

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL

3-9

3-9

3-9

3-10

3-11

CHAPTER 4

Intercepting Web Requests 4-1

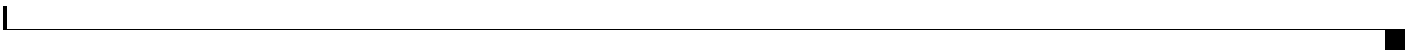
4-1

4-2

4-2












 C-3

APPENDIX D

End User License Agreement D-1

 D-1

 D-8

CHAPTER 1

Introduction to the Product and the Release

- [Introduction to the Web Security Appliance, page 1-1](#)
- [What's New, page 1-1](#)
- [Ug\(b 81\(,\)3uriIn75cterf\)12\(ace\)-27g/T1_2 1 Tf0 Tc 0 Tw 9 0 0 9 148.56 522.9 Tm\(48825\)Tj/CS0 cs 0 0 1](#)

Web Interface Browser Requirements

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

The Cisco Web Security Appliance follows the Target Environments set by YUI:

CHAPTER 2

Connect, Install, and Configure

- [Overview of Connect, Install, and Configure, page 2-1](#)
- [Deploying a Virtual Appliance, page •](#)

Step 1

- Passphrase: `ironport`

Step 3 You must immediately change the passphrase.

Step 4 If the appliance is already configured, choose **System Administration > System Setup Wizard**.

If the appliance is already configured, you will be warned that you are about to reset the configuration.





Service

The service group type for the router. Choose from:

Standard service. This service type is assigned a fixed ID of zero, a fixed redirection method of

Configuring an SMTP Relay Host



Identification Profiles and Authentication with Cloud Web Security Connector

CHAPTER



Web Proxy Options for Intercepting Web Requests

CHAPTER 5

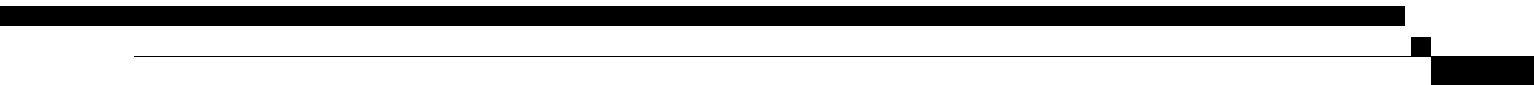
Acquire End-User Credentials

- [Overview of Acquire End-User Credentials, paFBT5r705](#)•



Authentication Realms

Step 8





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

Setting	Description
Credential Encryption	This setting specifies whether or not the client sends the login credentials to the Web Proxy through an encrypted HTTPS connection.

Step 4 Submit and commit your changes.

Supported Authentication Surrogates for Explicit Requests

Supported Authentication Surrogates for Transparent Requests



Authentication and Authorization Failures

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

If authentication succeeds but authorization fails, it is possible to



**Define Members by
Machine ID**

- **Do Not Use Machine ID in This Policy** – The user is not identified by machine ID.
-

Step 9 Submit and Commit Changes.



- Step 3** If you choose Identity provider initiated flow, the appliance redirects users to the SaaS application.
- Step 4** If you choose Service Provider initiated flows, you must configure this URL in the SaaS application.
- Always prompt SaaS users for proxy authentication. After entering valid credentials, users are logged into the SaaS application.
 - Transparently sign in SaaS users. Users are logged into the SaaS application automatically.



Related Topics

- [Using Self-signed Certificates, page 8-3](#)
- [Using CA-signed Certificates, page 8-3](#)
- [Overview of the Identity Services Engine Service, page 8-1](#)
- [Tasks for Certifying and Integrating the ISE Service, page 8-3](#)
- [Connect to the ISE Services, page 8-6](#)

Using Self-signed Certificates

When self-signed certificates are used on the ISE server, all three certificates—the ISE pxGrid and Admin certificates, developed on the ISE server, as well as the WSA Client certificate, developed on the cS0 5(h)

Click





News

CHAPTER

- **All Identification Profiles** – This policy will apply to all existing profiles. You must also define at least one **Advanced** option.
- **Select One or More Identification Profiles** – A table for specifying in







Step 8 Submit and commit your changes.







- Step 3** In the **Edit Destination Settings** section, select “Define Destinations Scanning Custom Settings” from the drop-down menu.
- Step 4** In the **Destinations to Scan** section, select one of the following:
- Step 5** Submit your changes.
- Step 6** In the Anti-Malware Filtering column, click the link for the policy group.
- Step 7** In the Anti-Malware Settings section, select “Define Anti-Malware Custom Settings”.
- Step 8** In the Cisco IronPort DVS Anti-Malware Settings section, select which anti-malware scanning engines to enable for this policy group.
- Step 9** In the Malware Categories section, select whether to monitor or block the various malware categories. The categories listed in this section depend on which scanning engines you enable.

CHAPTER













Step 3





CHAPTER



-
- Step 1** **Create and configure Data Security Policy groups.** Cisco IronPort Data Security Policies use URL filtering, web reputation, and upload content information when evaluating the upload request. You configure each of these security components to determine whether or not to block the upload request. When the Web Proxy compares an upload request to the control settings, it evaluates the settings in order.



CHAPTER

Step 4 In the Notification Page URL field, enter the URL which you want to redirect blocked websites.

Step 5

ERR_ADULT_CONTENT Policy Acknowledgment	The warning page that is displayed when the end-user accesses a page that is classified as adult content. Users can click an acknowledgment link to continue to the originally requested site.	You are trying to visit a web page whose content are rated as explicit or adult. By
--	--	---

ERR_CONTINUE_UNACKNOWLEDGED Policy Acknowledgment	Warning page that is displayed when the user requests a site that is in a custom URL category that is assigned the Warn action. Users can click an acknowledgment link to continue to the originally requested site.	You are trying to visit a web page that falls under the URL Category <i><URL category></i> . By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content. Data about your browsing behavior may be monitored and recorded. You will be periodically asked to acknowledge this statement for continued access to this kind of web page. Click here to accept this statement and access the Internet.
ERR_DNS_FAIL DNS Failure	Error page that is displayed when the requested URL contains an invalid domain name.	The hostname resolution (DNS lookup) for this hostname <i><hostname></i> has failed. The Internet address may be misspelled or obsolete, the host

ERR_PROXY_PREVENT
_MULTIPLE_LOGIN



- Step 4** Select a time range for the data included in the report.
- Step 5** Choose the format for the generated report.
The default format is PDF. Most reports also allow you to save raw data as a CSV file.
- Step 6** Depending on the type of report you configure, you can specify different report options, such as the number of rows to include and by which column to sort the data. Configure these options as necessary.
- Step 7** Select whether to archive the report (if so, the report will appear on the Archived Reports page).
- Step 8** Specify whether to email the report, and list the email addresses of the recipients.

System Capacity Page

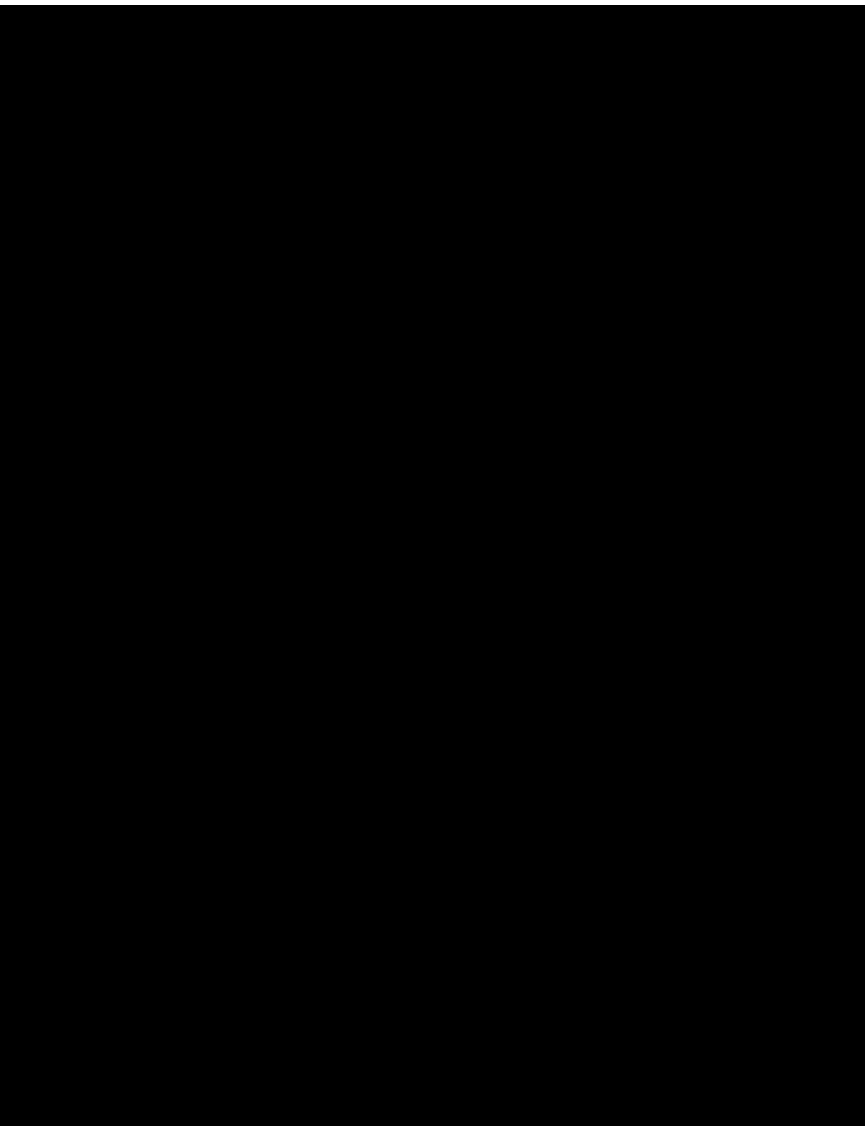
The **Reporting > System Capacity** page displays current and historical information about resource





- Rollover by File Size The maximum file size to which the current log file can grow before it is archived and a new log file started. Enter a number between 100 kilobytes and 10 gigabytes.
- Rollover by Time The maximum time interval before the current log file is archived and a new log file started. The following interval types are available:
- **None.** AsyncOS only performs a rollover when the log file reaches the maximum file size.
 - **Custom Time Interval.** AsyncOS performs a rollover after a specified amount of time has passed since the previous rollover. Specify the number of days, hours, minutes, and seconds between rollovers using *d*, *h*, *m*, and *s* as suffixes.
 - **Daily Rollover.** AsyncOS performs a rollover every day at a specified time. Separate multiple times a day using a comma. Use an asterisk (*) for the hour to have rollover occur every hour during the day. You can also use an asterisk to rollover every minute of an hour.
 - **Weekly Rollover.** AsyncOS performs a rollover on one or more days of the week at *a3ec*

Log Fields
(W3C Access Logs)



%L	x-local_time	<p>Request local time in human-readable format: DD/MMM/YYYY : hh:mm:ss +nnnn. This field is written with double-quotes in the access logs.</p> <p>Enabling this field allows you to correlate logs to issues without having to calculate local time from epoch time for each log entry.</p>
%m	cs-auth-mechanism	<p>Used to troubleshoot authentication issues.</p> <p>The authentication mechanism used on the transaction. Possible values are:</p> <ul style="list-style-type: none">•






```
remotepower
```

```
setup
```

Step 4 Follow the prompts to specify the following:

- The dedicated IP address for this feature, plus netmask and gateway.

-





certificate may be issued by example.com who, in turn, is granted the rights to issue certificates by a



Authentication Problems

- [Troubleshooting Tools for Authentication Issues](#)
- [Failed Authentication Impacts Normal Operations](#)
- [LDAP Problems](#)
- [Basic Authentication Problems](#)
- [Single Sign-On Problems](#)
- Also see:
 - [General Troubleshooting Best Practices](#)
 - [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication](#)
 -


```
Priority: 100, Interval: 3 seconds
Status: MASTER
Choose the operation you want to perform:
- NEW - Create new failover group.
- EDIT - Modify a failover group.
- DELETE - Remove a failover group.
- PREEMPTIVE - Configure whether failover is preemptive.
- TESTFAILOVERGROUP - Test configured failover profile(s)
[]> testfailovergroup
Failover group ID to test (-1 for all groups):
[]> 61
```

Failover Issues on Virtual Appliances

Zero Byte File Appears On FTP Servers After File Upload





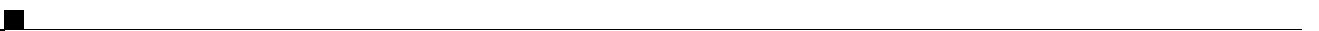


Subsequent Access


```
resetconfig
```


APPENDIX C





- (i) transfer, assign or sublicense its license rights to any other person or entity (other than in compliance with any Cisco relicensing/transfer policy then in force), or use the Software on Cisco equipment not purchased by the Customer from an Approved Source or on secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;
 - (ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;
- (il(e s2o)67unng6(ent)5(nem)-9.1 asee coiw,reaca do,resi



I N D E X

A

access log file

see also *W3C access logs*

ACL decision tags [21-16](#)

no category (nc) [21-20](#)

no score (ns) [21-20](#)

overview [21-13](#)

result codes [21-16](#)

URL category abbreviations [9-23](#)

access logs

header format specifier [21-36](#)

Access Policies



extreme [9-25](#)
fashion [9-25](#)
file transfer services [9-25](#)
filter avoidance [9-25](#)
finance [9-25](#)
freeware and shareware [9-25](#)





