17-15
configuring for application types 17-13
overall 17-11
overriding for application types 17-13
overview 17-11
per user 17-12
Basic authentication
securely sending credentials 20-37
blacklist address
see known malware address
blocking
adult content 16-20
applications 8-18, 17-9
file types 8-21
HTTPS traffic 10-12
instant messenger 8-18
objects 8-16, 8-21, 12-17
peer-to-peer 8-20
ports 8-14, 21-5
protocols 8-14
traffic 21-5
upload requests 12-3, 16-26
upload requests due to AVC engine 17-3
upload requests due to malware 11-2
URL categories 8-15, 12-17
user agents 8-14
user experience 11-2, 12-3, 16-26, 17-3
blocking traffic
L4 Traffic Monitor 21-3
browsers
see web browsers
browse view
application control 17-5
bypassing
application scanning 5-18
scanning and filtering 5-15
upload requests from scanning 12-3
C
CA
see certificate authorities
capturing network packets
overview 26-6
case-sensitivity
in CLI 27-4
category filtering
database 16-5
certificate authorities
validating 10-10
certificate authority
defined 10-6
certificate files
see also root certificates
converting formats 10-20
supported formats 10-16
uploading 10-25, 14-10
certificates
generating and signing your own 26-34
installing for credential encryption 20-38
installing on appliance 26-35
invalid 10-26
overview 10-9
root 10-16
SaaS Access Control 14-4
validating 10-12
validating certificate authorities 10-10
Change Password link 26-16
changing passwords 26-16
cipher
defined 10-6
ciphertext
defined 10-6
Cisco ASA integration
configuring 13-5
overview 13-3
Cisco IronPort Web Usage Controls
overview 16-2
cleartext
defined 10-7
CLI
case-sensitivity in 27-4
clearing changes 2-16
committing changes 2-16
configuring host keys 24-13
overview 2-4, 27-1
rolling over log files 24-12
SSH 27-2
supported languages 2-10
viewing most recent log files 24-13
warning message 26-20
welcome message 26-20
Client Malware Risk 23-22
Client Malware Risk report 23-22
Client Malware Risk report page 23-22
command line interface
see CLI
Commit Changes button
overview 2-14
commit command 2-16, 27-6
committing changes
commit command 2-16
overview 2-14
community string
SNMP 22-17
compressing
log files 24-12
computer account
joining an Active Directory domain 20-53
configuration file 26-2
configuring 25-7
administrator settings 26-20
application control settings 17-4
custom text at login 26-20
data interfaces 25-3
FTP proxy, advanced options 5-30
host keys 24-13
HTTPS Proxy 10-21
Identities 7-28
proxy cache options 5-30
return addresses 26-21
URL filters 16-6
WCCP router 3-9
web proxy, advanced options 5-30
Web Reputation Filters 18-5
configuring the appliance
anti-malware 19-10
browser requirements 2-10
clearing changes 2-14
committing changes 2-14, 26-3
enabling features 26-10
L4 Traffic Monitor 21-3
log files 24-9
network interfaces 25-2
P2 port 25-3
reporting 22-1
scheduling reports 22-13
submitting changes 26-3
upstream proxies 3-15
Web Proxy settings 5-3
connecting
L4 Traffic Monitor 3-17
web proxy in explicit forward mode 3-7
web proxy in transparent mode 3-8
connecting the appliance
L4 switch 3-5, 4-2
P1 and P2 ports 3-5, 4-2
serial line 2-5
WCCP router 3-5, 4-2
content filtering
IronPort Data Security Policies 12-17
controlling applications
overview 17-1
controlling bandwidth
overall limits 17-11
overview 17-11
user limits 17-12
control settings
Decryption Policies 10-34
creating
Access Policies 8-7
authentication realms 20-15
authentication sequences 20-17
Decryption Policies 10-30
External DLP Policies 12-10
Identities 7-20
IronPort Data Security Policies 12-10
log subscriptions 24-14
Outbound Malware Scanning Policies 11-6
Routing Policies 9-8
time ranges 6-14
user agent based policies 6-16
credential encryption
certificate and key 20-38
HTTPS requests 20-38
overview 20-38
Index

cryptography
  certificate authority 10-6
  cipher 10-6
  ciphertext 10-6
  cleartext 10-7
  digital certificate 10-6
  digital signature 10-6
  key 10-6
  overview 10-6
  plaintext 10-7
  private key 10-7
  public key 10-7
  public key infrastructure 10-7
  root certificate 10-7
  self-signed certificate 10-7
  symmetric key 10-7

CSS
  in end-user notification pages 15-23

custom certificate authority
  importing 10-37

custom fields
  access and W3C logs 24-51

customizing
  log files 24-39

custom text 26-20
  at login 26-20

custom URL categories
  overview 16-16
  redirecting traffic 16-23

custom welcome message
  configuring for CLI 26-20

D

data interfaces
  configuring 25-3
  overview 3-4

data loss prevention
  see Data Security Policies
  see External DLP Policies
  see Outbound Malware Scanning Policies

datasecurityconfig
  CLI command 12-3

Data Security logs
  overview 12-27

Data Security Policies
  configuring 12-15
  content 12-17
  creating 12-10
  flow diagram 12-16
  logging 12-27
  membership 11-3, 12-7
  minimum request size 12-3
  Monitor action 12-5
  overview 12-1
  protocol of request 12-12
  proxy port of request 12-12
  subnet of request 12-13
upload request definition 12-4
URL category of request 12-13
URL filters 12-17
user agent of request 12-14
Web Reputation 12-17
Data Security Policy groups
see policy groups
debugging
policy groups 6-18
decrypting
HTTPS traffic 10-1
overview 10-13
decrypting HTTPS traffic
configuring Decryption Policies 10-3
overview 10-13
Decryption Policies
blocking 10-12
controlling traffic 10-34
ccontrol settings 10-34
creating 10-30
cryptography 10-6
decrypting traffic 10-3, 10-13
dropping traffic 10-3
enabling 10-21
flow diagram 10-28, 10-36
guest users 7-13
membership 10-27
Monitor action 10-5
overview 10-1
passing through traffic 10-3
proxy port of request 10-32
root certificates 10-16
subnet of request 10-32
time of request 10-33
URL category of request 10-33
user agent of request 10-33
user location of request 10-33
Decryption Policy groups
see also policy groups
default gateway 25-7
default route
configuring 25-7
deleting
a URL from the web proxy cache 5-2
authentication realms 20-16
authentication sequences 20-19
log subscriptions 24-19
WCCP service 25-25
DEM format
converting 10-20
deploying the appliance
L4 Traffic Monitor 3-3, 3-16
multiple appliances and WCCP routers 3-15
overview 3-1
see also deployment
web proxy 3-2
deployment
connecting to a WCCP router 3-8
example scenario 3-5
existing proxies 3-15
L4 Traffic Monitor 3-16
overview 3-1
PAC files 3-7
preparing for 3-2
web proxy in explicit forward mode 3-6
web proxy in transparent mode 3-7
depth of appliance 3-18
DHCP
  WPAD 5-23
digital certificate
defined 10-6
see also certificates
digital cryptography
defined 10-6
digital signature
defined 10-6
dimensions of appliance 3-18
DLP servers
defining 12-20
failover 12-24
DNS
  authoritative name servers 25-28
  configuring 25-28
  installing the appliance 4-6
  split 25-28
  WPAD 5-23
DNS cache
  flushing 25-30
domain
derenting for authentication 20-4
dropping traffic
  Decryption Policies 10-3
duplex
deploying the L4 Traffic Monitor 3-17
  network tap 4-3
DVS engine
  how it works 19-5
  overview 19-4
  working with multiple malware verdicts 19-6
Dynamic Content Analysis engine
  enabling 16-6
  overview 16-3
dynamic service
  WCCP services 25-18
Dynamic Vectoring and Streaming engine
defined 16-3
dynamic service
  WCCP services 25-18
Dynamic Vectoring and Streaming engine
  see DVS engine
E
editing
  authentication realms 20-15
  authentication sequences 20-18
  WCCP service 25-21
editing the appliance
  concurrent editing 2-10
enabling
  active mode for FTP 5-47
  HTTPS Proxy 10-21
  P2 port 25-3
  Secure Mobility 13-3
end-user acknowledgement page
  configuring 15-20
  overview 15-18
end-user notification pages
  customizing 15-8
  formatting text 15-23
  HTML tags 15-23
  IronPort notification pages 15-5
  native FTP 15-23
  overview 15-1
  tokens 15-8
  user defined notification pages 15-14
  variables 15-8
end-user URL category page
  configuring 15-21
  warning users 16-24
etherconfig command
  VLAN 25-11
evaluating Access Policy membership
  matching client requests 8-5
evaluating Data Security Policy membership
  matching client requests 11-4, 12-8
evaluating Decryption Policy membership
  matching client requests 10-28
evaluating External DLP Policy membership
  matching client requests 11-4, 12-8
evaluating Identity group membership
  authentication 7-4
  authentication scheme 7-9
  examples 7-31
  matching client requests 7-10
  overview 7-2
evaluating policy group membership
  overview 6-10
evaluating Routing Policy membership
  matching client requests 9-6
exempting
  user agents from authentication 6-18
expired keys
  overview 26-12
exporting
  reports 22-10
externaldlpconfig
  CLI command 12-3
External DLP Policies
  configuring 12-25
  creating 12-10
  defining external DLP servers 12-20
  ICAP 12-2
  load balancing 12-24
  logging 12-27
  membership 11-3, 12-7
  minimum request size 12-3
Index

overview 12-1
protocol of request 12-12
proxy port of request 12-12
subnet of request 12-13
URL category of request 12-13
user agent of request 12-14
user location of request 12-14

External DLP Policy groups
see policy groups

external DLP servers
see DLP servers

failed authentication
  allowing guest access 7-13
  overview 20-4
failing authorization 20-39
failover
  DLP servers 12-24
  Routing Policies 9-2
feature keys
  adding manually 26-11
  expired keys 26-12
  overview 26-10
  settings 26-11
filtering
  adult content 16-20
  anti-malware 8-17
category 8-15, 12-17
data in IronPort Data Security Policies 12-17
objects in Access Policies 8-16
protocols 8-14
user agents 8-14
Web Reputation 8-17, 12-17

Firefox
  PAC files 5-29
formatting
  access log 24-39
  end-user acknowledge pages 15-23
  end-user notification pages 15-23
forwarding method
  GRE 25-20
  L2 25-19
  WCCP service 25-19

FTP
  see also native FTP
  active mode 5-8, 5-31
  configuring notification messages 15-23
  enabling active mode 5-47
  FTP over HTTP 5-8
  passive mode 5-8
FTP Poll 24-17
FTP Proxy
  overview 5-8
FTP proxy
  advanced configuration 5-30
FTP Push 24-17
Index

G

G

G
generating
  root certificates 10-24
  root certificates for HTTPS 10-16
global Identity policy
  authentication 7-6
global policy group
  overview 6-7
GRE
  forwarding method 25-20
greylist address
  see ambiguous address
guest access
  overview 7-13
GUI
  supported languages 2-10

H

H

H

hash assignment
  WCCP assignment method 25-19
height of appliance 3-18
heuristic analysis
  McAfee scanning engine 19-9
hostkeyconfig command 24-13
host keys
  configuring 24-13
hostname
  appliance 4-6
  changing 25-1
HTTP/HTTPS headers
  logging 24-51
HTTPS
  authentication 7-6
  certificate authority definition 10-6
  cipher definition 10-6
  ciphertext definition 10-6
  cleartext definition 10-7
  credential encryption 20-38
  digital certificate definition 10-6
  digital signature definition 10-6
  key definition 10-6
  overview 10-8
  plaintext definition 10-7
  private key cryptography definition 10-7
  public key cryptography definition 10-7
  public key infrastructure definition 10-7
  root certificate definition 10-7
  self-signed certificate definition 10-7
  symmetric key cryptography definition 10-7
HTTPS Proxy
  configuring 10-21
  decrypting traffic 10-13
HTTPS requests
  authentication 7-6
ICAP
  External DLP Policies 12-2
  identifying users transparently
    see transparent user identification
Identities
  about 7-1
  authentication 7-4
  configuring in policy groups 7-28
  creating 7-20
  evaluating membership 7-2
  guest privileges 7-13
  local users 13-2
  multiple 7-28
  remote users 13-2
Identity groups
  proxy port of request 7-3
  see also policy groups
  URL category of request 7-3
  user agent of request 7-3
identity provider
  configuring 14-7
  defined 14-2
identity provider initiated flow
  SaaS Access Control 14-3
importing
  trusted root certificates 10-37
installing the appliance
  prerequisites 4-1
  setup worksheet 4-4
  instant messaging traffic
    controlling 17-17
  interfaceconfig command
    VLAN 25-15
  interfaces
    see network interfaces 25-2
Internet Explorer
  re-authentication 20-40
  WPAD 5-24
invalid certificates
  handling 10-26
IP based access
  about 26-20
IPMI
  SNMP 22-18
IP spoofing
  WCCP service 25-20
IronPort Data Security Filters
  overview 12-1
IronPort Data Security Policies
  see Data Security Policies
  user location of request 12-14
IronPort notification pages
  formatting text 15-23
  HTML tags 15-23
  overview 15-5
IronPort URL Filters
  see URL filters

J
joining
  Active Directory domain 20-53

K
key
defined 10-6
key files
  see also root certificates
  converting formats 10-20
  supported formats 10-16
keys
  overview 26-10
known allowed address
defined 21-2
known malware address
defined 21-2

L
L2
  forwarding method 25-19
L4 Traffic Monitor
  allowing traffic 21-2
  allow list 21-6
  ambiguous addresses 21-2
  anti-malware rules 21-4
  blocking 21-5
  blocking traffic 21-3
  configuring 21-3
  database 21-3
  deploying 3-3, 3-16
  how it works 21-1
  interfaces 3-5
  known allowed addresses 21-2
  known malware addresses 21-2
  L2 switch 3-17
  log files 24-53
  monitoring 21-5
  monitoring traffic 21-2
  overview 21-1
  report 23-31
  span/mirror port 3-17
  unlisted addresses 21-2
  viewing activity 21-9
L4 Traffic Monitor interfaces
  overview 3-5
languages
  supported 2-10
last command 26-17
Layer 4 switch
  connecting to the appliance 4-2
LDAP
  overview 20-43
  testing settings 20-21
load balancing
  traffic to external DLP servers 12-24
  traffic to upstream proxies 9-2
load-balancing method
  see assignment method
local users
  overview 13-2
log fields
  W3C access logs 24-38
log files
  see also log subscriptions
  compressed 24-12
  configuring host keys for SSH 24-13
  configuring the level of information recorded 24-15
  custom 24-39
  extensions in filenames 24-11
  formatting access and W3C logs 24-39
HTTP/HTTPS headers 24-51
L4 Traffic Monitor 24-53
naming convention 24-11
overview 24-1
types 24-2
viewing most recent version 24-13
logging
  HTTP/HTTPS headers 24-51
  Secure Mobility 13-6
log subscriptions
  adding 24-14
  compressing 24-12
  deleting 24-19
  editing 24-14
  overview 24-9
  rolling over 24-11
logging in
  web interface 2-9
login 26-20
login message
  configuring for CLI 26-20
logs
  see also log files
  FTP Poll 24-17
  FTP Push 24-17
  overview 24-1
  rolling over 24-11
  SCP Push 24-18
  Syslog Push 24-18
M
M1 interface
  overview 3-4
M1 port
  connecting to a laptop 4-2
MAIL FROM
  configuring for notifications 26-21
malware
  configuring scanning 19-10
  see also anti-malware

malware verdicts
  multiple 19-6

management interface
  overview 3-4

managing the appliance
  connecting to a laptop 4-2
  connecting to the management interface 2-3
  System Setup Wizard 2-2

mask assignment
  WCCP assignment method 25-19

matching client requests
  Access Policies 8-5
  Decryption Policies 10-28
  External DLP Policies 11-4, 12-8
  Identities 7-10
  IronPort Data Security Policies 11-4, 12-8
  Routing Policies 9-6

McAfee scanning engine
  categories 19-9
  database 19-5
  heuristic analysis 19-9
  overview 19-8

membership diagram
  Access Policies 8-5
  Decryption Policies 10-28
  External DLP Policies 11-4, 12-8

Identities 7-10
  IronPort Data Security Policies 11-4, 12-8
  Routing Policies 9-6

Metadata File for Service Provider
  SaaS applications 14-14

MIB file
  SNMP 22-17

mirror port
  deploying the L4 Traffic Monitor 3-17

misclassified URLs
  reporting 15-8

mobile users
  overview 13-2
  Mobile User Security Daemon log
    Secure Mobility 13-6
    Monitor
      Access Policies 8-3
      Decryption Policies 10-5
      IronPort Data Security Policies 12-5

monitoring
  L4 Traffic Monitor 21-5
  ports 21-5
  scheduling reports 22-13
  summary data 22-1
  system activity 23-2
  traffic 21-2
  users from the CLI 26-16

MSN Messenger
  authentication 7-26
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
</table>
| multiple Active Directory domains  
  overview 20-51  
| multiple Identities  
  overview 7-28  
| musconfig command  
  overview 13-7  
| musstatus command  
  overview 13-7  
| |
| N |
| native FTP  
  authentication 5-9  
  configuring notification messages 15-23  
  guidelines 5-8  
  overview 5-8  
  transparently redirected connections 5-10  
| navigating  
  web interface 2-7  
| negotiating  
  SSL session 10-9  
| Netscape  
  PAC files 5-29  
| network interfaces 25-2  
  appliance ports 3-3  
  enabling P2 25-3  
  M1 3-4  
  P1 and P2 3-4  
  T1 and T2 3-5  
| |
| O |
| object filtering  
  Access Policies 8-16  
| objects  
  blocking 8-16, 12-17  
| on-demand reports 22-15  
| outbound malware scanning  
  overview 11-1  
| Outbound Malware Scanning Policies  
  configuring 11-11  
  creating 11-6  
  logging 11-14  
| overview 11-1  
| |
| VLANs 25-9  
| network tap  
  duplex 3-17, 4-3  
  simplex 3-17, 4-3  
| no category (nc) 24-30  
| no score (ns) 24-30  
| notification pages  
  see end-user notification pages  
| NTLM  
  computer account 20-53  
  entering a domain 20-4  
  joining an Active Directory domain 20-53  
  overview 20-51  
  testing settings 20-21  
| |
protocol of request 11-8
proxy port of request 11-8
subnet of request 11-9
URL category of request 11-9
user agent of request 11-10
user location of request 11-10
Outbound Malware Scanning Policy groups
see also policy groups
Overview report 23-2

P

P1 and P2 interfaces
overview 3-4

P2 port
configuring 25-3

PAC files
configuring browsers 5-22
deployment 3-7
format 5-21
Netscape and Firefox 5-29
overview 5-19
re-authentication 20-41
storing on the appliance 5-24
WPAD 5-23

packet capture
editing settings 26-7
overview 26-6
starting 26-7

pages in the web interface 2-8
passing through traffic
Decryption Policies 10-3
passwords
Active Directory 20-43
changing 26-16
creating 26-13
special characters 20-56
PDF
reports 22-10
PER format
converting 10-20
physical dimensions of appliance 3-18
pinout
serial connection 2-5
plaintext
defined 10-7
policies table
examples 7-31
overview 6-7
policy group member definition
Access Policies 8-4
Decryption Policies 10-27
External DLP Policies 11-3, 12-7
Identities 7-2
IronPort Data Security Policies 11-3, 12-7
overview 6-10
Routing Policies 9-5
user agent based 6-5
Index

policy groups
  about 6-1
  Access Policies 8-1
  All Identities 6-12
  creating 6-7
  custom URL categories 16-16
  Decryption Policies 10-3
  evaluating group membership 6-10
  External DLP Policies 12-1
  global policy group 6-7
  guidelines 6-12
  IronPort Data Security Policies 12-1
  Outbound Malware Scanning Policies 11-1
  overview 6-6
  policies table 6-7
  time based 6-13
  tracing 6-18
  types of policies 6-3
  user agent based 6-16
policy types
  overview 6-3
ports
  Access Policies 8-9
  blocking 8-14
  Decryption Policies 10-32
  External DLP Policies 12-12
  Identities 7-3
  IronPort Data Security Policies 12-12
  Outbound Malware Scanning Policies 11-8

Routing Policies 9-10
  see also network interfaces
  private key cryptography
    defined 10-7
  protocol filtering
    Access Policies 8-14
    protocols
    Access Policies 8-9
    blocking 8-14
    External DLP Policies 12-12
    IronPort Data Security Policies 12-12
    Outbound Malware Scanning Policies 11-8
    Routing Policies 9-10
  proxy
    see web proxy
    proxy bypass list
      about 5-15
      using with WCCP 5-18
    proxy cache
      configuring 5-30
    proxy groups
      creating 9-3
    public key cryptography
      defined 10-7
    public key infrastructure
      defined 10-7
realms
    see authentication realms
re-authentication
    overview 20-39
    using with Internet Explorer 20-40
    using with PAC files 20-41
redirecting traffic
    overview 16-23
Redirect setting
    URL categories 16-23
regular expressions
    overview 16-28
    using in URL filters 16-28
remote upgrades 26-44
remote users
    overview 13-2
reporting misclassified URLs 15-8
reports
    anonymizing usernames 22-2
    Anti-Malware 23-18
    Application Visibility 23-16
    archiving 22-16
    Client Detail 23-24
    Client Malware Risk 23-22
    Client Malware Risk Page 23-22
    custom date ranges 22-3
    exporting data 22-10
    interactive display 22-1
    L4 Traffic Monitor 23-31
    making usernames unrecognizable 22-2
    Malware Category 23-20
    Malware Threat 23-21
    on-demand 22-15
    Overview 23-2
    printing to PDF 22-10
    Reports by User Location 23-33
    return address 26-21
    scheduling 22-13
    search option 22-5
    System Capacity 23-40
    System Status 23-44
    time range for scheduled reports 22-13
    time ranges 22-3
    uncategorized URLs 23-15
    URL Categories 23-12
    Web Reputation Filters 23-29
    Web Sites 23-10
    Reports by User Location report
        overview 23-33
        result codes 24-23
        return addresses
            configuring 26-21
        RFC
            1065 22-16
            1066 22-16
            1067 22-16
Index

1213  22-16
1907  22-16
2571-2575  22-17
rolling over log files
  overview  24-11
rollovernow command  24-12
root certificate
  defined  10-7
root certificates
  generating  10-24
  importing trusted  10-37
  uploading  10-24
  using  10-16
Routing Policies
  creating  9-8
  failover  9-2
  guest users  7-13
  load balancing  9-2
  membership  9-5
  overview  9-2
  protocol of request  9-10
  proxy port of request  9-10
  subnet of request  9-11
  time of request  9-11
  URL category of request  9-11
  user agent of request  9-12
  user location of request  9-12
Routing Policy groups
  see also policy groups
routings tables
  configuring  25-8
routing traffic  9-2

S

SaaS Access Control
  authenticating users  14-4
  authentication requirements  14-4
  certificate  14-4
  configuring identity provider  14-7
  enabling  14-5
  identity provider  14-2
  identity provider initiated flow  14-3
  multiple appliances  14-6
  overview  14-1
  prompting for authentication  14-4
  SAML  14-2
  service provider  14-3
  service provider initiated flow  14-3
  single sign-on  14-15
  single sign-on URL  14-5
  understanding  14-2
  zero day revocation  14-2
SaaS Application Authentication Policies
  creating  14-11
SaaS applications
  see SaaS Application Authentication Policies
  authentication requirements  14-4
creating SaaS policies 14-11
Metadata File for Service Provider 14-14
single sign-on 14-15

safe search
enforcing 16-20

SAML
identity provider 14-2
SaaS Access Control 14-2
service provider 14-3

scanning verdicts
anti-malware 24-52

SCP Push 24-18

search view
application control 17-7

secure LDAP 20-43

Secure Mobility
configuring from the CLI 13-7
enabling 13-3
logging 13-6
overview 13-1
remote users 13-2
report 23-33
transparent user identification 13-5

see upstream proxies

self-signed certificate
defined 10-7

SenderBase Network 2-5

sequences
see authentication sequences

serial connection
connecting to the appliance 2-5

service provider
defined 14-3
service provider initiated flow
SaaS Access Control 14-3

sethostname command
overview 25-1

setting up the appliance
prerequisites 4-1

Simple Network Management Protocol
see SNMP

simplex
deploying the L4 Traffic Monitor 3-17
network tap 4-3

single sign-on
see also transparent user identification
defined 20-6

SaaS applications 14-15
URL for SaaS access 14-5

site content rating
enforcing 16-20
warning 16-21

SMI file
SNMP 22-17

SNMP
community string 22-17
hardware failure trap conditions 22-18
hardware objects 22-18
IPMI 22-18
MIB file 22-17
overview 22-16
SMI file 22-17
SNMPv1 22-17
SNMPv2 22-17
SNMPv3 passphrase 22-17
specifying multiple trap targets 22-19
traps 22-19
Sophos scanning engine
overview 19-10
span port
deploying the L4 Traffic Monitor 3-17
special characters
authentication 20-56
splash page
web proxy usage agreement 5-18
SSH
configuring host keys 24-13
using with the CLI 27-2
SSL
negotiating a session 10-9
used in HTTPS 10-8
SSL ciphers
configuring for administrator access 26-21
SSL handshake
overview 10-9
SSO URL
SaaS Access Control 14-5
standard service
WCCP service 25-18
Start Test button
overview 20-22
streaming upgrades 26-43
Submit button 26-3
submitting changes
configuring the appliance 26-3
subnet
Access Policies 8-10
Decryption Policies 10-32
External DLP Policies 12-13
IronPort Data Security Policies 12-13
Outbound Malware Scanning Policies 11-9
Routing Policies 9-11
supported languages
GUI and CLI 2-10
supportrequest command 26-3
surrogates
authentication 20-42
symmetric key cryptography
defined 10-7
Syslog 24-18
System Capacity report
overview 23-40
system configuration file 26-2
System Setup Wizard
logging in 4-8
Network page 4-9
overview 4-6
password 4-8
Review page 4-26
Security page 4-22
Start page 4-8
URL 4-8
username 4-8
System Status report 23-44
system time 26-30

creating 6-14
Decryption Policies 10-33
policy groups 6-13
Routing Policies 9-11
TLS
used in HTTPS 10-8
tokens
see variables
to upstream proxies 9-2
tracing policies
overview 6-18
traffic
redirecting 16-23
transaction result codes 24-23
transparently identifying users
see transparent user identification
transparent mode
native FTP 5-10
transparent redirection 25-17
traansparent redirection
adding a WCCP service 25-21
assignment method 25-18
forwarding method 25-19
GRE forwarding method 25-20
hash assignment 25-19
L2 forwarding method 25-19
mask assignment 25-19
overview 25-17
WCCP services 25-17

T

T1 and T2 interfaces
overview 3-5
tabs in web interface 2-7
tail command 24-13
tcpdump
see packet capture
testauthconfig command 20-23
testing authentication settings 20-20
threat risk rating 19-12
threat risk threshold 19-12
time 26-30
time based policies
overview 6-13
time ranges 6-14
URL Filters 16-26
time ranges
Access Policies 8-10
transparent user identification
  configuring for Novell eDirectory 7-19
  overview 7-16
  remote users 13-5
  rules and guidelines 7-18
  SaaS applications 14-15
  Secure Mobility 13-5
  working with Novell eDirectory 7-17
troubleshooting
  policy groups 6-18
  TRR (Threat Risk Rating) 19-12
  TRT (Threat Risk Threshold) 19-12
trusted root certificates
  importing 10-37
tty connection
  connecting to the appliance 2-5

updates
  available 26-40
  configuring upgrade settings 26-42
  overview 26-40
  remote 26-44
  requirements for local upgrade servers 26-46
  streaming 26-43
upgrading
  AsyncOS 26-40
uploading
  certificate files 10-25, 14-10
  root certificates 10-24
  root certificates for HTTPS 10-16
upload request
  defined 12-4
upstream proxies
  adding proxy information 9-3
  authentication 20-3
  creating proxy groups 9-3
  deployment 3-15
  overview 9-1
  routing traffic 9-2
URL
  Access Policies 8-10
  Decryption Policies 10-33
  External DLP Policies 12-13
  Identity groups 7-3
  IronPort Data Security Policies 12-13
  Outbound Malware Scanning Policies 11-9

uncategorized URLs 16-4
  in reports 23-15
unlisted address
  defined 21-2
unrecognized root authority
  invalid certificates 10-26
updates
  manual updates 26-51
  overview 26-42
Routing Policies 9-11
URL categories 16-24
  abbreviations 16-32
  blocking 8-15, 12-17
descriptions 16-32
redirecting traffic 16-23
uncategorized URLs 23-15
URL Categories report 23-12
URL Filters
  bypassing 5-15
  configuring 16-6
custom categories 16-16
database 16-5
Dynamic Content Analysis engine 16-3
enabling 16-5
IronPort URL Filters 16-2
no category 16-4
regular expressions 16-28
time based 16-26
URL category descriptions 16-32
viewing filtering activity 16-27
URL processing
  L4 Traffic Monitor 21-1
user accounts
  about 26-12
  managing 26-13
types of 26-14
user agent
  Decryption Policies 10-33
Identity groups 7-3
Routing Policies 9-12
user agent based policies
  overview 6-16
user agent filtering
  Access Policies 8-14
user agents
  Access Policies 8-11
  blocking 8-14
  creating policies 6-16
  exempting from authentication 6-18
External DLP Policies 12-14
  file types 8-21
  instant messenger 8-18
IronPort Data Security Policies 12-14
  objects 8-21
Outbound Malware Scanning Policies 11-10
  peer-to-peer 8-20
user defined notification pages
  example 15-17
  overview 15-14
  parameters 15-15
User Discovery Service log
Secure Mobility 13-6
user location
  Access Policies 8-11
Decryption Policies 10-33
  External DLP Policies 12-14
IronPort Data Security Policies 12-14
Index

Outbound Malware Scanning Policies 11-10
Routing Policies 9-12

user name 26-15
usernames
making unrecognizable in reports 22-2
user password length 26-13
user passwords 26-16
user types 26-14

V
validating certificates 10-12
validating certificate authorities 10-10
variables
access logs 24-39
end-user notification pages 15-8

VLAN
defined 25-9
etherconfig command 25-11
example use 25-10
interfaceconfig command 25-15
labels 25-10
overview 25-9

W
W3C access logs
   custom fields 24-51
   custom formatting 24-39
   log fields 24-38
   overview 24-36
   user defined log fields 24-51
warning
   accessing adult content 16-21
   warning page
      end-user URL category page 15-21
   warning users 16-24
      configuring end-user warning page 15-21
      using URL categories 16-24
WBRS
   see also Web Reputation Filters
WCCP
   bypassing the web proxy 5-18
WCCP cluster
   overview 3-15
WCCP configuration
   example configuration 3-11
   syntax 3-10
WCCP router
   cluster 3-15
   configuration syntax 3-10
   configuring 3-9
   connecting to the appliance 4-2

Cisco IronPort AsyncOS 7.1 for Web User Guide

IN-28
OL-23207-01
deploying the appliance 3-8
multiple 3-15
WCCP services 25-17
WCCP services
adding 25-21
assignment method 25-18
deleting 25-25
dynamic service 25-18
editing 25-21
forwarding method 25-19
IP spoofing 25-20
overview 25-17
standard service 25-18
well known service 25-18
web browsers
configuring 5-22
detecting PAC files automatically 5-23
PAC files 5-22
supported 2-10
web interface
browser requirements 2-10
clearing changes 2-14
committing changes 2-14
logging in 2-9
navigating 2-7
pages 2-8	web proxy
tabs 2-7
user name and password 2-9

web proxy
advanced configuration 5-30
bypassing 5-15
cache 5-2
cache, configuring 5-30
deploying 3-2
deploying in explicit forward mode 3-6
deploying in transparent mode 3-7
eexisting 3-15
overview 5-1
splash page 5-18
usage agreement 5-18
Web Proxy Autodiscovery Protocol
see WPAD
web proxy cache
modifying 5-2
removing a URL from the cache 5-2
Web Reputation Filters
about 18-1
access log file 18-10
access log information 24-30
bypassing 5-15
configuring Access Policies 18-5
database 18-1
how it works 18-4
report 23-29
scores 18-2
viewing activity 18-9
Webroot scanning engine
  database 19-5
  overview 19-7
Web Security appliance
  physical dimensions 3-18
  user name and password 2-9
Web Sites report 23-10
weight of appliance 3-18
welcome page
  web proxy usage agreement 5-18
well known service
  WCCP service 25-18
whitelist address
  see known allowed address
whoami command 26-17
who command 26-16
width of appliance 3-18
Windows domain
  entering for authentication 20-4
WPAD
  detecting PAC files 5-23
  Internet Explorer 5-24
  using with Netscape and Firefox 5-29
  using with the appliance 5-24

X
X.509
  standard for certificates 10-7

Z
zero day revocation
  defined 14-2