



User Guide for ASA CX and Cisco Prime Security Manager 9.3

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-32018-01

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

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

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

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

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

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

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

Google, Google Play, Android and certain other marks are trademarks of Google Inc.

© 2011-2014 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface xv

Audience xv

Related Documentation xv

Conventions xv

Obtaining Documentation and Submitting a Service Request xvii

CHAPTER 1

Introduction 1

Context-Aware Security and PRSM: The Big Picture 1

Product and Documentation Overview 3

ASA CX Features 3

Cisco Prime Security Manager Features 5

CHAPTER 2

Preparing CX Devices 7

Initial ASA CX Setup 7

ASA Configuration Restrictions for ASA CX 9

Setting Up the ASA CX Software 9

Altering the ASA Configuration for the ASA CX SSP 12

Configuring ASA Access Rules for ASA CX 13

Configuring ASA Inspection Rules for ASA CX 13

Configuring the ASA to Send Traffic to the ASA CX SSP 14

Redirecting Traffic to ASA CX Using the ASA CLI 14

Configuring ASA CX in Monitor-Only Mode 16

Redirecting Traffic to ASA CX Using PRSM 17

Troubleshooting PRSM Traffic Redirection Policies 18

CHAPTER 3

Getting Started 21

Browser Requirements 21

Changing the Language for the Web Interface	21
Logging Into the System	22
Logging Into the Web Interface	22
Logging Into the ASA CX CLI	23
Logging Into the PRSM CLI	23
Web Interface Basics	24
Your User Role Controls What You Can See and Do	24
Menus	24
Lists and Tables	25
Policy, List, and Alert Icons	26
Select or Mouse Over List Items to See Commands	26
Selecting Items	27
Getting Help	28
Viewing Basic System Information	29
Working with Other Users	29
Troubleshooting Web Interface Problems	30
Committing or Discarding Changes	30
The Commit and Deploy Changes Page	32
Managing Deployment Jobs	33
Viewing Change History	35
Dealing with Out-of-Band Changes	36
When Do Configuration Changes Become Active?	37
Deployment Job and Device Status	37

CHAPTER 4

Use Cases for ASA CX 41

How to Set Up ASA CX in Transparent Mode	41
How to Configure High Availability	44
How to Gain Insight Into Your Network Traffic	46
How to Control Application Usage	51
How to Use Passive Authentication	53
How to Create Access Policies that Apply to AD/LDAP User Groups	56
How to Implement an Acceptable Use Policy (URL Filtering)	59
How to Enable Access to YouTube for Schools	61
How to Block Malware Using Web Reputation	63
How to Scan for Threats (IPS Filtering)	66

How to Monitor and Control AnyConnect Secure Mobility Devices 67

CHAPTER 5

Managing System Licenses 71

CX Feature and PRSM Licenses 71

Feature Licenses 71

Cisco Prime Security Manager Licenses 72

How Feature Licenses Affect Policy Configuration 72

Overview of the Licenses Page 73

Configuring System Licenses 74

Using Evaluation Licenses 74

Uploading License Files 75

Assigning Feature Licenses 76

Applying Licenses 76

Renewing Licenses 76

Obtaining and Installing the 3DES/AES (K9) License for Strong Encryption 77

Revoking Licenses 78

Deleting Licenses 78

PART I

The Basics 79

CHAPTER 6

Managing Devices 81

Managing CX Devices in Multiple Device Mode 81

Preparing ASA Devices for Management 83

Understanding Device Discovery 84

CX Device Discovery 84

ASA Device Discovery 85

Actions that Require You to Delete and Re-import a Device 87

The Device Inventory 89

Adding Devices 89

Restrictions on Adding Devices 89

Handling Object Naming Conflicts 91

Adding an ASA and its CX 91

Adding a Standalone ASA 93

Adding an ASA High Availability Pair 94

Troubleshooting Device Import 95

Converting Monitor-Only Devices to Full Management	97
Viewing Device License Assignments	97
Updating Device Management Credentials	97
Changing the Management IP Address	98
Refreshing Certificates	98
Deleting Devices	99
Troubleshooting Device Communications	99

CHAPTER 7

Managing Policies 103

Policy Concepts	103
Configuring the Device	104
Device Configuration Policies and Settings	106
Policy Basics	107
Configuring Policy Sets	108
Configuring Rule-Based Policies	109
Moving Policy Sets and Rules	109
Changing Policy Sharing Status	110
Making Per-Device Exceptions for Shared Policy Sets	111
Editing Rule-Based Policies and Policy Sets	112
Disabling or Enabling Rule-Based Policies	112
Analyzing Shared Policy Assignments	113
Deleting Policies or Policy Sets	113

CHAPTER 8

Managing Policy Objects 115

Policy Objects	115
Policy Object Types	116
Configuring Policy Objects	118
Customizing Object Contents for a Device	119
Importing Objects	120
Deleting Policy Objects	121
Policy Object Reference	121
Common Policy Object Properties	122
Network Group and Network Objects	123
CX Network Groups	123
Network Object Groups	125

Network Objects	126
Service Group Objects	127
TCP and UDP Port Keywords	129
CX Identity Objects	132
URL Objects	134
User Agent Objects	137
Application Objects	138
Secure Mobility Objects	139
Application Service Objects	140
Destination Object Groups	142
Source Object Groups	143
File Filtering Profile Objects	144
Web Reputation Profile Objects	146
NG IPS Profile Objects	148
Header-Injection Profile	149
Interface Role Objects	150
ASA Identity Objects	151
Time Range Objects	152

PART II

Monitoring Devices 155

CHAPTER 9

Viewing Dashboards and Reports 157

Overview of Dashboards	157
Available Dashboards	160
Dashboard Basics	162
Understanding Dashboard and Report Data	162
Drilling Into Dashboards	164
Changing the Dashboard Time Range	166
Controlling the Data Displayed in Dashboards	167
Dashboard Columns	169
Creating Reports	171
Generating Reports	171
Report Properties	171
Report Types	172
Interpreting the Network Overview Dashboard	173

Monitoring Health and Performance	174
Resolving Device Alerts	176
Interpreting the Malware Traffic Dashboard	179
Interpreting the NG Intrusion Prevention Dashboard	180
Interpreting the ASA Traffic Dashboard	181

CHAPTER 10

Viewing Events 183

Overview of Event Viewer	183
Using Event Views	187
Configuring Custom Views	187
Switching Between Real Time and Historical Views	188
Filtering Events	188
Event Filter Rules	189
Improving Historical Event Filter Performance	190
Working with Individual Events	191
Configuring Syslog	192
Configuring Syslog Settings for CX Devices	192
CX Syslog Settings	193
Configuring Logging and Syslog Settings for ASA Devices	193
ASA Logging Properties	194
ASA Syslog Server Properties	195
Event Messages	196
Context-Aware Security Traffic Events	196
CX Device and PRSM System Events	201
Event Columns	214

PART III

Configuring Context-Aware Security 223

CHAPTER 11

Managing Authentication and Identity Services 225

Overview of Authentication and Identity Services	225
Supported AAA Servers and Authentication Methods	226
Types of User Identity	226
What to Tell Users About Authentication	227
Configuring Authentication and Identity Services	227
Overview of Directory Realms	228

Configuring Directory Realms	230
Directory Properties	231
Determining the Directory Search Base	233
Deleting Directory Realms or Directories	234
Configuring Identity Policies	235
Identity Policy Properties	236
Enabling Active Authentication	240
Enabling Transparent User Authentication	241
Requirements for Transparent Authentication	242
Configuring Internet Explorer for Transparent Authentication	243
Configuring Firefox for Transparent Authentication	243
Identifying the Active Directory Agent	245
Configuring Authentication Settings	246

CHAPTER 12

Controlling Network Access with Context-Aware Access Policies 249

Overview of Context-Aware Access Policies	249
Default Context-Aware Access Policy Behavior	250
Configuring Context-Aware Access Policies	250
Context-Aware Access Policy Properties	253
Warning Users of Undesirable Sites	257
Applying Rate Limits (Policing)	258
Enforcing Safe Search	259
Notifying Users of Blocking Policies	259
When Are Notifications Sent?	259
End User Notifications Page	261
Customizing End User Notifications	263
Editing End User Notifications	263
Importing End User Notifications	264
End User Notification Variables	265
URL and Application Filtering	266
Comparing URL and Application Filtering	267
Controlling Applications	268
Decryption Requirements for Application Filtering	269
Tips for Application Filtering	269
Using the Application Viewer	270

URL Filtering 271

URL Categories 272

Determining the Category for a URL 272

Web Reputation Filtering (Malware Protection) 273

Guide to Web Reputation Scores 273

Configuring Web Reputation Filtering 274

Configuring Malware Protection (Web Reputation) Settings 275

Next Generation IPS Filtering 276

Configuring Next Generation IPS Filtering 276

Configuring Intrusion Prevention Settings 277

Viewing Next Generation IPS Threats 278

Configuring Signature and Engine Updates 279

Troubleshooting Signature and Engine Updates 281

CHAPTER 13

Managing SSL/TLS Traffic Flows 283

Overview of SSL/TLS Traffic Management 283

Why Decrypt Traffic? 285

Decrypted Traffic Flow 286

Do Not Decrypt Traffic Flow 287

Tips and Limitations for Decryption 288

Configuring SSL/TLS Decryption 288

Configuring Decryption Settings 289

Configuring the Decryption Certificate 291

Converting Certificate and Key Formats 293

Downloading and Installing the SSL/TLS Certificate 293

Managing Supplemental Trusted Certificates 294

Configuring Decryption Policies 295

Decryption Policy Properties 297

Bypassing Decryption for Unsupported Applications 300

Troubleshooting TLS/SSL Decryption 302

PART IV

Configuring the ASA 305

CHAPTER 14

Managing High Availability 307

About High Availability 307

Configuring Devices for Failover	308
Managing High Availability	308
High Availability Configuration Properties	309

CHAPTER 15

Interface Management 313

Understanding Device Interfaces	313
About EtherChannels	314
EtherChannel Load Balancing	315
About Static Routes	316
Route Tracking Using SLAs	317
Managing Device Interfaces	317
Physical Interface Properties	318
Subinterface Properties	322
EtherChannel Properties	325
Redundant Interface Properties	328
Bridge Group Properties	332
Interface: IPv4 Properties	335
Interface: IPv6 Properties	339

CHAPTER 16

Configuring Network Address Translation 343

Address Translation Overview	343
Address Translation Definitions	344
PAT Pools and Round Robin Allocation	345
Managing NAT Rules	347
Twice NAT Rule Properties	348
Object NAT Rules	351

CHAPTER 17

Configuring Access Policies 357

About Access Policies	357
Managing ASA Access Policies	358
Access Policy Properties	359

APPENDIX A

System Maintenance and Troubleshooting 363

Managing Users	363
Overview of the Users Page	363

User Roles and Privileges	364
Using the Pre-Defined Admin User	367
Configuring the Directory Realm for Remote Users	368
Configuring Users	368
User Properties	369
Configuring Single Sign-On for Cisco Security Manager	370
Configuring SSO Directories and Users	371
Changing Your Password	372
Deleting Users	373
Installing a Server Certificate	373
Obtaining a Server Certificate	374
Configuring Network Participation	375
Configuring an HTTP Proxy	376
Basic Troubleshooting	377
Checking System Connectivity	377
Capturing Packets	378
Managing System Processes	381
Creating a Diagnostics File for the Cisco Technical Assistance Center	383
Logging Configuration Properties (CX, PRSM)	384
Maintaining the System	385
Backing Up and Restoring the Database	385
Scheduling Database Backups	387
Backing Up and Restoring the PRSM VM	388
Reclaiming Disk Space	389
Resetting the Admin Password	390
Resetting to Factory Defaults	391

APPENDIX B

Installing Software	393
Image and Software Packages	393
Cisco Prime Security Manager Installation	394
Preparing the Server for PRSM Installation	394
Installing the PRSM Virtual Machine	395
Managing PRSM Disk Space	400
Upgrading the System	402
Installing System Upgrades from the CLI	402

Applying Upgrades from the Web Interface	404
The Upgrade Manager	404
Uploading Upgrade Packages	405
Installing System Upgrades from the Web Interface	405
Troubleshooting System Upgrades	406
Reimaging the ASA 5585-X CX SSP	407
Reimaging the ASA CX Software Module	410
Open CX and PRSM Ports	414



Preface

The preface contains the following topics.

- [Audience, page xv](#)
- [Related Documentation, page xv](#)
- [Conventions, page xv](#)
- [Obtaining Documentation and Submitting a Service Request, page xvii](#)

Audience

This document is for network and security personnel who install, configure, deploy, and manage security infrastructure.

Related Documentation

Use the following documentation road maps to find related documentation.

- *Finding ASA CX and Cisco Prime Security Manager Documentation*
<http://www.cisco.com/c/en/us/td/docs/security/asacx/roadmap/asacxprsmroadmap.html>
- *Navigating the Cisco ASA 5500 Series Documentation*
<http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html>

Conventions

This document uses the following conventions:

Convention	Indication
Command Menu > Menu Item	Commands, keywords, buttons, field names, and user-entered text appear in bold font. For menu-based commands, the full path to the command is shown.

Convention	Indication
<i>variable</i>	Variables, for which you supply values, are in <i>italic</i> font. Italic font is also used for document titles and for general emphasis.
[]	Elements in square brackets are optional.
{x y z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
courier font	Terminal sessions and information that the system displays appear in <i>courier</i> font.
< >	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document uses the following conventions for reader alerts:



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Tip

Means *the following information will help you solve a problem*.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

**Warning**

Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.



Introduction

Cisco ASA Next-Generation Firewall Services, also known as Cisco ASA CX Context-Aware Security, gives security administrators visibility and control of the traffic flowing through the network, including the users connecting to the network, the devices used, and what applications and web sites are accessed. In addition to tradition IP address and service (protocol/port), you can control access based on application use, user identity, web address, user agent, and user location.

Cisco Prime Security Manager (PRSM) provides multi-device management for ASA and CX devices.

- [Context-Aware Security and PRSM: The Big Picture, page 1](#)
- [Product and Documentation Overview, page 3](#)

Context-Aware Security and PRSM: The Big Picture

The firewall has long been the mainstay of an enterprise's defense perimeter. To fight off modern-day threats, the firewall needs to be made “context-aware.” That is, it needs to extract the user and application identity, origin of the access and the type of device used for the access, and then permit or deny the access based on these attributes, in accordance with configured policy. In addition, the firewall must have the ability to detect and protect against emerging threats.

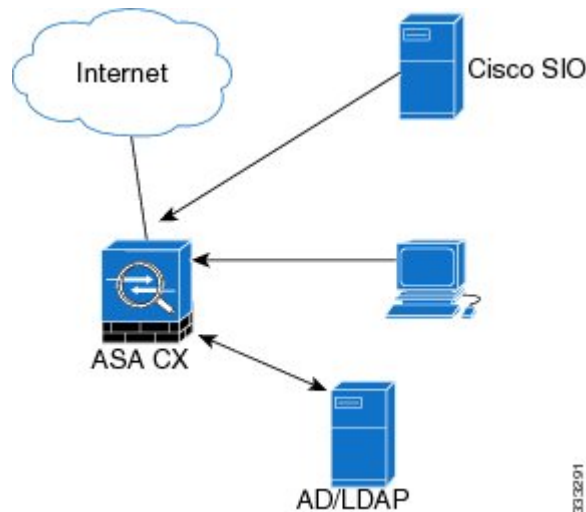
These are the capabilities that Context-Aware Security provides. Context-aware devices (CX devices) such as ASA CX let you enforce security based on the complete context of a situation. This context includes the identity of the user (who), the application or website that the user is trying to access (what), the origin of the access attempt (where), and the properties of the device used for the access (how). With ASA CX, you can extract the full context of a flow and enforce granular policies such as permitting access to Facebook but denying access to games on Facebook or permitting finance employees access to a sensitive enterprise database but denying the same to other employees.

The firewall is the right place to obtain the full context of the traffic flowing through the network. The firewall already sees all the traffic crossing the trust boundary between the enterprise network and the world at large.

As shown in the following figure, CX devices sit at the boundary between your network and the Internet or any other network from which protection is required. The devices regularly download signature and engine updates from the Cisco Security Intelligence Operations center, and use your Active Directory or OpenLDAP directories for user identity. You can optionally use the Cisco Context Directory Agent (CDA) or AD Agent to augment user identification (not shown). To configure the device, you log into it using a web browser (when

configuring policies) or an SSH or Console client (when configuring device settings or doing basic system troubleshooting).

Figure 1: Context-Aware Security in the Network

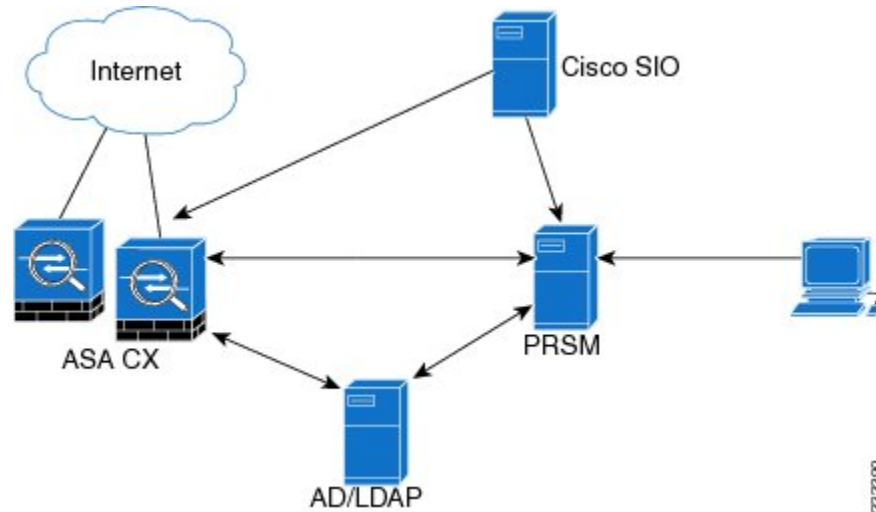


Cisco Prime Security Manager (PRSM) fits in when you want to manage multiple CX devices. By adding your CX devices to the PRSM inventory, you can apply consistent policies among your devices. The PRSM web and CLI interfaces are identical to those of the single CX device, with the addition of multiple-device management capabilities, so you can quickly apply what you have learned about single device management to multiple devices.

As shown in the following figure, when managing multiple devices with PRSM, you log into PRSM instead of the individual devices. All configuration is done through PRSM and then deployed to the managed devices, and all events generated by managed devices are shown in PRSM. In addition, both the CX device and PRSM download signature and engine updates from the Cisco Security Intelligence Operations center, and interact with your AD/LDAP directories and optionally, CDA or AD Agent (not shown). The CX CLI remains available

so you can do basic device-level troubleshooting, but you cannot use the CX web interface to change the device configuration without first removing the device from the PRSM inventory.

Figure 2: PRSM and CX in the Network



Product and Documentation Overview

CX and Cisco Prime Security Manager (PRSM, pronounced “prism”) are closely related. They share the same user interface, so that your experience in directly managing a CX device is easy to translate into managing multiple devices in Cisco Prime Security Manager.

Thus, this documentation covers both the CX platform and the Cisco Prime Security Manager device management software, as well as ASA device configuration to the extent that the ASA is supported. When reading the documentation, keep the following in mind:

- PRSM Multiple Device mode refers to the multi-device management application, which you can use to manage more than one CX device and ASA. Where a feature applies to this platform only, we explicitly state that it is for Multiple Device mode.
- ASA CX (or CX) only, Single Device mode, or PRSM Single Device mode refers to the management application that is hosted on the CX device itself. You can use this application to configure that single device only. Thus, functions that relate to managing multiple devices, such as the device inventory, do not appear.

The following topics describe the products in more detail.

ASA CX Features

ASA CX is a Security Services Processor (SSP) available on some models of the Cisco ASA 5500 Series Adaptive Security Appliance. The SSP can be a hardware module, such as the one for the 5585-X, or it can be a software module, such as the one for the 5545-X. You configure the parent ASA to redirect traffic to the ASA CX SSP, which then applies its policies.

**Tip**

Although the Cisco ASA 5585-X CX Security Services Processor includes GigabitEthernet network interfaces, these interfaces are controlled by the ASA SSP and logically belong to the ASA. The ASA CX SSP does not directly handle traffic that goes through these interfaces. Only the Console port and two Management interfaces are directly managed by the ASA CX SSP.

The CX Software includes the following features:

- A web interface for policy configuration. You cannot configure policies using the CLI; the CLI provides basic setup and troubleshooting facilities only.
- Support for both IPv4 and IPv6 addresses in every policy that uses addresses. Note that for some features, such as web reputation, the services available for IPv6 might be considerably less than those available for IPv4 simply because IPv4 is more widely used in the Internet.
- Context-aware firewall policies that provide identity and authentication, decryption, and access control. In addition to the traditional traffic matching criteria of IP address, protocol, and port (5-tuple), you can define matching criteria that includes:
 - Usernames and user groups defined in LDAP AAA servers, including Active Directory and OpenLDAP.
 - Application signatures that can identify traffic related to specific applications regardless of the port used for a traffic flow.
 - URL categories that enable you to define policies based on the type of web site (for example, gambling) in addition to individual URLs.
 - User agents that are used to access web sites.
 - Client types that are used to make remote access VPN connections to your network.

**Note**

Traffic matching propositions can be highly complex so that you can precisely identify the traffic for which you want to provide special processing. Most policy objects have both an include and exclude list; you use the exclude list to define exceptions to the items specified in the include list. If you use certain policy objects, such as source object groups, destination object groups, or application service objects, you can create an OR'ed list of AND'ed conditions to define exactly the traffic that you are targeting.

Similarly, context-aware access policies provide granular control for allowed traffic flows. For allowed traffic flows, you can selectively deny parts of the traffic flow based on:

- Next Generation IPS filtering. You can drop traffic that matches known threats.
- Web reputation scores. You can selectively control web traffic based on the public reputation of a web site regardless of the category of the web site. For example, you could screen out advertisements from low reputation sources while allowing them from higher reputation sources. Reputation scores go from -10 (lowest) to 10 (highest).
- File uploads, downloads. You can selectively deny the uploading or downloading of files based on the MIME type of the file.
- Application behavior. Some application types, such as Facebook and LinkedIn, have several separately controllable application behaviors. You can in general allow the application type, yet

disallow unwanted behaviors. For example, you could allow users to post to Facebook but not upload attachments to Facebook messages.

- Rate limiting. You can limit the bandwidth available to bandwidth-hogging applications, dropping packets that exceed the rate.
- Safe Search enforcement. You can enforce Safe Search settings for supported search engines to ensure users cannot perform unfiltered searches. If a search engine is not supported, this prevents users from using those search engines.
- Policy objects that let you define proposition criteria so that you can easily reuse the same criteria in different policies. When you update a policy object, all policies that use the object are automatically updated.
- Automatic deep inspection of HTTP traffic, which enables the use of deep criteria when defining access rules. There is no separate inspection policy to separate inspection with access, simplifying the configuration of the access policies.
- Dashboards that let you view information on a number of criteria, including users, web reputation, policies, URL categories, web site DNS names (domains), applications, and the operating system of remote access VPN clients, and so forth.
- An event viewer to view traffic flow and system events.
- Dynamically updated signatures for applications, web categories, web reputation, and IPS threats. You can configure the time window for these updates.

Cisco Prime Security Manager Features

PRSM is a network security management application. You can use it to do the following:

- Manage multiple devices of the following types:
 - ASA
 - ASA CX
- Monitor the system health and performance of managed devices.
- Monitor traffic events generated by managed devices.
- Create shared policies and apply them to devices, ensuring simple and consistent policies for devices that perform the same role in your network.
- Configure all CX features.
- Reuse network, network group, service, and service group objects defined on the ASA in CX policies.
- Configure the following features on ASA devices:
 - Access rules and their associated objects.
 - NAT rules and their associated objects.
 - ASA High Availability configuration.
 - ASA Interface configuration.

- Traffic redirection to the ASA CX.
- Various platform policies, such as logging and syslog servers.
- Control access to PRSM by defining users and associating security roles, known as role-based access control (RBAC).
- Apply upgrades to managed CX devices.



Preparing CX Devices

Before you can use a CX device, you must configure some basic settings and redirect traffic to the device.

- [Initial ASA CX Setup, page 7](#)
- [Configuring the ASA to Send Traffic to the ASA CX SSP, page 14](#)

Initial ASA CX Setup

Before you can use ASA CX or manage it in Cisco Prime Security Manager, you must install it into your network and complete an initial configuration. The following procedure explains the overall process.

Before You Begin

Although you can configure the ASA and ASA CX to operate in transparent mode, you must put the ASA inline into your network. Do not connect the ASA to a switch port running in span mode.

Also, ensure that the ASA meets the requirements explained in [ASA Configuration Restrictions for ASA CX, on page 9](#).

Procedure

- Step 1** Install the ASA CX SSP into the ASA, and the ASA into the network.
For the ASA CX software module, install the hard drive if necessary.

Follow any instructions that come with the ASA CX SSP and the following documents:

- *Cisco ASA CX Module Quick Start Guide*, http://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/cx/cx_qsg.html.
- *Cisco ASA 5585-X Adaptive Security Appliance Hardware Installation Guide*, <http://www.cisco.com/c/en/us/td/docs/security/asa/hw/maintenance/5585guide/5585Xhw.html>.
- *Cisco ASA 5500-X Hardware Installation Guide*, <http://www.cisco.com/c/en/us/td/docs/security/asa/hw/maintenance/5500xguide/5500xhw.html>.
- *Regulatory Compliance and Safety Information for the Cisco ASA 5585-X Adaptive Security Appliance*, http://www.cisco.com/c/en/us/td/docs/security/asa/hw/regulatory/compliance/asa5585_rcsi.html.

- *Regulatory Compliance and Safety Information for the Cisco ASA 5500-X Series Appliances and the Intrusion Prevention System 4300 Series Appliances*, http://www.cisco.com/c/en/us/td/docs/security/asa/hw/regulatory/compliance/asa5500x_rcsi.html.
- For a list of all ASA documentation, see the documentation roadmap at <http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html>.

Step 2 Connect the management interface to the network.

For hardware platforms such as the ASA CX SSP on the ASA 5585-X, the port is Management 1/0 on the ASA CX SSP (not the ASA SSP). For the ASA CX SSP software module, ensure that the ASA management port is connected.

You use a connection to the ASA CX SSP management interface to configure the device through the web interface.

There is also a minimal CLI that you use for initial setup and for troubleshooting. You can access the CLI through the Console port or by an SSH connection to the management address. For the ASA CX software module, you can open a console session using the **session cxsc console** command in the ASA CLI.

The default management IP address is 192.168.8.8/24, with the gateway 192.168.8.1. You can change this address during setup.

Determine a static IP address that is available on the management network that you can assign to the ASA CX SSP. For the ASA CX software module, the address must be on the same subnet as the ASA management address. For hardware platforms, connect Management1/0 to the network using a standard Cat-6 cable with RJ-45 connector.

Step 3 Set up the software as explained in [Setting Up the ASA CX Software](#), on page 9.

For the ASA CX software module, if the hard drive does not have a pre-installed image, you need to reimage the system before setting up the software. For detailed information, including the setup, see [Reimaging the ASA CX Software Module](#), on page 410.

Step 4 Modify the ASA firewall configuration as explained in [Altering the ASA Configuration for the ASA CX SSP](#), on page 12.

What to Do Next

You can now do the following:

- When managing the ASA CX directly:
 - Configure ASA CX policies using a web browser pointing to the ASA CX management address.
 - Use ASDM or the ASA CLI to redirect traffic to ASA CX.
- When managing the ASA CX with Cisco Prime Security Manager:
 - Add the ASA that contains the ASA CX SSP to the inventory.
 - Configure ASA CX policies using a web browser pointing to Cisco Prime Security Manager.
 - Use Cisco Prime Security Manager to redirect traffic to ASA CX.

ASA Configuration Restrictions for ASA CX

You cannot configure the following ASA features when using the ASA with ASA CX:

- Cisco Ironport Web Security Appliance (WSA). The **mus** commands define a relationship with a WSA appliance, which you cannot use at the same time as an ASA CX, which performs similar functions.
- Do not configure Cloud Web Security (ScanSafe) inspection for any traffic you redirect to ASA CX. If you configure both inspections for the same traffic, traffic is redirected to ASA CX only and Cloud Web Security is not applied.
- Do not enable ASA clustering; it is not compatible with the ASA CX module.

Setting Up the ASA CX Software

You can set up the ASA CX software using one of the following methods:

- Connect to the Console port and run the **setup** command. Use the console cable included with the ASA product to connect your PC to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control. See the hardware guide for your ASA for more information about the console cable.
- For the ASA CX software module, you can open a console session using the **session cxsc console** command in the ASA CLI and run the **setup** command.
- Use an SSH client to make a connection to the ASA CX management address and run the **setup** command. Log in using the username admin, default password Admin123. You should change this password as explained in this procedure.

Unless you connected Management1/0 to a network on which 192.168.8.8 is a valid address, you will use the console for initial configuration. Subsequently, you can rerun the setup command through an SSH session. The methods are equivalent, although if you change the IP address during an SSH session, you will lose the connection after you commit the changes (reestablish the connection to the new IP address).

**Tip**

For information on the commands available in the CLI, enter **help** or **?**.

Before You Begin

The **setup** command is a wizard that prompts you for the required information. Before you start the wizard, be sure you determine the correct input for the following values:

Host name for the system.

The hostname must be fewer than 65 characters and can contain characters, numbers, and hyphens only. The first and last character must be a letter or number and the hostname cannot be all numbers.

The type of addressing to use for the management IP address.

You can configure the following types of address: static IPv4, DHCP for IPv4, static IPv6, IPv6 stateless autoconfiguration. For the ASA CX software module, the address must be on the same subnet as the ASA management address, and the ASA management interface must be up and available. You can configure both IPv4 and IPv6 addressing. Do the following:

- IPv4 static address—Determine the IPv4 management IP address, subnet mask, and gateway.
- DHCP—Ensure there is a DHCP server that will respond on the management network.



Note DHCP is not recommended. The system will stop functioning correctly if DHCP changes the assigned address due to lease expiration or other reasons. We suggest you use static addressing instead.

- IPv6 static address—Determine the IPv6 management IP address and prefix length and gateway.
- IPv6 stateless autoconfiguration—IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link.



Note IPv6 stateless autoconfiguration assigns a global address based on network prefix and a device identifier. Although this address is unlikely to change, if it does change, the system will stop functioning correctly. We suggest you use static addressing instead.

DNS information.

If you do not use DHCP, you need to specify the IP addresses (IPv4 or IPv6) of the primary and optionally, secondary, DNS servers and the local domain name. If you configure both IPv4 and IPv6 management addresses, you can enter DNS addresses in either or both formats; otherwise, you must match the format of the management address.

You can also enter a comma-separated list of search domains, which are sequentially appended to host names that are not fully qualified in an attempt to resolve the name to an IP address. For example, a search domain list would allow you to ping `www` instead of a fully-qualified name such as `www.example.com`.

NTP information.

You can decide whether to configure Network Time Protocol (NTP) for system time. When using NTP, specify the NTP server names or IPv4 addresses.

You will be asked if you want to use NTP symmetric key authentication. Authentication is useful if you want to ensure your time source is trusted. If you configure authentication, follow the prompts to add the key number (e.g. 2), key type, key, and then assign the keys to your servers based on key number. Supported key types include MD, MD2, MD5 SHA, SHA1, MDC2, and RIPEMD160. Because the key must first be defined on the NTP server, obtain the keys from the server administrator. If you own the NTP server, consult the server documentation to learn how to configure authentication.

Procedure

- Step 1** Open a console session or make an SSH connection to the management IP address and log in using the **admin** username.
- Step 2** Enter the **setup** command to start the setup wizard:

Example:

```
asacx> setup
```

```

Welcome to Cisco Prime Security Manager Setup
[hit Ctrl-C to abort]
Default values are inside [ ]

```

You are prompted through the setup wizard. The following example shows a typical path through the wizard; if you enter Y instead of N at a prompt, you will be able to configure some additional settings mentioned above. Bold text indicates the values that you enter; replace these sample values with your own. In some cases, the entered value is the same as the default value for clarity; you could instead simply press Enter without typing any value.

This example shows how to configure both IPv4 and IPv6 static addresses. You can configure IPv6 stateless autoconfiguration by answering N when asked if you want to configure a static IPv6 address. If you answer N when asked if you want to configure IPv4, then IPv6 is the only address configured.

```

Enter a hostname [asacx]: asa-cx-host
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management
interface? (y/n) [N]: N
Enter an IPv4 address [192.168.8.8]: 10.89.31.65
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 10.89.31.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: Y
Enter an IPv6 address: 2001:DB8:0:CD30::1234/64
Enter the gateway: 2001:DB8:0:CD30::1
Enter the primary DNS server IP address [ ]: 10.89.47.11
Do you want to configure Secondary DNS Server? (y/n) [N]: N
Do you want to configure Local Domain Name? (y/n) [N] Y
Enter the local domain name: example.com
Do you want to configure Search domains? (y/n) [N] Y
Enter the comma separated list for search domains: example.com
Do you want to enable the NTP service?(y/n) [N]: Y
Enter the NTP servers separated by commas: 1.ntp.example.com, 2.ntp.example.com
Do you want to enable the NTP symmetric key authentication? [N]: N

```

- Step 3** After you complete the final prompt, you are presented with a summary of the settings. Look over the summary to verify that the values are correct, and enter Y to apply your changed configuration. Enter N to cancel your changes.

Example:

```

Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Restarting network services...

```

```
Restarting NTP service...
Done.
Generating self-signed certificate, the web server will be restarted after that
...
Done.
Press ENTER to continue...
asacx>
```

Note If you change the host name, the prompt does not show the new name until you log out and log back in.

Step 4 If necessary, configure the time settings.

Use the **show time** command to determine the current date, time, and time zone for the system. The default is to use the UTC time zone.

If you are using NTP, you can configure the local time zone using the **config timezone** command. If you are not using NTP, also configure the local time using the **config time** command.

Step 5 (Optional) Change the admin password.

If you have not yet changed the password for the admin user, change it now using the **config passwd** command. The command output explains password requirements.

Example:

Following is an example of changing the admin password:

```
asacx> config passwd

The password must be at least 8 characters long and must contain
at least one uppercase letter (A-Z), at least one lowercase letter
(a-z) and at least one digit (0-9).

Enter password: (type password)
Confirm password: (retype password)
SUCCESS: Password changed for user admin
```

Step 6 Enter the **exit** command to log out.

What to Do Next

The device is now ready for use. Use a browser to open the web interface as described in [Logging Into the Web Interface, on page 22](#).

Altering the ASA Configuration for the ASA CX SSP

The ASA CX SSP is a module in an ASA. All traffic first must enter the ASA before being redirected to the ASA CX SSP. In turn, after the ASA CX SSP processes traffic, it is returned to the ASA for further processing and routing to the next destination.

Thus, a correctly-configured ASA is critical to the functioning of the ASA CX SSP.

There are two basic policies that might need to be adjusted in the ASA when you add an ASA CX SSP: access rules and inspection rules.

- Access rules, whether global rules or those applied to specific interfaces, are always applied before traffic is redirected to the ASA CX SSP. Thus, the ASA CX SSP sees only the traffic already permitted, and does not process traffic that was dropped at entry to the ASA. You might want to adjust the rules to ensure that all traffic that you want the ASA CX SSP to handle is permitted.

- Inspection rules determine which traffic is inspected. The ASA CX SSP will not inspect traffic that has already been inspected by the ASA. Therefore, you must ensure that you do not inspect traffic that you intend for the ASA CX SSP to inspect. Specifically, do not inspect HTTP traffic, because HTTP inspection is one of the core functions of the ASA CX SSP. The default inspection rules on the ASA do not include HTTP inspection, so you must alter your inspection rules only if you added HTTP rules.

The following topics explain the things to consider and how to redirect traffic to the ASA CX SSP.

Configuring ASA Access Rules for ASA CX

The ASA allows access rules to be applied globally to all interfaces or specifically to one or more interface. These rules determine which traffic is permitted to pass through the device and which traffic is dropped immediately.

Determine if you need to create access rules for an interface, or global access rules that apply to all interfaces. Use ASA access rules to pre-filter the traffic before it is redirected to the ASA CX. If you already know there are classes of traffic that you never want to pass, it is efficient to drop them immediately at entry to the ASA.



Tip

Ensure that the access rules allow HTTPS access to port 443 on the ASA CX management address. If you also install PRSM Multiple Device mode, ensure that HTTPS traffic is allowed between the ASA CX, ASA, and PRSM.

The default access rules for the ASA provide the following services:

- All traffic from a higher security interface is allowed when flowing to a lower security interface. For example, all traffic entering the inside interface (security level 100) is allowed to leave the outside interface (security level 0).
- All return traffic for an allowed traffic flow is also allowed, even if it goes from a lower security interface to a higher security interface. For example, a web request from a user on the inside interface that goes to the Internet through the outside interface will result in return traffic (that is, the requested web page will appear in the user's browser, assuming that the page exists and there is a route to the web site).
- All traffic from a lower security interface to a higher security interface is dropped.

If you already have access rules, there is no requirement to change them. However, you should evaluate whether they might need to be relaxed in order to have ASA CX process certain types of traffic that you are now dropping in access rules.

Configuring ASA Inspection Rules for ASA CX

The ASA uses service policy rules to define application layer protocol inspection. Inspection is required for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports.

ASA inspection for TCP-based traffic is not compatible with ASA CX inspection. Therefore, ASA CX does not inspect TCP traffic that has already been inspected by the ASA.

**Tip**

Never inspect HTTP traffic on the ASA if you send the traffic to ASA CX. Many ASA CX features are designed specifically for HTTP traffic. Ensure that at least HTTP traffic is redirected to ASA CX, and do not inspect that traffic in the ASA.

If you send inspected HTTP traffic to ASA CX, some advanced features, such as application-based access control or URL filtering, cannot be accomplished by ASA CX. Thus, you might not get the results that you expect if you use these features.

Because HTTP inspection is not part of the default inspection rules on the ASA, you need to modify your inspection rules only if you added HTTP inspection. You have the following options:

- Remove all HTTP inspection rules from the ASA.
- Limit traffic sent to ASA CX so that it does not include inspected HTTP traffic streams. This method is an option if you are performing HTTP inspection on the ASA for specific interfaces or for specific classes of traffic based on subnet or other traffic matching criteria.

Configuring the ASA to Send Traffic to the ASA CX SSP

All traffic initially enters the ASA, and the ASA applies access rules to the traffic. You can then redirect any traffic that passes these rules to the ASA CX SSP, which then applies its policies to the traffic and sends the allowed traffic back to the ASA to be sent to its ultimate destination.

You use service policy rules to redirect traffic to the ASA CX SSP. Typically, you would redirect all packets to the ASA CX SSP. After applying policies to the traffic, the ASA CX SSP returns the permitted traffic to the ASA for further handling and routing to the next destination.

**Note**

Before redirecting traffic to the ASA CX SSP, the ASA applies interface-specific and global access rules. Thus, a service policy rule that redirects all traffic is in fact redirecting just the traffic that was permitted entry by the ASA.

To configure the ASA to redirect traffic, you can use the ASA CLI, ASDM, or PRSM Multiple Device mode. The following topics explain the configuration for ASA CLI and PRSM.

Redirecting Traffic to ASA CX Using the ASA CLI

This procedure explains how to use the ASA CLI to redirect traffic to an ASA CX SSP. The procedure assumes that the ASA is already configured and functional, for example, that you have configured ASA interfaces so that network traffic can pass through the device. Typically, at least one interface would be Internet facing, and one would be internal network facing.

Procedure

- Step 1** Log into the ASA using the Console port or SSH to the management IP address.
- Step 2** Enter **enable** and enter the required enable password to access privileged EXEC mode.
- Step 3** Enter **config t** to enter configuration mode.
- Step 4** Create the service policy rule to redirect traffic.
The class map command is:

```
cxsc {fail-open| fail-close} [auth-proxy]
```

where:

- **fail-open** specifies that if the ASA CX SSP fails for any reason, the ASA will continue to pass traffic that would otherwise be redirected to the ASA CX SSP.
- **fail-close** specifies that if the ASA CX SSP fails, the ASA will drop all traffic that would otherwise be redirected to the ASA CX SSP.
- **auth-proxy** enables the authentication proxy, which is required if you want to use active authentication in the identity policies on the ASA CX SSP. If you do not include this keyword, you can do passive authentication only.

Example:

This example shows how to update the default global policy to include redirection for all interfaces, enabling the authentication proxy and allowing traffic to pass through the ASA if the SSP fails. This command sequence leaves your other service policy rules intact, including your default inspection policies. If you want to limit the redirection to specific interfaces or traffic flows, create a new policy with class maps that define the flows to redirect (see the ASA documentation for detailed information on configuring class maps).

```
asa(config)# policy-map global_policy
asa(config-pmap)# class class-default
asa(config-pmap-c)# cxsc fail-open auth-proxy
asa(config-pmap-c)# exit
asa(config-pmap)# exit
asa(config)#
```

- Step 5** If the policy map is not already an active service policy, you need to enable it using the **service-policy** command.
If necessary, remove an existing service policy using the **no** form of the command. For example, the following commands remove a user-defined global policy and replace it with the default global policy.
- Tip** If you have an active service policy redirecting traffic to an IPS module, you must remove that policy. For example, if the policy is a global one, you would use **no service-policy ips_policy global**.

Example:

```
asa(config)# no service-policy existing_global_policy global
asa(config)# service-policy global_policy global
asa(config)#
```

- Step 6** If you enabled the authentication proxy, and you want to use a non-default port for active authentication, configure the authentication proxy port.

The authentication proxy port command is:

cxsc auth-proxy port *number*

where the port number is higher than 1024. The default authentication proxy TCP port is 885. If users must be prompted for authentication credentials, the prompting is done through this port. You can see the currently configured port using the **show run all cxsc** command.

Example:

For example:

```
asa(config)# cxsc auth-proxy port 1025
asa(config)#
```

Step 7 Enter **write memory** to save the changes to the running configuration.

Configuring ASA CX in Monitor-Only Mode

In monitor-only mode, the device is not inline to the traffic flowing through the ASA. Instead, the ASA sends a copy of the traffic to the device, which can then analyze and categorize the traffic. Monitor-only mode is intended for demonstration and evaluation purposes, and not for normal operation. If you want to operate the device as part of your network with the purpose of collecting information only, a better option is to configure the device as described in [How to Gain Insight Into Your Network Traffic](#), on page 46.

When the device is in monitor-only mode, there will be a message in the web interface banner indicating the fact.

There are many limitations to monitor-only mode:

- Monitor-only mode works in Single Device mode only. Do not attempt to add a device running in monitor-only mode to the inventory of a PRSM server.
- Some small portion of the traffic might not get categorized as it would when the device runs inline. However, the amount of miss-classified data should not impact the general analysis of the traffic.
- Several features are completely unavailable, including the following. However, these features remain in the web interface, so if you configure them, you might get unexpected results.
 - Deny actions in access policies have no meaning. All traffic is allowed, because the device is examining a copy of the traffic only. The real traffic flow remains in the ASA and is allowed or denied by ASA policies only.
 - Active authentication, configured in identity policies, does not work. Your only option for obtaining user identity information is to set up a CDA or AD Agent, for use with Active Directory, to obtain user identity passively.
 - Decryption is completely unavailable. Do not configure decryption policies.
- Monitor-only mode must be configured in both the ASA and the ASA CX. If the mode configured on the devices does not match, you might get unexpected results. If you configure the ASA redirection policy for inline mode, but put the ASA CX in monitor-only mode, all redirected traffic will be dropped.

This happens because the ASA is sending the real traffic stream to the ASA CX, but ASA CX believes it has a copy of the traffic and will not send the traffic back to the ASA for final processing. Thus, you should configure monitor-only mode on the ASA before configuring it on ASA CX.

- You must use the ASA CLI to configure monitor-only mode. You cannot use ASDM or other management applications to configure the option.
- The minimum required ASA Software release is 9.1(2).

Before You Begin

This procedure assumes you have installed the hardware and software and that you have run the **setup** command to configure the basic network settings.

Procedure

- Step 1** Configure the traffic redirection policy on the ASA to use monitor-only mode. Use the class map command **cxsc fail-open monitor-only**. You can also use the **fail-close** keyword.

Example:

The following example, in configuration mode, shows how to configure the class map and service policy for redirecting traffic to the ASA CX.

```
asa(config)# policy-map global_policy
asa(config-pmap)# class class-default
asa(config-pmap-c)# cxsc fail-open monitor-only
asa(config-pmap-c)# exit
asa(config-pmap)# exit
asa(config)#
asa(config)# no service-policy existing_global_policy global
asa(config)# service-policy global_policy global
asa(config)#
```

- Step 2** Log into the web interface for the device and configure the device to use monitor-only mode.
- a) Select **Configurations > Monitor-only Mode**.
 - b) Select **Enable Monitor-only Mode: On**.
 - c) Click **Save**.

Redirecting Traffic to ASA CX Using PRSM

This procedure explains how to use PRSM Multiple Device mode to redirect traffic to an ASA CX SSP. The procedure assumes that the ASA is already configured and functional, for example, that you have configured ASA interfaces so that network traffic can pass through the device. Typically, at least one interface would be Internet facing and one would be internal network facing.

**Note**

PRSM always configures redirection using the **fail-open auth-proxy** keywords. Fail open means that if the ASA CX SSP fails for any reason, traffic that would otherwise be redirected would instead pass through the ASA based on the ASA policies only. The **auth-proxy** (authentication proxy) keyword ensures that you will be able to configure active authentication. If you want to use **fail-close**, or omit the **auth-proxy** keyword, you must use ASDM or the ASA CLI to configure redirection.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and open the **Traffic Redirection** tab. You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Configure the following options to define the state of this policy:
- **Manage Traffic Redirection in PRSM: On/Off**—Whether you want PRSM to configure this policy on the device. If you change from **On** to **Off**, any existing redirection policy on the device is left untouched, even if PRSM configured it previously. If you change from **Off** to **On**, any existing policy is erased and replaced with the one you define here. If you select **Off**, you are done; click **Save** and skip the remainder of this procedure.
 - **Enable Traffic Redirection on Device: On/Off**—Whether to configure a traffic redirection policy on the device. If you select **Off**, any existing redirection policy is removed from the device, and no traffic is forwarded to the CX module.
- Step 3** If you elect to enable the policy, configure the following settings if desired:
- **TCP/UDP Ports**—Leave the field blank if you want all types of traffic to be redirected. You can also limit the redirection to specific TCP/UDP ports by specifying ports in protocol/port format, such as tcp/80 or udp/80. You can enter port ranges using a hyphen, for example, tcp/1-100, udp/1-100. If you enter any ports, redirection is limited to those protocols and ports; no non-TCP/UDP traffic will be redirected.
 - **Interfaces/Interface Roles**—Leave the field blank if you want traffic that passes through any interface on the device to be redirected (the policy is defined as global). If you want to limit redirection to specific interfaces, select the desired interfaces or interface role objects that define the desired names.
- Step 4** Click **Save**.
-

Troubleshooting PRSM Traffic Redirection Policies

The traffic redirection policy that you can configure in PRSM does not include all of the options available through the ASA CLI or through ASDM. Thus, you might run into the following problems when you configure redirection through PRSM:

Unsupported redirection policies

Because you can use CLI or ASDM to configure redirection policies before you add an ASA to the PRSM inventory, it is possible to configure policies that PRSM cannot manage. For example, if you use ACLs as matching conditions for the policy, PRSM will not import the policy. Instead, the traffic redirection policy for that device will be considered unmanaged. Although you can change it to a managed policy, you will not be able to recreate the same policy.

PRSM supports the following commands as part of the traffic redirection CLI:

- Class maps—Either **class-default** or the **match port** command.
- Service-policy command—Either **global** or **interface** specifications, but you cannot have a mix of both global and interface policies.

Unsupported redirection keywords

The redirection policy can include the following keywords: **fail-open**, **fail-close**, **auth-proxy**. During discovery, these keywords are ignored, and **fail-open auth-proxy** is always configured. Thus, if you configured your redirection policy with the **fail-close** keyword, or you intentionally omitted the **auth-proxy** keyword, after discovery and deployment, your policy will change.

As mentioned above, if the redirection policy includes unsupported class maps, it will not be discovered and the keywords will not be changed.



Tip The **monitor-only** keyword is also not supported, but you cannot even add a device that is configured in monitor-only mode to the inventory.

Port limitations

If you explicitly specify ports, only the TCP or UDP traffic on those ports will be processed by ASA CX. Because ASA CX policies can apply to non-TCP/UDP traffic, you could potentially write ASA CX policies that will never apply because of the limits placed on redirected traffic. For example, policies for ICMP traffic will never be matched for a device if you specify ports in the redirection policy.



Getting Started

The following topics explain how to get started with Context-Aware Security and PRSM.

- [Browser Requirements, page 21](#)
- [Changing the Language for the Web Interface, page 21](#)
- [Logging Into the System, page 22](#)
- [Web Interface Basics, page 24](#)
- [Committing or Discarding Changes, page 30](#)

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 following list indicates the minimum supported browser version for the cited platforms. You might be able to use a more recent version, or another operating system, but these versions and operating systems might not have been tested with the application, and some functions might work differently or not at all.

- Windows 7, Mac OS X—Mozilla Firefox 22
- Windows 7, Mac OS X—Google Chrome 17
- Windows 7—Windows Internet Explorer 9 (64-bit)

Some buttons and links open additional windows. Therefore, you might need to configure the browser's pop-up blocking settings to at least allow pop-ups from the application's host device.

Changing the Language for the Web Interface

You can view the web interface in English and Japanese. To get Japanese, change the preferred language setting in the browser to Japanese. You will get English for all other language settings, although dates and times might be formatted based on the selected language.

You cannot change the language or date/time format directly in the web interface.

Logging Into the System

There are two interfaces to the PRSM and CX products:

Web Interface

The main interface to the product runs in your web browser. Whether you are using Multiple Device mode to manage several devices, or Single Device mode when logging directly into a CX device, the web interface is called Cisco Prime Security Manager (PRSM). Multiple Device mode and Single Device mode interfaces look the same so that you can directly transfer your experience with one mode to the other mode. The differences relate to the availability of features related to managing multiple devices, such as the device inventory.

When you add a CX to the PRSM Multiple Device mode inventory, the web interface for the managed device becomes limited, so that you cannot inadvertently configure policies directly on the device that should be configured in PRSM Multiple Device mode. The web interface will clearly show you that the device is in managed mode, including the address of the PRSM server that is managing the device.

Command Line Interface (CLI, Console)

Use the CLI for initial system setup and troubleshooting. Once you have the system configured and running correctly, you should rarely need to enter the CLI. The method for logging into the CLI console differs based on the PRSM mode.

The following topics explain how to log into these interfaces.

Logging Into the Web Interface

Use the web interface to configure policies, settings, and other properties. To log in, you use a web browser to open the site, then log in with your username and password. The features that you can configure through the browser are not configurable through the command-line interface (CLI); you must use the web interface to implement your security policies.

The log in procedure for Single Device mode or Multiple Device mode web interface is the same; you are simply opening different web sites.

When you log into a CX device that is currently being managed by a PRSM server, the home page tells you that the device is in managed mode and it provides the address of the PRSM server that is managing it. Most of the web interface for a CX device is disabled in managed mode.

Before You Begin

Before anyone can log into the web interface, you must complete the initial system setup and connect the system to the network.

Procedure

-
- Step 1** Using a browser, open the home page of the system, for example, <https://cx.example.com>. You can use the IPv4 or IPv6 address or the DNS name, if you have configured one. Use the management address configured during system setup.

Tip If your browser is not configured to recognize the server certificate, you will see a warning about an untrusted certificate. Accept the certificate as an exception, or in your trusted root certificate store. Some versions of Firefox do not allow you to create an exception if you connect using an IPv6 address. In these cases, use a different supported browser, or configure the system with a certificate the browser will trust.

Step 2 Enter your username and password defined for the CX device or for PRSM, then click **Login**. You can use the **admin** username, which is a pre-defined user. The default admin password for a CX device is Admin123. There is no default password for PRSM Multiple Device mode; you are prompted to configure the password during initial system setup.

If the administrator defined your normal directory username as your CX device or PRSM username, you can log in as DOMAIN\username (e.g. EXAMPLE\user1), username@domain (e.g. user1@example.com), or just username.

Logging Into the ASA CX CLI

Use the ASA CX command-line interface (CLI) to set up the system and do basic system troubleshooting. You cannot configure policies through a CLI session.

To log into the ASA CX CLI, do one of the following:

- Use the console cable included with the ASA product to connect your PC to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control. See the hardware guide for your ASA for more information about the console cable.
- For the ASA CX software module, use the **session cxsc console** command in the ASA CLI to open a console session.
- Use an SSH client to make a connection to the management IP address. Log in using the **admin** username (default password is Admin123).

After logging in, for information on the commands available in the CLI, enter **help** or **?**.

Logging Into the PRSM CLI

Use the PRSM Multiple Device mode command-line interface (CLI) to set up the system and do basic system troubleshooting. You cannot configure policies through a CLI session.

To access the PRSM CLI, you use an SSH client or the VMware vSphere console for the PRSM virtual machine (VM). Read the vSphere help for detailed information about how to use the console.

The following procedure explains both methods.

Procedure

- Step 1** To use an SSH client, make a connection to the management IP address and log in using the **admin** username and password.
- Step 2** To use the VMware vSphere console, do the following:

- a) Log into the vSphere client, connecting to the vCenter Server on which you are running the PRSM VM.
- b) Select the PRSM VM from the list of VMs on the server, and open the VM Console, either in the right pane or as a separate window (by clicking the **Launch Virtual Machine Console** button in the toolbar or selecting **Inventory > Virtual Machine > Open Console**).
- c) Double-click in the Console window to enter the console, then log in using the **admin** username and password.
If you are logging into the console to recover the admin password, or to reset the system to factory defaults, log in using the **recovery** username. You must use the console to log in as the recovery user; you cannot use an SSH client.

Step 3 After logging in, for information on the commands available in the CLI, enter **help** or **?**.

Web Interface Basics

The following topics provide overview information about how to use the CX/PRSM web interface.

Your User Role Controls What You Can See and Do

Your user name is assigned to a role, and your role determines what you can do or what you can see in the user interface. If you have no authority to use a feature, the menu to access the feature does not even appear; if you have read-only access, you will not see buttons or controls that allow you to make changes.

Thus, as you read the online help or other documentation, you might find features mentioned that you cannot see or use.

You can determine your role by selecting **Administration > Users** and looking at your account.

For detailed information on the possible roles and their privileges, see [User Roles and Privileges](#), on page 364.



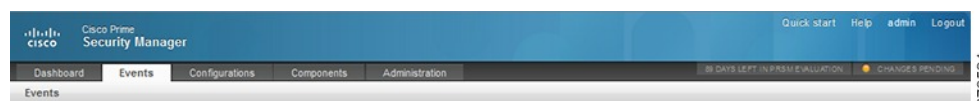
Tip

The **admin** user is the only user who can log into the CLI.

Menus

The top part of the web interface includes the main menu, which gives you access to the main pages of the application. The upper right also includes important links. Although the menus are mostly identical between Single Device mode and Multiple Device mode, there are additional commands available in Multiple Device mode.

Figure 3: PRSM Menus



Following is a description of the main menus and features of the menu bar:

- **Dashboard**—The Dashboard menu includes the primary landing page, the Network Overview, and links to each of the available dashboards. Use these features to monitor and evaluate the performance of your devices, policies, and so forth.
- **Events**—The Events menu includes the Event Viewer. Use the Event Viewer to view and analyze traffic and system events. These events can help you identify and resolve problems with user access or system performance and behavior.
- **Configurations**—The Configurations menu includes the core policies and settings, and signature and engine updates that implement your security policies. In Multiple Device mode, the Repository view **Overview** tab lists the device inventory.
- **Components**—The Components menu includes the features you use as building blocks for your policies, including policy objects and directory realms. You can also view the applications and Next Generation IPS threats for which you can configure policies.
- **Administration**—The Administration menu includes features related to managing the system, such as user account management, licensing, and so forth.
- **License Alerts**—The space in the menu bar next to the Administration menu shows license alerts if there are any current or pending issues related to product licenses. The alert indicates the problem or potential problem. Click the alert to go to the Licenses page, where you can take action.
- **Changes Pending/No Changes Pending**—The link in the far right of the menu bar is always present and takes you to the Commit and Deploy Changes page. The text of the link indicates whether there are changes that are waiting for you to commit to the database and deploy to the device or devices. When you make changes to policies, you must commit the changes to make them take effect.
- **Upper Right Commands**—The commands in the upper right include the following:
 - **Quick Start**—To open the quick start welcome page, which provides overview information and videos.
 - **Help**—To open the online help.
 - **Username**—Indicates the name of the user currently logged in. This is not a link, but helps you know which username you used to log in, in cases where you have more than one user account.
 - **Logout**—To log out of the web interface.

Lists and Tables

Lists, such as those for rule-based policies or policy objects, and tables, such as Event Viewer and dashboards, are continuously scrolling. That is, as you scroll down towards the end of a list or table, new entries are fetched and added to your view.

You will typically see some delay as items are fetched and added.

When dealing with very large lists and tables, use the filtering features to narrow down the content to make it easier to find the items that interest you.

Consider the following tips for using lists and tables:

- When filtering the policy objects list, take advantage of the object type list to target the specific object type that interests you.
- To filter on a phrase, enclose it in double quotes. For example, filtering on all remote shows matches for “all” and “remote” whereas filtering on “all remote” shows matches for that phrase only.
- Filter results are both syntactic (exact match) and semantic (sensitive to the meaning of the search term). For example, a search for 10.100.10.1 will also match 10.100.10.0/24. Results consider not just the name of the items but their contents.
- Event Viewer has unique filtering features, which are described in [Filtering Events](#), on page 188.
- You can sort dashboard tables by clicking a column header. Clicking the header toggles between ascending and descending sort on that column.
- You can filter any list or table that shows time-stamped data by time ranges. For change history, you can even filter by username.

Policy, List, and Alert Icons

Policy lists might show several icons for policies or policy sets. Some of these icons can appear elsewhere in the web interface. Icons are also used for action buttons.

To determine the purpose or meaning of an icon, mouse over it or click it. The tool tip provides details about the icon; these details can change depending on the context. In some cases, the tip includes a link to perform an action related to the notification. For action buttons, the tip might include links for the device type, and you need to click the link for the device you are targeting.

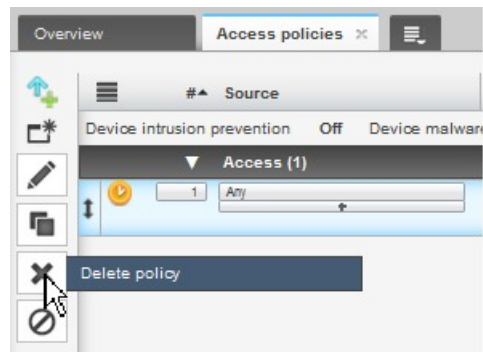
Typically you will see icons related to the following:

- Pending changes—Edits that you have made that are saved but not yet committed to the device configuration.
- Alerts—Mostly seen in dashboards and the inventory list, indicate device problems, such as device unreachable.
- User conflicts—Potential or actual conflicts between your edits and edits made by other users.
- License problems—Expired or expiring feature licenses and their impact on policies that use features covered by the license.
- Packet capture—Indicates that the access policy is enabled for packet capture.

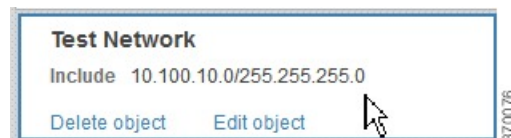
Select or Mouse Over List Items to See Commands

Commands or buttons that operate on items in a list are revealed only when you select the item or mouse over it. Selection or mouse-over can also be required for other features, such as events in Event Viewer, so in general, if you are not sure what to do on a page, start selecting or mousing-over items to see if commands appear on the item.

In the following example, selecting the first access policy shows several buttons to the left related to the policy, such as **Edit Policy** and **Delete Policy**.



Similarly, the following example of the objects list shows that mousing over a list item is sufficient to reveal the commands related to it. You could also select the object to see the commands.

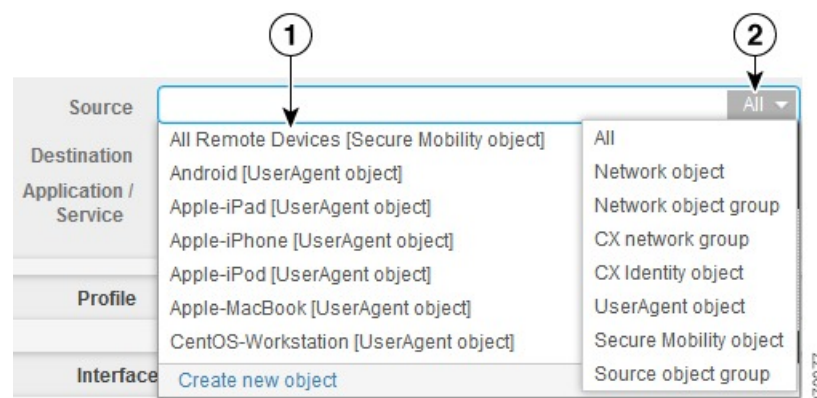


Selecting Items

Many fields allow you to enter information or to select items from a list. In many cases, you can select multiple items, and even items of different types. For example, in the Source field of an ASA CX access policy, you can select multiple network, identity, user agent, Secure Mobility, and source policy objects. When entering ticket IDs, you can type in multiple items in addition to selecting existing items from a list.

The following illustration shows an item picker field. Although an item picker is similar to a traditional combo box, it is unique because it allows you to select multiple items, and the item picker can contain two separate drop-down lists.

Figure 4: Item Picker with Object and Object Type Lists



1	Object list.

2	Object type filter.

If you can select more than one type of item, you can select an item type to filter the list to show objects of that type only. For example, if you select **CX Network Group** from the filter list for the Source field, you see network group objects only in the item list. Selecting a type from the filter list does not limit what you can enter in the field; instead, it limits what you see in the list so that you have an easier time finding the item you want to select.

Following are some additional tips for item pickers:

- When you click in an item picker and start typing, the item list is automatically filtered to show only those items that contain the string anywhere within the item name (not necessarily from the start of the item name).
- You can select multiple items from the list using Shift+click.
- If you select multiple items in an item picker, the items are separated by spaces. To view details on a selected item, click it.
- If you are not sure which object to pick, mouse over the object in the list and click the **View Details** link to the right. If you can change the object, you can do so from the details window by clicking **Edit Object**.
- If an object with the desired contents does not already exist, you can create a new one by clicking **Create New Object** or **Create New Profile** at the bottom of the drop-down list.
- If you want to remove an item, mouse over it and click the **X** to the right of the item name. To add another item, click in the empty space to the right of the last item.

Getting Help

Online help is included with the product. The help not only covers the web interface, it also includes a reference of the commands available in the CLI. The help covers both Single Device mode and Multiple Device mode, so it might address features not available in the interface you are using.

To open the help, click the **Help** link in the upper right corner of the web interface. This link typically opens a page relevant to the application page you are currently viewing.

When you are filling in a form, for example, when creating a policy, there is typically a **Help** link in the upper right corner of the input form. Click this link for more information about the form.

The online help opens in a different window than the application. When you open the help system, you can use the table of contents or the index to find more information. You can also use Search to find information in the help system.



Tip

You can also find more information and documentation on Cisco.com at <http://www.cisco.com/go/asacx> or <http://www.cisco.com/c/en/us/support/security/asa-next-generation-firewall-services/tsd-products-support-series-home.html>.

Viewing Basic System Information

You can see basic information about the system by selecting **Administration > About PRSM**. The information shown on this page includes the following:

- PRSM server name—The hostname for this system as defined using the setup command in the CLI.
- Version—The software version running on the system.
- PID—The product identifier.
- Serial number—The system's serial number.
- Device mode—Whether you are logged directly into a CX device (Single Device mode) or a PRSM server (Multiple Device mode).
- Last Upgrade Attempt—When you last tried to upgrade the system software.
- Last Upgrade Status—The result of the last attempt to upgrade the system software.

Working with Other Users

You can create multiple users who can configure policies in the web interface. However, if there are multiple users, there is the possibility that two or more users might try to edit the same object, policy, or other setting at the same time.

The web interface will not prevent multiple users from editing the same item. This ensures that if someone is away on vacation, or leaves the company, with uncommitted changes, other users can make needed edits without being prevented from doing so.

But this does mean that you can find yourself in a situation where your edits, or intended edits, conflict with what another user wants to do.

It is critical for you to understand that only a single user can commit changes to a given item at one time. If you make edits to an object that another user edited, and the other user commits changes before you do, you will have to discard all of your changes, not just to that object, but to all other objects you changed, even those without conflicts. If you find that you need to change an item, and another user has already edited it, work directly with the other user to ensure changes are committed in a timely manner so that you can complete your changes.

In the web interface, icons indicate whether an item has been edited by another user, and the type of conflict that exists for that object:

- Warning—This item is being edited by another user. Mouse over the icon to see the user name. Except in extraordinary circumstances, you should not edit the item until the user commits changes.
- Pending—You and other users have made edits to this item. Whoever commits their changes first will create a Commit conflict for the other users.
- Commit—Another user has committed changes to this item that you have also edited. You must now discard all of your pending changes, not just the change to this item. At this point, you would waste your time making additional edits before discarding changes. You can examine your pending changes to understand the edits you will have to redo.

Troubleshooting Web Interface Problems

If you run into problems using the web interface, first ensure that you are using a supported browser (see [Browser Requirements](#), on page 21).

The following are some problems you might encounter when using the web interface and their solutions.

Value errors or other javascript errors appear, or the operation you are trying to perform fails (such as an attempt to delete something).

Try logging out and clearing your cache. The problem might be stale browser cache entries.

Browser popup indicates that a slow script is running.

You must select the option to continue waiting for the script.

A simple operation seems to be stuck.

If you select a menu or click a button, and the browser or interface indicates that it is waiting for a very long time (30 seconds or more), it is possible that another user has made some change that is affecting communications between your browser and the device. For example, another user might have changed the certificate used for the web interface, or changed critical settings using the **setup** command in the CLI. Try refreshing the browser page, or log out and log back in. But be aware that some operations can require a long time, such as loading pages that display long lists of policies or objects, so please be patient before assuming there is a communication problem.

Typing usernames in an identity object or user account form does not show users from the directory.

When you enter usernames for directory-based items, for example, when creating identity objects or defining remote (directory) user accounts for PRSM access, the drop-down list should provide auto-complete suggestions fetched from the AD/LDAP directory. This problem has been seen to occur if the DNS server is configured incorrectly so that a directory's DNS name resolves to the wrong IP address, but there could be other problems in communicating between the system and the directory or in your directory configuration. If you are not seeing these auto-complete suggestions, check the following:

- For AD realms, select **Components > Directory Realm**, mouse over the realm and click **Edit Realm**, then click the **Test Domain Join** link. If domain join fails, correct the problem.
- Select **Components > Directory Realm**, then mouse over each directory and click **Edit Directory**. Click the **Test Connection** link to check communications with the directory. Fix any problems you encounter.
- Verify that the **User Search Base** and **Group Search Base** values are correct for each directory. You must evaluate the AD/LDAP configuration to validate your entries.

Committing or Discarding Changes

When you update a policy or setting in the web interface, the change is not immediately applied to the device. There is a two step process for making configuration changes:

- Make your changes.

- Commit your changes.

This two-step process gives you the opportunity to make a group of related changes without forcing you to run a device in a “partially configured” manner. For example, when adding a directory realm, you also need to add an identity policy for the realm, and you might also want to create new access policies or alter your existing policies to use the new realm.

After you complete the changes you want to make, use the following procedure to commit them.

Procedure

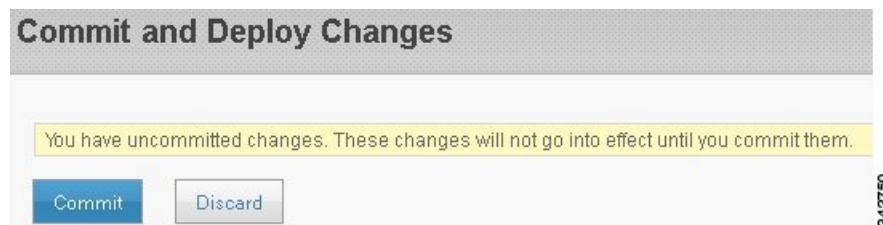
- Step 1** Click the **Changes Pending** link in the menu bar to open the Commit and Deploy Changes page.



If there have been no changes since the last commit, this link is labeled **No Pending Changes**. You can still click the link to get to the Commit and Deploy Changes page, for example, if you want to check deployment status. You can also get to the page by clicking the Pending Change icon displayed on a changed item, such as a policy object or policy.

(Multiple Device mode.) If there are changes to an ASA, you can click **View ASA device transcript (CLI)** to view the delta change (changes since the last commit), full configuration, transcript of communications during deployment, and any out-of-band change issues.

- Step 2** Evaluate the Pending Changes list to ensure that you want to apply your changes. All changes since your last commit are listed on the **Pending Changes** tab in expanding/collapsing folders. The tab is not explicitly labeled in Single Device mode.
- Step 3** Click **Commit** to update the device configuration.



Managed devices are updated as follows:

- CX device, Single Device mode—The changes are immediately applied. The page shows the progress of the deployment.
- CX device, PRSM Multiple Device mode—The CX device is notified of the changes. Each affected device retrieves the changes and applies them. This is a polling model.
- ASA—The changes are sent (pushed) to the ASA and applied to the ASA configuration.

Tip If you decide you do not want to commit the changes, click **Discard**. All policies or settings configured since the last commit are erased; you cannot selectively undo or discard a single change among a group of changes.

Step 4 (PRSM Multiple Device mode only.) To track the deployment status of your changes, you are automatically taken to the **Deployment Status** tab.

Watch the messages and status indicators to track the progress of the job. A successfully completed job remains on the page until you leave the page. To see completed jobs in the future, either click the **View Historic Changes** link on this tab, or select **Administration > Change History**.

If there are other active deployment jobs, they are also listed on this tab.

If there are problems with deployment, a section lists the devices that require your attention. There can be two main problems: ASA out-of-band (OOB) changes, where the configuration was changed outside of PRSM control, or the device has an out-dated configuration (e.g. you recovered the database on that device or successive failed deployments left the device down-level). Make the following selections and click **Deploy** to redeploy changes:

- Deselect any devices that you do not want to retry.
- For devices with out-of-band changes, you must elect to overwrite those changes to get a successful deployment.

The Commit and Deploy Changes Page

Use the Commit and Deploy Changes page to save changes to the database and deploy them to all affected devices.

The page looks significantly different based on the PRSM mode:

- **Single Device mode**—When directly configuring a CX device, the page simply allows you to commit or discard changes.
- **Multiple Device mode**—In this mode, the page contains all features and is also referred to as the Deployment Manager. The page is divided into tabs to present views of current changes and a list of current deployment jobs with their changes and status.

To open the Commit and Deploy Changes page (the Deployment Manager), click the link in the far right of the menu bar. The name of link varies:

- **Changes Pending**—This link name indicates that you have outstanding changes that need to be committed.
- **No Pending Changes**—This link name indicates that there are no outstanding changes that can be committed.

In PRSM Multiple Device mode, the Commit and Deploy Changes page is divided into separate tabs. In Single Device mode, the Pending Changes tab is shown but it is not presented as a tab.

Pending Changes tab

Click this tab to view outstanding changes that need to be committed. All changes for the currently-logged-in user are shown, and each change indicates whether it is a modification of an existing item, or the creation of a new item. You cannot see the changes for another user.

(Multiple Device mode.) If there are changes to an ASA, you can click **View ASA device transcript (CLI)** to view the delta change (changes since the last commit), full configuration, transcript of communications during deployment, and any out-of-band change issues.

The following buttons are available:

- **Commit**—Click this button to commit the changes to the database and to start a deployment job. Be patient while the database commit occurs. In Multiple Device mode, you are then moved to the Deployment Status tab where you can track the results of the job.
- **Discard**—Click this button to erase all listed changes. You cannot selectively delete a single change. To discard any change, you must discard them all. Therefore, if you simply want to remove a small number of changes from a long list of changes, go back to the appropriate page and delete or modify the item as appropriate.

Deployment Status tab

(Multiple Device mode only.) Click this tab to view current deployment job results. The list of jobs is ordered from most recent to the oldest.

Each deployment job is given a number so you can see the relative order of the jobs; higher numbers being more recent than lower numbers. Click the version heading to open the job details if they are not already in view. The job information includes the date and time of the job, the names and addresses of the devices affected by the job, the overall job status, the deployment status for each device within the job, and the user who is committing the change. The types of change are listed; for some changes, whether it was new (INSERT) or a change to an existing setting (UPDATE) is also indicated.

The deployment status tab includes the following controls:

- **View Historic Changes**—Click this link to open the Change History page, where you can see older deployment jobs and other committed versions that are no longer active. You can also get to the Change History page by selecting **Administration > Change History**.
- **Devices Require Your Attention**—This section appears if a deployment job failed for one or more devices. The failed devices are listed in this section. To attempt a redeployment, make the following selections and click **Deploy** to redeploy changes:
 - Deselect any devices that you do not want to retry.
 - For devices with out-of-band changes, where the configuration was changed outside of PRSM control, you must elect to overwrite those changes to get a successful deployment.

Managing Deployment Jobs

In PRSM Multiple Device mode, deployment jobs apply a set of changes to the devices affected by the changes. Each time you commit changes to the database, the changes are deployed to the applicable devices. You use the Deployment Manager to commit changes and to view the results of the current deployment jobs. You can run a single deployment job at a time.

In PRSM Single Device mode, when you commit changes, the changes are applied immediately. The following procedure explains the various things you can do when managing deployment jobs.

**Tip**

In Single Device mode, the Commit and Deploy Changes page is not divided into tabs; where this procedure says to click the **Pending Changes** tab, you do not need to do anything, that tab is always active and unnamed.

Procedure

Step 1 Click the link in the far right of the menu bar to open the Commit and Deploy Changes page. The name of the link varies:

- **Changes Pending**—This link name indicates that you have outstanding changes that need to be committed.
- **No Pending Changes**—This link name indicates that there are no outstanding changes that can be committed.

Step 2 Do any of the following:

- **View current changes**—(All modes.) To see the changes that you have made since the last time you committed changes, select the **Pending Changes** tab. The policies, objects, settings, and other changes are shown in expanding/collapsing folders. These changes are view only; you cannot modify them from this view.
 - **Commit changes**—(All modes.) To commit the changes you have made and deploy them to all applicable devices, select the **Pending Changes** tab and click **Commit**. In Single Device mode, the changes are immediately deployed. In Multiple Device mode, you are taken to the **Deployment Status** tab, where you can track the progress of deployment.
 - **Discard changes**—(All modes.) To discard changes that you do not want to implement, select the **Pending Changes** tab and click **Discard**. All changes since the last commit are discarded; you cannot selectively discard a subset of changes.
 - **View currently active jobs**—(Multiple Device mode only.) To view currently active jobs, select the **Deployment Status** tab. The list shows all active jobs, including the job status, the date and time of the job, and the user who committed the changes. Click a version heading to open it and view the changes that were committed, the devices that were affected, and the deployment results for each device. When the deployment is completed, the job is no longer available from this page. Click the **View Historic Changes** link to see completed jobs.
 - **Redeploy changes to failed devices**—(Multiple Device mode only.) If the deployment to one or more device failed, a section on this page lists the devices that require your attention. To attempt a redeployment, make the following selections and click **Deploy** to redeploy changes:
 - Deselect any devices that you do not want to retry.
 - For devices with out-of-band changes, where the configuration was changed outside of PRSM control, you must elect to overwrite those changes to get a successful deployment.
-

Viewing Change History

The Change History page shows a history of deployment jobs or other committed changes. Whenever you click **Commit** on the Commit and Deploy Changes page, a change history version is created. Any version that involved changing device configurations is also called a deployment job in PRSM Multiple Device mode.

Each version is given a number so that you can see the relative order of the jobs, higher numbers being more recent than lower numbers.

Use the change history list to review past changes, including the status of deployment jobs, who made the changes, which changes were made, and so forth. These versions provide auditing information that you can use for internal tracking purposes.

Procedure

Step 1 Select **Administration > Change History**.

The list is initially filtered to show versions committed in the past one day only.

Tip In PRSM Multiple Device mode, you can also get to the Change History page by clicking the **View Historic Changes** link on the Deployment Status tab on the Commit and Deploy Changes page.

Step 2 Set filter conditions to limit which records are displayed. You can use the following criteria:

- **Device**—(PRSM Multiple Device mode only). Enter a filter string to do a partial match for a device IP address or host name, then click **Filter**. You can select the criteria to filter on from the drop-down list.
- **Time Range**—Select a time limit for the list. You can select the last 30 minutes, hour, 24 hours, 7 days, or 30 days, or select **Custom Date Range** to specify starting and ending times (minimum of 30 minutes). The time is based on the time zone defined on the device, not the zone configured on your workstation.
- **Users**—Select the user who committed the changes. Select **All Users** (the default) if you do not want to restrict the list to a particular user.

Step 3 Analyze and evaluate version records.

Versions are displayed in order from most recent to oldest. The Version heading summarizes the job, including version number, date and time, and the user who committed the changes.

In PRSM Multiple Device mode, each version that involved device deployment includes the names and addresses of the devices affected by the job, the overall job status, and the deployment status for each device within the job. If a job deployed to a device that has since been deleted from the inventory, the device name and IP address is removed from the job information and the device is indicated as deleted.

You can do the following with the version records:

View Changes

Click the Version heading to open the record and view the changes committed for the version.

If the action for a setting says INSERT, the setting was new (inserted into the database). An UPDATE action indicates a change to an existing setting.

Evaluate Failures

In PRSM Multiple Device mode, if a job includes failed devices, the Version heading includes a red icon and the list of failed devices is shown even when the job record is collapsed. A history of failures is also visible.

You can attempt to redeploy to these failed devices by clicking the **Pending Changes/No Pending Changes** link in the menu bar and then selecting the **Deployment Status** tab. The devices will be listed on the tab as devices that need attention. There can be two main problems: ASA out-of-band (OOB) changes, where the configuration was changed outside of PRSM control, or the device has an out-dated configuration (e.g. you recovered the database on that device or successive failed deployments left the device down-level). Make the following selections and click **Deploy** to redeploy changes:

- Deselect any devices that you do not want to retry.
- For devices with out-of-band changes, you must elect to overwrite those changes to get a successful deployment.

View CLI and Transcripts

(Multiple Device mode.) If there are changes to an ASA, you can click **View ASA device transcript (CLI)** to view the delta change (changes since the last commit), full configuration, transcript of communications during deployment, and any out-of-band change issues.

Dealing with Out-of-Band Changes

(Multiple Device mode only.) An out-of-band change is any change to the configuration of a managed ASA device that happens outside the control of PRSM. These changes could be made through CLI or through another management application such as ASDM. PRSM considers a change to be out-of-band only if the change is to a feature or command that PRSM can configure; changes are not considered out-of-band if they are made to unmanaged features.

You can configure a global setting to determine how out-of-band changes are handled during deployment. If you elect to fail deployment when out-of-band changes are discovered, you can relax your setting and redeploy the job after it fails.

The following procedure explains how to configure the global setting.

Procedure

Step 1 Select **Administration > Out-of-band Settings**.

Step 2 Select your default out-of-band change behavior:

- **Abort and alert**—If there is an out-of-band change, fail the deployment. This option allows you to investigate the changes. If you want to keep them, you can duplicate the change in PRSM, then elect to overwrite the change in the deployment job for the device before redeploying.
- **Overwrite**—If there is an out-of-band change, overwrite it without warning. This option prevents deployment failures, but can erase configuration changes that you might want to keep.

Step 3 Click **Save**.

You can also click **Restore to Default** if you want to use the default setting.

When Do Configuration Changes Become Active?

When you deploy changes to a device, the changes become part of the device configuration as soon as the device applies the changes. However, if a change involves how traffic transmitted through the device is handled, these changes will not necessarily affect existing connections.

Thus, if you make policy changes to deny certain types of traffic that were previously allowed, you might see some delay in effectiveness:

- Connections that start after policy commit are handled according to the new rules.
- HTTP has the concept of “persistent connections,” which means that a single traffic flow can carry many separate transactions. A browser does not necessarily close a persistent connection when navigating to a new web page. When a browser tries to go somewhere new, it first checks to see if it already has a connection open to that destination, and if it has a connection, it reuses the connection if possible.

Thus, if your policy change would otherwise prevent the user from seeing a page on a particular site, a user with an existing connection to the site might be able to continue browsing to new pages for an indeterminate period of time (typically a matter of a few minutes). This behavior differs from the normal behavior of web proxies, which apply policy to transactions individually.

Deployment Job and Device Status

Each deployment job, and the devices contained within the job, have their own statuses that indicate the results of the job. The following sections explain the possible deployment statuses for jobs and devices.

Deployment Job Status

Following are the possible deployment job statuses. These statuses apply to the job as a whole.

- **Queued**—The job is ready and waiting in the deployment queue to be started.
- **Deploying**—The job is running and changes are being deployed to the applicable devices.

A job in Deploying state might have timed out while waiting to hear from a CX device, so you could have more than one job in Deploying state. Because the CX device pulls configuration changes from the PRSM server, rather than PRSM actively sending the changes, the device must notify the PRSM server that the update was successful. Eventually, the status of a Deploying job will change to Deployed or Deploy Failed. The job is considered to have failed if a response is never received.

- **Deployed**—The job successfully deployed changes to all applicable devices.
- **Partially Deploy**—The job successfully deployed to some but not all applicable devices.
- **Deploy Failed**—The job failed to deploy to any applicable device.

Device Status

Each device has a separate status. When included in a deployment job, the status is based on the results of deployment with that device. In some cases, detailed messages help you identify specific problems; if a [+]
appears next to the status message, click it to see detailed messages.

Following are the possible statuses, which include statuses related to device discovery as well as configuration deployment:

- **Discovering**—PRSM is currently loading the device configuration into the database.
- **Discovered**—PRSM successfully discovered the device. It is available for deployment.
- **Discover Failed**—An error occurred when PRSM was discovering the device. You must delete the device and try adding it again to the inventory. You cannot do anything else with a device in this state.
- **Deleting**—You deleted the device and PRSM is in the process of removing all device information from the database.
- **Delete Failed**—PRSM failed to delete the device from its inventory. Try again.
- **Queued**—The device is in the queue ready to have changes deployed.
- **Deploying**—PRSM is currently deploying changes to the device. For a CX device, this indicates that PRSM has notified the device to retrieve the changes.
- **Deployed**—The changes were successfully deployed to the device.
- **Deploy Failed**—The changes could not be deployed to the device. The most likely problems include the following:
 - Failed connecting to device, invalid username or password—If the error indicates that the username and password is invalid, it typically means that the password for the user specified when adding the device to the inventory has changed. Update the credentials from the device overview tab.
 - Deployment timed out for device—The device did not respond within a reasonable amount of time. Ensure that the device is online, available, and that there are no network problems that are causing significant delay.
 - The CX device did not acknowledge that it received the deployed change—The device did not acknowledge receiving the updated configuration. Verify that there are no network problems and retry the deployment.
- **Unavailable**—The device cannot be reached. Common messages you might see are:
 - Device is unavailable (not reachable)—Ensure that there are no problems in the network path between the PRSM server and the device, and that the device is powered on and functional, then retry the deployment job.
 - Certificate for device is out of date—The TLS/SSL certificate for the device in PRSM is no longer current. To fetch a new certificate, select the device in the inventory list and use the **Refresh Certificate** command. You can then redeploy the job.
 - Device is unavailable (not reachable) for unknown reason—A detailed message is shown to help you determine the problem.
- **Out of Band**—An out-of-band change was discovered on the ASA device.

- **Not Allowed**—The device's current state does not allow deployment. You can deploy to devices that have been successfully discovered, deployed to, failed to deploy to, or whose current state is unknown. You cannot deploy to devices that are currently in the process of being discovered, for which discovery failed, which are in the process of being deployed to, or which you deleted from the inventory.



Use Cases for ASA CX

The following topics explain some common tasks you might want to accomplish with ASA CX.

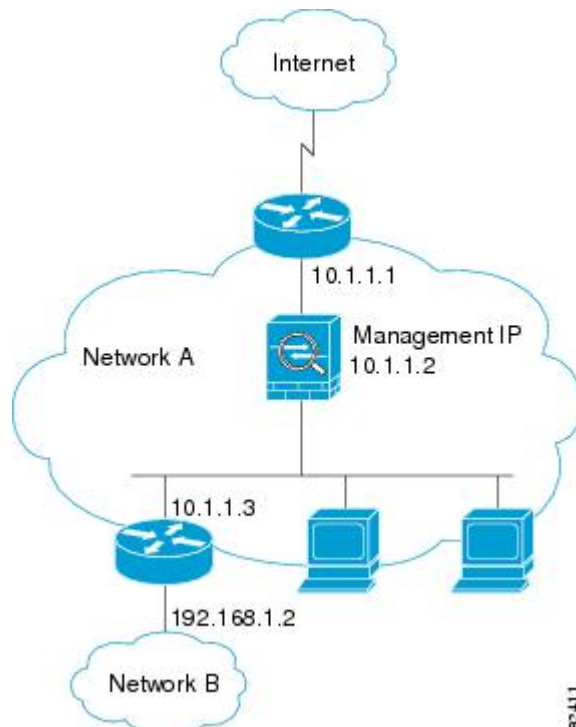
- [How to Set Up ASA CX in Transparent Mode, page 41](#)
- [How to Configure High Availability, page 44](#)
- [How to Gain Insight Into Your Network Traffic, page 46](#)
- [How to Control Application Usage, page 51](#)
- [How to Use Passive Authentication, page 53](#)
- [How to Create Access Policies that Apply to AD/LDAP User Groups, page 56](#)
- [How to Implement an Acceptable Use Policy \(URL Filtering\), page 59](#)
- [How to Enable Access to YouTube for Schools, page 61](#)
- [How to Block Malware Using Web Reputation, page 63](#)
- [How to Scan for Threats \(IPS Filtering\), page 66](#)
- [How to Monitor and Control AnyConnect Secure Mobility Devices, page 67](#)

How to Set Up ASA CX in Transparent Mode

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices. Instead, the ASA connects the same network between its interfaces.

The following figure shows a typical example of a transparent firewall. You configure a bridge group interface to group the interfaces that are connected to the same network.

Figure 5: Transparent Firewall Network



Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network. When you configure the ASA to operate in transparent mode, the ASA CX automatically operates in transparent mode.

The following procedure shows a basic example of configuring an ASA in transparent mode. You configure the mode using the ASA CLI. For more extensive information on configuring transparent mode, see the chapter on transparent mode in any of the ASA configuration guides, for example, http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/intro_fw.html.

Before You Begin

This example assumes that you have already configured the ASA CX network settings as described in [Setting Up the ASA CX Software](#), on page 9. However, you can do the basic setup after completing this procedure.

Procedure

-
- Step 1** Log into the ASA CLI using the Console port.
If you change the firewall mode while using an SSH client, you will be disconnected when the configuration is cleared, and you will have to reconnect to the ASA using the console port in any case.
- Step 2** Enter configuration mode and set the firewall mode to transparent.

Example:

```
ciscoasa# conf t
ciscoasa(config)# firewall transparent
INFO: UC proxy will be limited to maximum of 2 sessions
by the UC Proxy license on the device
```

Step 3 Configure the interfaces and the bridge group.**Example:**

The following example shows how to create the inside and outside interfaces, add them to bridge group 1, and assign a management IP address to the bridge group. The example assumes there is no previous interface configuration and uses show commands to verify input.

```
ciscoasa(config)# int g0/0
ciscoasa(config-if)# no shut
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# bridge-group 1
ciscoasa(config-if)# int g0/1
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# no shut
ciscoasa(config-if)# bridge-group 1
ciscoasa(config-if)# int BVI1
ciscoasa(config-if)# ip address 10.1.1.2 255.255.255.0
ciscoasa(config-if)# sh run int g0/0
!
interface GigabitEthernet0/0
 nameif inside
 bridge-group 1
 security-level 100
ciscoasa(config-if)# sh run int g0/1
!
interface GigabitEthernet0/1
 nameif outside
 bridge-group 1
 security-level 0
ciscoasa(config-if)# sh run int BVI1
!
interface BVI1
 ip address 10.1.1.2 255.255.255.0
ciscoasa(config-if)# exit
ciscoasa(config)#
```

Step 4 Configure the traffic redirection policy.**Example:**

The following example shows how to redirect all traffic to the ASA CX with the authentication proxy enabled, which supports active authentication policies. If the ASA CX is unavailable for any reason, traffic continues to pass through the ASA based on ASA security policies (fail-open).

```
asa(config)# policy-map global_policy
asa(config-pmap)# class class-default
asa(config-pmap-c)# cxsc fail-open auth-proxy
asa(config-pmap-c)# exit
asa(config-pmap)# exit
asa(config)#
```

Step 5 If the policy map is not already an active service policy, you need to enable it using the **service-policy** command.

If necessary, remove an existing service policy using the **no** form of the command. For example, the following commands remove a user-defined global policy and replace it with the default global policy.

Example:

```
asa(config)# no service-policy existing_global_policy global
asa(config)# service-policy global_policy global
asa(config)#
```

Step 6 Enter **write memory** to save the changes to the running configuration.

What to Do Next

You can now configure ASA CX security policies and monitor traffic using the ASA CX web interface.

How to Configure High Availability

Cisco High Availability (HA) enables network-wide protection by providing fast recovery from faults that may occur in any part of the network. With Cisco High Availability, network hardware and software work together and enable rapid recovery from disruptions to ensure fault transparency to users and network applications.

Configuring high availability on ASA devices requires two identical units connected to each other through a dedicated failover link, with one active unit passing traffic while the other unit waits in a standby state. The health of the active unit and its interfaces is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs and the standby unit begins processing traffic.

The following conditions must be met in order to configure two devices for high availability:

- Both units must be the same model, have the same number and types of interfaces, and the same amount of RAM installed.
- Both units must be operating in the same mode (routed or transparent, single or multiple context). They must have the same major (first number) and minor (second number) software version.
- Each must have the proper licenses.

You can use Cisco Prime Security Manager (PRSM) to manage and monitor pairs of ASA devices operating in Active/Standby failover mode. These devices can optionally include CX modules, which will also fail over. You also can manage CX modules as an HA pair if they reside in ASAs that are otherwise not supported, such as those configured in multiple-context mode. Each HA pair is managed as a unit.

The following functions are supported in PRSM for HA configuration:

- Active/Standby failover in single-context routed mode.
- Stateless and Stateful failover are supported.
- Interface failover monitoring.
- Interface standby configuration for all interfaces that require failover monitoring.
- Failover LAN configuration.
- HTTP replication, Key assignment, and failover criteria configuration.

Failover Triggers

Failover is triggered if any of the following occur:

- The primary ASA experiences a hardware or power failure.
- The primary ASA experiences a software failure.
- Too many monitored interfaces fail.
- The **no failover active** command is entered on the active unit, or the **failover active** command is entered on the standby unit.

ASA CX Failover Caveats

Please note the following ASA CX failover caveats:

Scenario	Solution with caveats
Stateful Failover	No stateful failover of transactions going through CX-1: • In-progress sessions will be processed by the ASA-2 correctly (they are not sent to CX-2). • New sessions are sent to the CX-2.
Events	Events are shown from both systems, but they are not aggregated.
CX User Authentication	CX user authentication does not fail over for in-progress transactions.
Decryption	For decrypted traffic, the user must clear the browser cache and reload the page.

Configuring and Monitoring an HA Pair

The following steps outline how to configure a device pair for failover, and make it available for monitoring in PRSM. (The steps are described in detail in [Managing High Availability](#), on page 307.)

Procedure

-
- Step 1** Use the Adaptive Security Device Manager (ASDM) or the command-line interface (CLI) to configure the pair of ASA devices for Active/Standby failover.
 - Step 2** Add the devices to the PRSM inventory.
 - Step 3** Go to the High Availability page for the active member of the paired devices to verify failover configuration. Be sure **HTTP Replication** is enabled for the devices. This allows HTTP connections to be included in the state information replication between devices, which in turn allows users to browse, stream and download files freely without interruption during a failover.
-

How to Gain Insight Into Your Network Traffic

Before you start implementing policies on ASA CX, you might find it beneficial to gain insight into the traffic that is actually occurring on your network. You can set up ASA CX to process all of your traffic without prohibiting any traffic. By leaving your existing firewall rules on the ASA intact, you will be able to use the monitoring capabilities of the ASA CX to analyze network traffic without reducing your current level of security.

ASA CX reporting helps you answer the following questions:

- What is my network being used for?
- Who is using the network the most?
- Where are my users going?
- What devices are they using?
- What policies are being hit the most?

The implicit access policy behavior for ASA CX is to allow all traffic. You can use this policy, which is named “Implicit Allow” in dashboards, but you might want to create an explicit allow all traffic policy. Although this rule is sufficient for providing a good amount of traffic analysis data, you need an identity policy to get user-based information in the dashboards.

The following procedure explains how to set up the ASA CX to monitor traffic and provides an overview of the end-to-end process of configuring and monitoring policies.

Procedure

Step 1 Redirect all traffic from the ASA to the ASA CX.

When defining the redirection policy, do not limit the policy to specific interfaces or ports. Instead, simply send all traffic to ASA CX, so that dashboards will reflect all traffic. Note that if traffic is dropped at the incoming interface by ASA access rules, that traffic will not be sent to ASA CX.

For detailed information on redirecting traffic, see [Configuring the ASA to Send Traffic to the ASA CX SSP, on page 14](#).

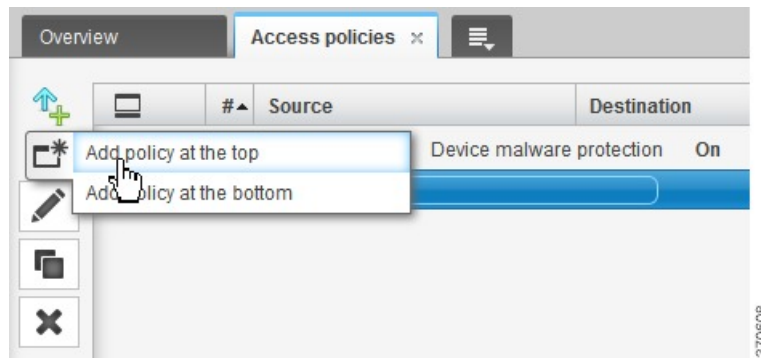
Step 2 (Optional) Configure an explicit Allow All Traffic access policy.

- a) Select **Configurations > Policies/Settings** and open the **Access Policies** tab.

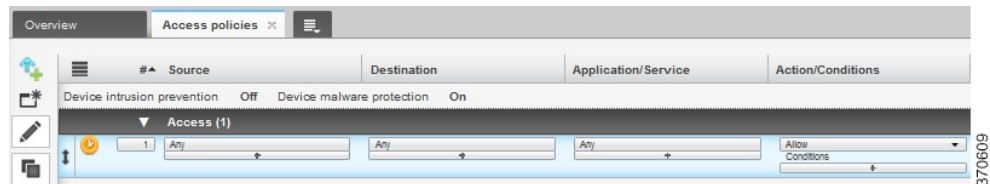
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Tip In Multiple Device mode mode, this tab includes access policies for both the CX device and the parent ASA. Ensure that you are working in the CX access policy section.

- b) Select the policy set and click the **Add policy at the top** button.



- c) In the access policy properties, enter a name for the policy, such as “Allow All Traffic,” keep the default “Any” for all traffic matching fields, and click **Save Policy**. The policy list will now show your new policy. The clock icon indicates that this is a pending change; the policy is not active until you commit changes.



Step 3 (Optional) To gain insight into user behavior, you need to configure an identity policy to ensure that the user associated with a traffic flow is identified. You have two non-exclusive options for obtaining user information:

- Use active authentication, which can transparently authenticate using NTLM or Kerberos or prompt users to respond to an authentication prompt when they make a network connection through the ASA CX. The benefit of active authentication is that you obtain user identity. However, users are authenticated only when they make their first HTTP connection attempt after logging into the network. Thus, there can be delay between login and having user identity for the user’s traffic, which can affect the value of identity-based policies.
- Set up a Context Directory Agent (CDA) or Active Directory (AD) agent to passively obtain user-to-IP address mappings based on AD login. The benefit of using CDA or AD agent is that user identity is obtained at user login, so your identity-based policies can apply to the user before the user makes an HTTP connection.

The following procedure explains how to use active authentication. You will need to create a directory realm, add directories to the realm, and then configure the identity policy.

- Select **Components > Directory Realm**.
- Select **I Want To > Add Realm**.
- In the Add Realm form, enter a name for the realm and select the directory type. If you select Active Directory, you also need to enter a primary domain name and username/password that can join the domain. For more detailed information, see [Configuring Directory Realms](#), on page 230. Click the **Test Domain Join** link to verify that you can join the device to the AD domain. The following illustration is an example of configuring an AD realm.

Name * Our AD Realm

Description

Directory Type * Active Directory

Primary domain * example.com

Join username Administrator@example.com

Join password

Test domain join

* Required

343758

- d) Click **Save** to create the directory realm and return to the list of realms. If you are directly configuring an ASA CX (in Single Device mode), and this is your first realm, an identity policy for the realm is automatically created.
- e) Mouse over the realm you created and click **Add New Directory**.

Realm

Filter Enter filter criteria Filter

Realm Name	Realm Type
▼ Our AD Realm	Active Directory

[Add new directory](#) [Delete realm](#) [Edit realm](#)

370582

- f) In the Add Directory form, enter the DNS name or IP address of the directory and the other attributes required to obtain user and group information from the directory. For detailed information on each field, see [Directory Properties, on page 231](#). Click the **Test Connection** link to verify the values you enter. The following illustration is an example of configuring an AD directory. Note the test result message next to the **Save** button.

Directory hostname / IP ^{*}

Port ^{*}

AD login name ^{*} e.g. "myname@cisco.com"

AD password ^{*}

User search base e.g. "cn=users,dc=cisco,dc=com"

Group search base e.g. "ou=groups,dc=cisco,dc=com"

Group membership attribute ^{*}

Test connection

^{*} Required

Connection succeeded Save Cancel

- g) Click **Save** to add the directory to the realm.
The following illustration shows the completed realm. Note the pending changes clock icon, which indicates you must commit the change before it becomes part of the active configuration.

Realm Name		Realm Type	
▼ Our AD Realm		Active Directory	
			
URL	AD login name	Group attribute	
ldap://ad.example.com:389	Administrator@example.com	dc=example,dc=com	member

- h) Select **Configurations > Policies/Settings** and open the **Identity Policies** tab.
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- i) Do one of the following to configure the identity policy:
- If an identity policy was automatically created when you added the realm, select the policy and click the **Edit Policy** button.
 - Otherwise, select the identity policy set and click the **Add policy at the top** button.
- j) Select **Get Identity via Active Authentication** as the action and adjust the other policy settings as needed. If using AD, you can select the type of authentication to perform. Select Advanced to allow the device to negotiate the strongest method supported by your AD directory server and the client. You can also adjust the policy name and the source and destination if you do not want the policy to apply to all sources and destinations. For information on the other options, see [Identity Policy Properties](#), on page 236.

The following illustration shows the action settings when configuring active authentication with a negotiated authentication method.

k) Click **Save Policy**.

Step 4 Commit your changes.

Policy changes are not immediately operational. You must explicitly commit them. This step ensures that you can make several closely-related changes without forcing you to operate the device in a partially-configured state.

a) Click the **Changes Pending** link on the right side of the menu bar.



b) Click **Commit** to commit the changes to the configuration database.

Step 5 Use the dashboards and Event Viewer to analyze your traffic.
You can view the following:

- Overall network usage.
- Top users, applications, destinations, policies hit.
- Local vs. remote (VPN) traffic, top device types.
- Threat information.
- Device health and performance.

You can also drill down detailed information, or link to events in the Event Viewer. In Event Viewer, you can view events as they happen in real time or view events that occurred in a specific time period.

What to Do Next

As you identify undesirable activity, you can create new policies or modify existing ones to implement your acceptable use policies:

- Use access policies to control the use of applications and web sites.
- Use access policies to selectively drop traffic to low reputation web sites.
- Use access policies to selectively prevent file uploads or downloads.
- Use decryption policies to decrypt traffic flows or to explicitly bypass decryption for TLS/SSL traffic that is safe and allowable. For example, you could create a rule that does not decrypt traffic to sites in the Finance web category. Decryption can give you additional insight into encrypted traffic, such as application behaviors and more precise threat analysis.
- Adjust identity policies if you do not want to require everyone to actively authenticate. For example, if you use Active Directory, you could set up a CDA or AD agent and obtain user information passively.

How to Control Application Usage

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.

ASA CX includes the Application Visibility and Control engine (AVC engine), which let's you apply deeper controls to particular application types. The AVC engine inspects web traffic to gain deeper understanding and control of the 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 access 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.

Using the AVC engine, you can block or allow applications by application type or tag, or by a particular application. You can also apply deeper controls to particular application types. For example, you can allow media traffic but disallow file uploads.

The AVC engine can dynamically receive updates from the Cisco update server, adding support for new applications, types, or tags.

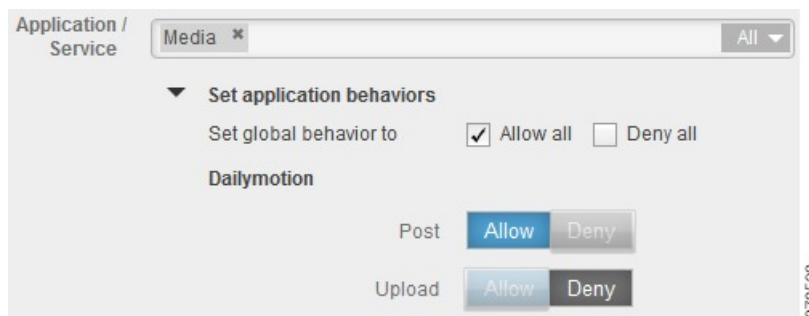
**Note**

If an application uses an encrypted traffic flow (TLS/SSL), you might want to pair an access policy for the application with a decryption policy that will decrypt the traffic flow. Although some encrypted flows might be assigned an application, others will require decryption. Additionally, decryption might provide a more specific application assignment (for example, Facebook Games rather than just Facebook), and behaviors can be identified only with decryption. However, be aware that many applications do not work with decryption, so you might have to use URL filtering to control some TLS/SSL applications.

The following example shows how to allow media applications, such as YouTube, yet block file uploads.

Procedure

- Step 1** Select **Configurations > Policies/Settings** and open the **Access Policies** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Tip** In Multiple Device mode mode, this tab includes access policies for both the CX device and the parent ASA. Ensure that you are working in the CX access policy section.
- Step 2** Use one of the **Add Policy** buttons to add a new policy.
If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.
- Step 3** Enter a name for the policy and modify the source and destination fields if you want to limit the policy to specific networks. Leave source and destination as Any to create a policy for all uses of media applications on the network.
Keep **Allow** as the action.
- Step 4** In the Application/Service field, select **Media [Application Type]**.
When you select an application, type, or tag, if the applications contain any configurable behaviors, the behaviors appear beneath the Application field. For example, YouTube has Post and Upload behaviors. Behaviors provide granular control of activities available in an application, but not all applications have explicitly identifiable behaviors.
- In this example, because we are trying to block file uploads through media applications, select Deny as the action for the Upload behavior for all applications listed. Ignore the **Set Global Behavior To** check boxes; these simply reset all toggles to “allow” or “deny” for your convenience and are not part of the configured policy.



- Tip** Explore other application types to determine if there are additional upload behaviors that you would like to restrict.

Step 5 Click **Save Policy**.



Step 6 If necessary, move the policy to the appropriate location in the policy list.

Step 7 Commit your changes.

How to Use Passive Authentication

To see user-based information in dashboards, or to implement user-based policies, the identity of the user associated with a traffic flow must be known. This requires that the user provide identification when connecting to the network.

You have two options for obtaining user identification. You can use passive authentication, where the identity of the user is captured when the user logs into the network domain through Active Directory (AD), or you can actively prompt the user for authentication. If you are using OpenLDAP, active authentication is the only available method. The following table compares and contrasts these methods.

Table 1: Comparing Passive and Active Authentication

Passive Authentication	Active Authentication
A mapping between the user name and IP address of the user's workstation is obtained during log in to the domain. The mapping is collected by the Cisco Context Directory Agent (CDA) or Cisco AD Agent, which sends the mapping to the ASA CX. Supports AD only.	Supports basic authentication for LDAP and AD, and also NTLM and Kerberos for AD. Authentication occurs when the user attempts an HTTP connection only.
Best-effort user identification, not real authentication.	Real authentication.
Useful for applications and clients that do not support active authentication.	The client used to access the network must support active authentication, that is, it must be able to supply authentication information or prompt the user to supply it.
Completely transparent to the user	NTLM and Kerberos are usually transparent, while basic authentication shows a popup to the user to obtain username and password.
The CDA or AD agent is required. The agent is separate software that you must install and configure on a server in the network. It communicates with the AD server and with ASA CX.	No agent is required.

ASA CX uses the Cisco CDA or AD agent software to obtain passive authentication information for users in the network. When a user logs into Active Directory, the user's IP address mapping is sent to the agent, which then communicates the mapping to ASA CX.

User group membership is obtained directly from the AD or LDAP server; the ASA CX does not use the AD agent for this information.

The following procedure explains how to set up the AD agent and configure it for use in ASA CX.

Before You Begin

- Configuring a CDA or AD agent is optional. Configure it only if you want to support passive mappings. Note that if you do not support passive mappings, you must force active authentication in your authentication rules or you will not have user names available for access control, and events and dashboards will not include user information.
- Successful authentication is not required for network access. If the user fails to authenticate, whether passively or actively, it simply means that user identity is not available for traffic flows for the user.

Procedure

-
- Step 1** Install and configure the AD agent.
Follow the procedures in the product documentation:
- CDA—*Installing and Configuring Context Directory Agent*, http://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10.html.
 - AD Agent—*Installation and Setup Guide for the Active Directory Agent*, http://www.cisco.com/c/en/us/td/docs/security/ibf/setup_guide/ad_agent_setup_guide/ibf10_install.html
- Step 2** Configure CDA or AD agent to recognize the ASA CX device following the procedures in the agent documentation.
For CDA, the ASA CX is considered a consumer device. For AD agent, it is considered a client.
For both agents, you can either use the device's IP address, or you can add the subnet on which the device resides.
You also must define the RADIUS shared secret. You will need to define the same string in the ASA CX configuration. This secret encrypts and protects communications between ASA CX and the agent.
- Step 3** In PRSM (Single Device mode or Multiple Device mode), identify the CDA or AD agent (note that the web interface calls it AD Agent, but the newer CDA is also supported):
- a) Select **Configurations > Policies/Settings** and open the **AD Agent** tab.
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
 - b) Enter the DNS host name or IP address of the CDA or AD agent.
 - c) For **Password**, enter the RADIUS shared secret.
 - d) If you have a secondary CDA or AD agent configured for the device, click **Add Secondary CDA Agent** and fill in the settings.
 - e) Click **Save**.
- Step 4** If you have not created an AD realm, create a directory realm to identify the AD servers from which the CDA or AD agent is collecting login information:

- a) Select **Components > Directory Realm**.
- b) Select **I Want To > Add Realm**.
- c) In the Add Realm form, enter a name for the realm, select Active Directory as the directory type and enter a primary domain name and username/password that can join the domain.
Click the **Test Domain Join** link to verify that you can join the device to the AD domain. For more detailed information, see [Configuring Directory Realms, on page 230](#)
- d) Click **Save** to create the directory realm and return to the list of realms. If you are directly configuring an ASA CX (in Single Device mode), and this is your first realm, an identity policy for the realm is automatically created.
- e) Mouse over the directory realm and click **Add New Directory**. Enter the information for the primary AD server and click **Save**.
Repeat the process to add all of the AD servers for the domain. If necessary, rearrange them in priority order. For detailed information on the directory properties, see [Directory Properties, on page 231](#).

Step 5 Select **Configurations > Policies/Settings**, open the **Identity Policies** tab, and create or edit the identity policy for the realm to provide the desired service.
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

To use the passive mappings obtained from CDA or AD agent, the identity policy for the AD realm must use the **Get Identity Using AD Agent** action.

You can optionally enable active authentication if there is no passive mapping for a user's IP address by selecting **Yes** for the active authentication question. Also select the desired authentication type. For more information, see [Identity Policy Properties, on page 236](#).

The screenshot shows the configuration form for an identity policy. The 'Realm' dropdown is set to 'Our AD Realm'. The 'Action' dropdown is set to 'Get identity using AD agent'. Below this is a question: 'Do you want to use active authentication if AD agent can't identify user?' with a 'Yes' button selected. The 'Authentication type' dropdown is set to 'Advanced', with a note below it: 'Advanced tries Kerberos first, then NTLM and then Basic. See how to configure'. The 'Exclude user agent' dropdown is set to 'Any', with a 'Create new object' link below it. A vertical label '285292' is on the right side of the form.

- Step 6** Click **Save Policy**.
Keep in mind that identity policies are applied first-match, so if you include a rule with source = any and destination = any, that rule will prevent all subsequent rules from ever being matched. If necessary, move the policy to the desired location in the policy set.
- Step 7** Click the **Changes Pending** link in the menu bar to open the Uncommitted Changes page.
- Step 8** Click **Commit** to commit the changes to the configuration database.

How to Create Access Policies that Apply to AD/LDAP User Groups

You might want to create policies that grant different levels of access to different users. For example, you might have a contract with a partner that allows access to a partner site for specific employees only. If the partner cannot, or does not want to, control access at the server by creating accounts for the allowed users, you can block access at the firewall using a user-based access policy that specifies a group name defined in your directory server, such as Active Directory.

The following procedure shows how to create a pair of access policies that controls access to a destination, allowing only those users who are members of a specific user group. The procedure assumes that:

- You have already created a user group named ContractTeam in Active Directory.
- You have defined a directory realm for your active directory servers in PRSM.
- Your identity policies are set up to require or allow for active authentication. You can optionally use CDA or AD agent to acquire user identity.
- The partner site is a web site. If the partner site is not a web site, use a network group object to specify the IP address instead of a URL object as shown in this example.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and open the **Access Policies** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Tip** In Multiple Device mode mode, this tab includes access policies for both the CX device and the parent ASA. Ensure that you are working in the CX access policy section.
- Step 2** Create a policy that blocks all access to the partner site.
- Use one of the **Add Policy** buttons to add a new policy.
If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.
 - Enter a name for the policy.
 - Select **Policy Action: Deny**.
 - Keep **Any** as the traffic source.
 - Click in the **Destination** field and select **Create New Object** at the bottom of the drop-down list to create a URL object that identifies the partner site.
 - Enter a name for the object, for example, Partner A Site.
 - Select **URL Object** for **Object Type**.
 - Enter the DNS name of the partner site in the URL field, for example, contractAserver.example.com, in the **URL** field of the **Include** list.

Create URL object

Name *

Object type

Description

Tags

Ticket ID

Include

URL

Web category

URL objects

- i) Click **Save Object** to save the object and add it to the destination field.

Create Policy

Policy Name *

Enable Policy ☒ On ☐ Off

Policy Action

Eventing ☒ On ☐ Off

Capture packets ☐ On ☒ Off

Source

Destination

Application / Service

- j) Click **Save Policy**.
The policy is added to the policy set. If the policy is not already positioned correctly, move it to the desired position.

Step 3 Create a policy that allows access to the partner site to users who are members of a specific user group.

- Select the policy you just created and click the **Add Above Policy** button.
- Enter a name for the policy.
- Keep **Policy Action: Allow**.
- Click in the **Source** field and select **Create New Object** at the bottom of the drop-down list to create an identity object that identifies the user group.
- Enter a name for the object, for example, Partner A Contract Team.
- Select **CX Identity Object** for **Object Type**.

- g) Enter the user group name in the format `Realm_Name\group_name`, for example, `Our AD Realm\ContractTeam`, in the **Groups** field of the **Include** list. As you type, matching names defined in the directory appear in the drop-down list; select the group from the list as it becomes available.

Create CX Identity object

- h) Click **Save Object** to save the object and add it to the source field.
 i) Select the URL object you created above in the **Destination** field.

- j) Click **Save Policy**.
 The policy is added to the policy set above your deny policy.

Step 4 Commit your changes.

Going forward, only users who are members of the group can connect to the partner site. Keep in mind that group members only can access the partner site, so a user must be identified to the network or the user will be denied entry. Thus, if a member of the group connects to your network, but is not required to have identity by your identity policies, the user will not match this policy and will not be able to get to the partner site.

How to Implement an Acceptable Use Policy (URL Filtering)

You might have an acceptable use policy for your network. Acceptable use policies differentiate between network activity that is appropriate in your organization and activity that is considered inappropriate. These policies are typically focused on Internet usage, and are geared towards maintaining productivity, avoiding legal liabilities (for example, maintaining a non-hostile workplace), and in general controlling web traffic.

You can use URL filtering to define an acceptable use policy with access policies. You can filter on broad categories, such as Gambling, so that you do not need to identify every individual web site that should be blocked. Cisco's URL database categorizes over 20 million web sites worldwide in over 60 languages, and is automatically updated every five minutes.

The following procedure explains how to implement an acceptable use policy using URL filtering. For purposes of this example, we will block the Gambling, Games, and Pornography categories, and an unclassified site, badsite.example.com.

You must have a Web Security Essentials license to use category-based URL filtering.

Procedure

- Step 1** Select **Configurations > Policies/Settings** and open the **Access Policies** tab.
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
Tip In Multiple Device mode mode, this tab includes access policies for both the CX device and the parent ASA. Ensure that you are working in the CX access policy section.
- Step 2** Use one of the **Add Policy** buttons to add a new policy.
If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.
- Step 3** Enter a name for the policy, for example, Block Bad Sites.
- Step 4** Select **Policy Action: Deny**.
- Step 5** Keep **Any** as the traffic source.
- Step 6** Create the URL object that will define the destinations that users are not allowed to access:
 - a) Click in the **Destination** field and select **Create New Object** at the bottom of the drop-down list to create a URL object that identifies the objectionable categories and sites.
 - b) Enter a name for the object, for example, Bad Sites.
 - c) Select **URL Object** for **Object Type**.
 - d) Enter the DNS name of the undesirable site in the **Include: URL** field, in this example, badsite.example.com.
 - e) Select **Gambling** in the **Include: Web Category** field.
 - f) Select **Games** in the **Include: Web Category** field.
 - g) Select **Pornography** in the **Include: Web Category** field.

Create URL object

Name *

Object type

Description

Tags

Ticket ID

Include

URL

Web category

URL objects

343811

- h) Click **Save Object** to save the object and add it to the destination field.

Create Policy

Policy Name *

Enable Policy

Policy Action

Eventing

Capture packets

Source

Destination

Application / Service

370595

Step 7 Click **Save Policy**.

The policy is added to the policy set. If the policy is not already positioned correctly, move it to the desired position.

	1	Any	Bad Sites	Any	Deny Conditions

370596

Step 8 Commit your changes.

Going forward, if you want to add other sites to your Bad Sites list, you merely need to add the site or category to the URL object; you do not need to create a new policy.

How to Enable Access to YouTube for Schools

YouTube provides access to free educational videos from YouTube EDU (<http://www.youtube.com/education>). However, schools often want to block access to non-educational videos on YouTube, to reduce student distraction. YouTube for Schools provides a way for schools to limit access to educational videos without blocking all YouTube content.

YouTube for Schools offers schools the ability to pluck only the videos they want, scrubbed of all comments and linked only to other related educational videos.

In order to achieve this, the school or the school district has to register with YouTube, and YouTube will give a unique ID to the school or the school district. This unique ID needs to be passed in the HTTP header "X-YouTube-Edu-Filter" in all outgoing HTTP Request messages to youtube.com or yimg.com. For example:

```
X-YouTube-Edu-Filter:0LmSsk7HVX5iodWe_RoTY
```

You can use an access policy to inject this header, thus implementing your YouTube for Schools restrictions. You also need to decrypt YouTube traffic to inject the header into HTTPS requests to YouTube.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and open the **Access Policies** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Tip** In Multiple Device mode mode, this tab includes access policies for both the CX device and the parent ASA. Ensure that you are working in the CX access policy section.
- Step 2** Use one of the **Add Policy** buttons to add a new policy. If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.
- Step 3** Enter a name for the policy, for example, YouTube for Schools.
- Step 4** Select **Policy Action: Allow**.
- Step 5** Keep **Any** as the traffic source. Alternatively, if you have a identity object that defines the student body, you could select that object so that teachers and other staff can still access all of YouTube.
- Step 6** For destination, select the **YouTube for Schools URL** object.
- Step 7** Create the header-injection profile object for your YouTube for Schools ID.
- Open the **Profile** section, click in the **Header Injection** field, and select **Create New Object**.
 - Enter a name for the object, for example, YouTube for Schools ID.
 - Enter your ID in the **Header Value** field. The domain match default is the YouTube for Schools URL object, which you can change if you have an object that contains at least the same content.

Create Header-injection profile

Name* YouTube for Schools ID

Tags Enter associated keyword strings

Ticket ID Enter Ticket ID strings

Domain match YouTube for Schools *

Header name X-YouTube-Edu-Filter

Header value* 0LmSsk7HVX5iodWe_RoTY

371201

d) Click **Save** to save the object and add it to the Header Injection field.

Step 8 Click **Save Policy**.

The policy is added to the policy set. If the policy is not already positioned correctly, move it to the desired position.

1 Any + YouTube for Schools + Any +

Allow

Conditions

YouTube for Schools ID +

Time Range

-None- +

371202

Step 9 Create the matching decryption policy:

a) Open the **Decryption Policies** tab.

If you have not yet enabled decryption, first go to the **Decryption Settings** tab and click the **Help** link for detailed information.

b) Use one of the **Add Policy** buttons to add a new policy.

c) Enter a name for the policy, for example, Decrypt YouTube for Schools.

d) Enter the same source and destination used in the access policy, in this example, Any for source, YouTube for Schools URL object for destination.

e) For action, select **Decrypt Everything**.

f) Click **Save Policy**.

The policy is added to the policy set. If the policy is not already positioned correctly, move it to the desired position.

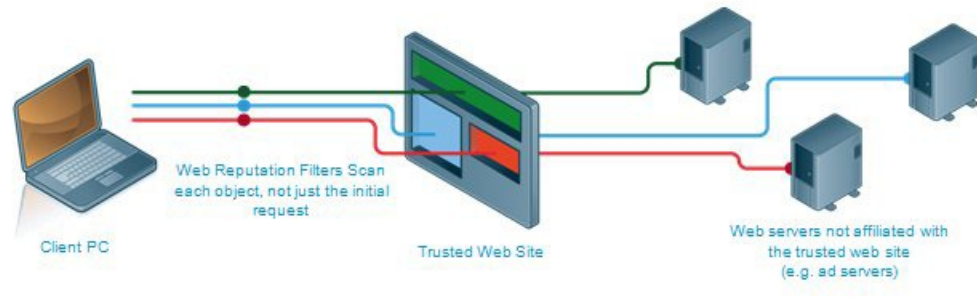
1 Decrypt YouTube for Schools Any YouTube for Schools Any Always decrypt for inspection

371203

Step 10 Commit your changes.

How to Block Malware Using Web Reputation

Users are continually at risk of obtaining malware from Internet sites. Even trusted sites can be hijacked to serve malware to unsuspecting users. As illustrated below, web pages can contain objects coming from different sources. These objects can include images, executables, Javascript, advertisements, and so forth. Compromised web sites often incorporate objects hosted on external sources. Real security means looking at each object individually, not just the initial request.



The Cisco Threat Operations Center uses dynamic updates and actionable intelligence obtained from ASAs, IPSs, Email security appliances, web security appliances, and system administrators to calculate a web reputation score for web sites. Web reputation is a statistical assessment based on context and past behavior and combines many factors of varying significance into one correlated metric. Similar to a person's credit score, web reputation is a continuous value along a graduated scale from -10 to 10. By defining a low reputation zone, you can implement predictive, zero-day protection against low reputation sites, the ones that are most likely to serve malware to your users.

Following is a general guideline to the web reputation scores:

-10 to -6

Sites in the lowest reputation zone are dedicated or hijacked sites that persistently distribute key loggers, root-kits, and other malware. Also included are phishing sites, bots, and drive-by installers. Sites in this reputation range are almost guaranteed to be malicious.

The pre-defined default web reputation profile defines this zone as the low reputation zone.

-6 to -3

Sites in this zone tend to be aggressive ad syndication and user tracking networks. These sites are suspected of being malicious, but maliciousness has not been confirmed.

-3 to 3

Sites in this zone tend to be well managed, responsible content syndication networks and user generated content sites.

0 to 5

Sites in this zone have some history of responsible behavior or third party validation.

5 to 10

Sites in this zone have a long history of responsible behavior, have significant traffic volume, and are widely accessed.



Tip

To look up the reputation of a site, select **Components > Web Filtering Categories**, then select **I want to > Look up web reputation score**.

To implement reputation-based processing, you apply a web reputation profile to the following types of policy:

- Access policies that allow traffic. By adding a web reputation profile, the policy will in general allow matching traffic, but drop any traffic from a low reputation site. You can apply the profile to any or all access policies that have the Allow action.
- Decryption policies whose action is Decrypt Potentially Malicious Traffic. By adding a web reputation profile, any low reputation sites that match the policy will be decrypted, so that access policies have knowledge of the content of the traffic. The access policies can then drop the traffic if configured to do so. Even if you do not have a matching access policy that drops the traffic, decrypting the low reputation traffic provides data for reports that is otherwise unavailable for encrypted TLS/SSL traffic flows.

For access policies, you can configure a device-level profile and have the policy use that profile. You can then easily change your default filtering policy by editing the **Malware Protection** settings.

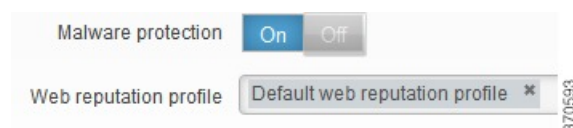
The following procedure shows how to implement reputation-based processing to drop or decrypt traffic flows for sites in the -10 to -6 zone. This example assumes that you have defined your access policies, that you have enabled decryption, and that you have some decryption policies that use the Do Not Decrypt action (or that you would like to reduce the amount of traffic that you decrypt).

Procedure

Step 1 Configure the device-level web reputation profile.

Although this is optional, the easiest way to implement web reputation filtering is to define a reputation profile to apply across your policies. You can configure the access policy to use the profile you define here. Then, changing your reputation settings is as easy as changing the object selected at the device level. You can also simply edit the object.

- Select **Configurations > Policies/Settings** and open the **Malware Protection** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Select **Default web reputation profile** as the device-level web reputation profile



- Click **Save**.

Step 2 Select **Configurations > Policies/Settings** and open the **Access Policies** tab.

(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Tip In Multiple Device mode mode, this tab includes access policies for both the CX device and the parent ASA. Ensure that you are working in the CX access policy section.

Step 3 Add the web reputation profile to the desired access policies.

- a) Select the “Allow” access policy that you want to modify and click the **Edit Policy** button.
- b) In the Profile section, select **Device Level Profile (Default web reputation profile)** in the **Web Reputation** field.

The screenshot shows the 'Profile' configuration page. It includes a 'Bandwidth limit' field set to 'No Limit', a 'Safe search' toggle set to 'On', a 'File filtering' dropdown, a 'Web reputation' dropdown set to 'Device level profile (Default web reputation profile)', and an 'NG IPS' dropdown set to 'Device level profile (Default NG IPS profile)'. There are also buttons for 'Mbps' and 'Kbps' and an information icon.

If you want to define a different low reputation range, select an existing profile or select **Create New Profile** at the bottom of the drop-down list and create your own profile. Name your object and simply move the slider to the top of your low reputation range, then click **Save Object**.

- c) Click **Save Policy**.
Repeat the process for all access policies you want to modify.

Tip You can quickly add reputation profiles to policies by clicking into the action column of a policy and selecting the desired profile. You do not need to open the edit form for each policy.

Step 4 Add the web reputation profile to the desired decryption policies.

You can configure a web reputation profile only if you use the Decrypt Potentially Malicious Traffic action, in which case specifying a profile is required. Thus, to add a profile, you must also change the action, which might mean you need to create new policies. Consider adding the profile to policies that use the Do Not Decrypt action, or to Decrypt Everything policies if you want to back off the blanket decryption requirement.

- a) Select **Configurations > Policies/Settings** and open the **Decryption Policies** tab.
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- b) Select the decryption policy that you want to modify and click the **Edit Policy** button.
- c) In the Action section, change the action to **Decrypt Potentially Malicious Traffic**.
- d) Select **Default web reputation profile** or another profile of your choosing in the **Web Reputation** field.

The screenshot shows the 'Action' and 'Web reputation' configuration page. The 'Action' dropdown is set to 'Decrypt potentially malicious traffic' and the 'Web reputation' dropdown is set to 'Default web reputation profile'.

- e) Click **Save Policy**.

#	Name	Source	Destination	Service	Action	Interface roles
1	Decrypt Malicious	Any	Any	Any	Decrypt malicious	Any to Any

Repeat the process for all decryption policies you want to modify. Add new policies as needed.

Step 5 Commit your changes.

How to Scan for Threats (IPS Filtering)

Next Generation IPS (Intrusion Prevention System) filtering analyzes network traffic in real time, comparing the traffic contents against known threats. If a connection matches a threat, you can drop the connection to block the threat. You can also choose to monitor but allow, or completely ignore, threats that you decide are benign.

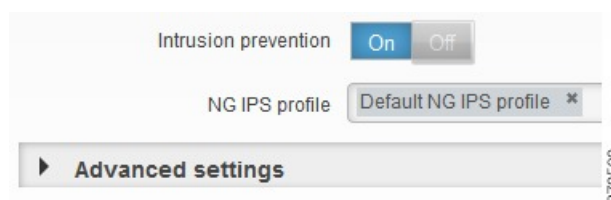
The Cisco Security Intelligence Operations Center develops signatures that identify threats. Multiple signatures can map to a single threat. New signature sets are downloaded on a regular basis unless you disable updates. You can also implement automatic blocking of blacklisted sites, which are sites considered to be always dangerous.

The following procedure shows how to implement threat scanning using the default profile. This example assumes that you have defined your access policies. You must have the Next Generation IPS license to enable the service.

Procedure

Step 1 Enable Next Generation IPS filtering and select a device-level NG IPS profile. You must enable the Next Generation IPS service, it is disabled by default. Although selecting a device-level profile is optional, the easiest way to implement Next Generation IPS filtering is to define an NG IPS profile to apply across your policies. You can configure the access policy to use the profile you define here. Then, changing your Next Generation IPS settings is as easy as changing the object selected at the device level. You can also simply edit the object.

- Select **Configurations > Policies/Settings** and open the **Intrusion Prevention** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Select **Intrusion Prevention: On** to enable Next Generation IPS filtering.
- Select **Default NG IPS profile** as the device-level profile



d) Click **Save**.

Step 2 Select **Configurations > Policies/Settings** and open the **Access Policies** tab.
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Tip In Multiple Device mode mode, this tab includes access policies for both the CX device and the parent ASA. Ensure that you are working in the CX access policy section.

Step 3 Add the NG IPS profile to the desired access policies.

- a) Select the “Allow” access policy that you want to modify and click the **Edit Policy** button.
- b) In the Profile section, select **Device Level Profile (Default NG IPS profile)** in the **NG IPS Profile** field.

The screenshot shows the 'Profile' configuration page. It includes a 'Bandwidth limit' section with a text box set to 'No Limit' and radio buttons for 'Mbps' and 'Kbps'. Below that is a 'Safe search' section with 'On' and 'Off' buttons. The 'File filtering' section has a text box with the placeholder 'Select a file filtering profile to block specific file types'. The 'Web reputation' section has a dropdown menu showing 'Device level profile (Default web reputation ...)'. The 'NG IPS' section has a dropdown menu showing 'Device level profile (Default NG IPS profile)'. A vertical label '370589' is on the right side of the form.

If you want to define a different NG IPS profile, select an existing profile or select **Create New Profile** at the bottom of the drop-down list and create your own profile. Name the object and adjust the sliders to determine the zones you will block (deny), allow and monitor (alert, that is, generate events), and allow and do not monitor (ignore, that is, do not generate events). You can also configure exceptions for these zones if you know of specific threats that fall into a zone but which you want to treat differently. Click **Save Object** when you are done.

Keep in mind that the score for a threat can change over time, so a threat can move between zones as its relative danger assessment changes.

You can see descriptions of the various threats by selecting **Components > Threats**.

- c) Click **Save Policy**.
Repeat the process for all access policies you want to modify.

Tip You can quickly add NG IPS profiles to policies by clicking into the action column of a policy and selecting the desired profile. You do not need to open the edit form for each policy.

Step 4 Commit your changes.

How to Monitor and Control AnyConnect Secure Mobility Devices

If you configure remote access VPN on the parent ASA, ASA CX can use information about the remote VPN users who connect with the AnyConnect Secure Mobility client. Information about the clients are available

in various dashboards, and you can also configure access and decryption policies that are based on location and client type. If you configure identity policies to collect user identity information, user information is also available in dashboards and for access and decryption control.

You can implement controls on the following types of remote access VPN client:

- Cisco IPsec VPN Client—IKEv1/IPsec connections.
- Cisco AnyConnect Secure Mobility Client version 2.5+—SSL VPN and IKEv2/IPsec connections.



Note

Clientless (browser-based) SSL VPN is not supported. You will not be able to apply Secure Mobility policies to these types of connections. However, they will be subject to your other access and decryption policies. Site-to-site VPN traffic is also not considered as matching Secure Mobility objects.

The following procedure summarizes what you need to do to use the AnyConnect Secure Mobility features of the ASA CX.

Procedure

-
- Step 1** Install the AnyConnect Secure Mobility client on client devices.
There are AnyConnect clients for a wide range of devices. Review the following information for specific instructions:
- AnyConnect Secure Mobility release notes—
<http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-release-notes-list.html>
 - AnyConnect Secure Mobility user guides for various client types—
<http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-user-guide-list.html>
- Step 2** Configure the clients and the ASA to provide remote access VPN support.
Find specific instructions in the *Cisco AnyConnect Secure Mobility Client Administrator Guide*. You can find the guide for your AnyConnect version at:
<http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html>
- Step 3** Select **Dashboard > User Devices** to view information on Secure Mobility clients.
You can also see information on Secure Mobility clients in the Top Sources dashboard on the network overview, **Dashboard > Network Overview**.
- Step 4** (Optional) Create access or decryption policies to selectively control Secure Mobility traffic.
For example, you might want to limit the bandwidth used by Secure Mobility clients by denying access to bandwidth-intensive applications. The following steps show an example of denying high-bandwidth applications for all remote users.
- a) Select **Configurations > Policies/Settings** and open the **Access Policies** tab.
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Tip In Multiple Device mode mode, this tab includes access policies for both the CX device and the parent ASA. Ensure that you are working in the CX access policy section.

- b) Use one of the **Add Policy** buttons to add a new policy.
If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.
- c) In the Create Policy form:
- Enter a name for the policy, for example, Control Secure Mobility Bandwidth.
 - Select **Policy Action: Deny**.
 - In the **Source** field, select the **All Remote Devices** Secure Mobility object.
 - In the **Destination** field, keep the default, Any.
 - In the **Application/Service** field, select the applications, application types, application tags, or objects that identify the services you want to deny. For example, YouTube, Facebook Photos, iTunes iPad, or perhaps the File Sharing application type, which covers many different applications with one selection.
- Note** Watch out for unintended consequences. For example, YouTube hosts a wide range of videos, including those used for educational purposes. Excluding an entire application could prevent network usage that might be required by your organization for remote access users, even though other uses of the application might not be appropriate for your network.
- d) Click **Save Policy**.
If you did not insert the policy in the desired location, move it.
- e) Commit and deploy your changes.
-



CHAPTER

5

Managing System Licenses

Both the CX device and the PRSM Multiple Device mode server require licenses. The following topics explain license management.

- [CX Feature and PRSM Licenses, page 71](#)
- [How Feature Licenses Affect Policy Configuration, page 72](#)
- [Overview of the Licenses Page, page 73](#)
- [Configuring System Licenses, page 74](#)

CX Feature and PRSM Licenses

CX features and PRSM Multiple Device mode use separate licenses, but you can use the PRSM server to manage the feature licenses used on CX systems. The following topics explain the different types of licenses.

Feature Licenses

Many features of the CX device are available without special licensing. However, you must install the following licenses to obtain the services covered by the license:

- **Application Visibility and Control license**—This subscription-based license allows the use of application-based access control. Specifically, you need this license if you want to create access policies based on applications or their attributes, including application or application services policy objects.
- **Web Security Essentials license**—This subscription-based license allows the use of URL filtering and the use of web-reputation-based policies. Specifically, you need this license if you want to use URL objects or web reputation profiles in policies.
- **Next Generation IPS license**—This subscription-based license allows the use of Next Generation IPS filtering. Specifically, you need this license if you want to create access policies that apply NG IPS profiles, which can identify threats and apply drop or monitor decisions based on IPS (intrusion prevention system) threats.
- **3DES/AES (K9) license**—The 3DES/AES (K9) license determines the relative strength of the encryption algorithms used in the product. The license is tied directly to the hardware (by serial number) and is a permanent license that does not require renewal. The license is free, but its availability is limited by

export restriction laws, so it is not available for all users. Consult Cisco.com to determine if you can download the 3DES/AES (K9) license.

Licenses are valid for specific device models only. You must purchase the correct license for the device model you are using.

Each CX device includes evaluation subscription licenses for each feature that you can configure on the device. These licenses are good for 60 days. You can renew the evaluation licenses one time to extend the period an additional 60 days. The PRSM server also includes these evaluation licenses for up to two devices.

Cisco Prime Security Manager Licenses

Cisco Prime Security Manager Multiple Device mode requires a license. The license determines the number of devices that you can manage using the PRSM server.

PRSM includes a 90-day unlimited device count license, which you can renew once by obtaining and uploading a new evaluation license. The remaining period available in the evaluation license is shown in the menu bar next to the Pending Changes link.

If the evaluation license expires, you can no longer deploy changes to devices.

Ensure that you purchase and upload a license with a sufficient device count.

How Feature Licenses Affect Policy Configuration

When you create a policy, you can use options that are controlled by feature licenses. A device must have a valid appropriate feature license to implement these policies.

However, features are divided into the following categories, and the impact of licensing problems differ based on them:

- **Hard Enforcement**—Any licensed feature that is used in traffic matching criteria is hard enforced. This means that you cannot use the features, or edit policies that use the feature, if you do not have a license (either you never applied a license, or the license expired). Hard enforced features include application filtering (which requires the AVC license) and URL filtering (that is, the use of URL objects in the destination criteria of a policy, which requires the WSE license).



Note

Policies that use hard-enforced features with an expired license continue to work if they are already configured on the device. However, the device does not receive updates related to the feature. For example, if the Web Security Essentials license expires on a device, that device stops downloading URL category updates. The longer the device operates without a license, the greater the difference between the signatures used by the policy and the current state of the signatures.

- **Soft Enforcement**—Any license feature that you configure using profile objects is soft enforced. This means that you can create and apply profiles at any time to any policy, but that the profiles are implemented only if a valid license is assigned to the device.

The reason for the difference between hard and soft enforcement is because the hard enforced features actually define the traffic to which a policy applies. If the system simply ignored those criteria when the associated

license was not available, your policies would have a different meaning, and you could see unwanted changes to how traffic is allowed or denied. Soft enforced features, on the other hand, do not change which traffic matches a policy, but whether that traffic is scanned for potentially harmful traffic, so these can be safely ignored if you do not have the required license.

The Details about License Enforcement

Because feature licenses have expiration dates, you must also ensure that the licenses have not expired. As licenses near their expiration dates, you will be warned about the pending expiration, and there is a 60 day grace period after expiration to give you some time to upload new licenses. A link appears in the menu bar, next to the Pending Changes link, that shows the number of expired licenses. Evaluation licenses do not have a grace period.

License problems are indicated by caution icons or messages. Mousing over the icon will show messages that explain the exact problem. The message can include links to the Licensing page or to filter the policy list to show affected policies.

License enforcement includes the following:

- When importing a device into the PRSM inventory, you must have sufficient licenses for hard-enforced features or the import fails. The licenses can be non-evaluation licenses on the device (which are imported), or available licenses in PRSM.
- When sharing policies, you cannot select devices that do not have the required licenses for policies that use hard-enforced features. You can, however, share soft-enforced features.
- If a policy is assigned to one or more devices that do not have a particular feature license, you cannot edit that policy to select an option that requires an unlicensed hard-enforced feature. Either exclude the unlicensed devices for that policy, create a separate policy to implement the feature, or simply apply the license to the unlicensed devices.
- If an assigned license is within 30 days of expiring, the policies lists will be littered with warning icons on the device and on any policy that will be affected by the expiration.
- If an assigned license has expired, but is within the 60 day grace period, you will see the same warning icons as you would for an expiring license. However, policy creation and edit will act as if the device is unlicensed. You will not be able to add hard-enforced options that require the license to policies shared with this device.
- If an assigned license has expired and is outside of its grace period, you will see all the same warning icons, but you will not be able to edit any policies that use unlicensed hard-enforced features that are shared with the device. You can delete these policies. Also note that dashboard data will not be generated for these policies.

Overview of the Licenses Page

Licenses determine the features you can use, or in the case of PRSM Multiple Device mode, how many devices you can manage. The Licenses page shows the licenses that are currently installed in the system. Each license shows the maximum number of devices it covers, the number of devices that are using the license, the available number of licenses remaining for device assignment, and the license expiration date, if any. From this page, you can upload licenses and perform other license management activities.

To open the Licenses page, select **Administration > Licenses**. You can also open the page by clicking a license notification link in the menu bar, which will appear next to the Pending Changes link if you are using an evaluation license or if a license has expired.

The Licenses page includes the following items:

I Want To

Contains the following commands:

- **Upload License File**—To add a license file. In Single Device mode, uploading a license automatically applies the license to the device if the new license has an expiration date more remote than the currently-used license.
- **Renew Evaluation Licenses**—To renew all evaluation licenses. You can renew evaluation licenses once before purchasing new licenses. This command is not available if you have already renewed licenses, or in Single Device mode if you have uploaded feature licenses.

List of Licenses

Shows each license available on the system. Each license also contains a list of devices that are using the license. Devices configured for high availability (HA) are shown once, using the logical name for the pair. HA devices use one license per pair.

Select or mouse over a license or device to see the commands related to it. The following are the available commands:

- **Apply License**—(License command.) To assign the license to a device that does not currently have a license of this type. You will not see this command if there are no available licenses to apply.
- **Renew License**—(License command.) To assign a new, different license to the devices that are using this license. For expiring licenses, ensure that you assign a new license using this command before the grace period expires. This command does not appear if there are no devices using the license.
- **Delete License**—(License command.) To delete a license that you no longer need. You can delete a license only if it is unused.
- **Revoke License**—(Device command.) To remove the license from this device. You can revoke a license only if no policies assigned to the device use hard-enforced services covered by the license. The purpose of revoking a license is to free it for use on another device.

Configuring System Licenses

The following topics explain the basic procedures for configuring system licenses.

Using Evaluation Licenses

Each CX device and PRSM server includes evaluation copies of the subscription feature licenses. In Multiple Device mode, the evaluation licenses are good for two devices; in Single Device mode, the evaluation licenses

are good for that device only. The PRSM server includes an additional evaluation license for the server to allow you to manage an unlimited number of devices.

- The feature evaluation licenses are good for 60 days. You can renew the evaluation licenses once for an additional 60 days, for a total of 120 days of evaluation. There is no grace period upon evaluation license expiration. The following procedure explains how to renew these licenses.
- The PRSM server license is good for 90 days. To renew the license, you obtain a new evaluation license from Cisco.com and upload the file.

Procedure

-
- Step 1** Select **Administration > Licenses**.
- Step 2** Select **I want to > Renew Evaluation Licenses**.
You are prompted with an explanation of the renewal and asked to confirm that you want to renew both evaluation licenses. If you have already used up your renewals, you are told so.
- Step 3** Click **Yes** to renew the licenses.
-

Uploading License Files

When you obtain a license, you get a license file with the file extension .lic. You need to upload the file to the system. The method for uploading the license is the same for Single Device mode or Multiple Device mode, but you must ensure that you are uploading the right type of license based on the mode you are in.

Besides the method described below, you can also upload licenses while renewing an old license.

Procedure

-
- Step 1** Select **Administration > Licenses**.
- Step 2** Select **I want to > Upload License File**.
- Step 3** Add license files to the **Upload License Files** box.
You can drag files from your system into the box (if supported) or click the box to open a file selector.
- The license is added to the list of licenses and further action is based on the mode you are in:
- Single Device mode—The license is applied and activated when you commit changes. If you have more than one of a particular type of license, the license with the longest remaining life is used and the others are not used. The licenses must be for the correct device type. Any evaluation license is removed.
 - Multiple Device mode, CX license—The license is available for use. You must apply it to a device.
However, 3DES/AES (K9) licenses are applied automatically to the appropriate device. 3DES/AES (K9) licenses are tied to a specific device based on serial number; if a device with the correct serial number is in the inventory, the license is automatically applied. The correct device must be in the inventory or upload is blocked.

- Multiple Device mode, PRSM license—The license replaces the evaluation license, if you still have one. If you upload multiple licenses, the license count is accumulative (for example, a 5-device plus a 10-device license gives you 15 devices).

Step 4 Click **Close** to return to the license list.

Assigning Feature Licenses

Each device that uses subscription-based features must have a license for the feature.

When you upload a license file to a CX device, it is automatically applied to the device. However, in PRSM Multiple Device mode mode, you need to explicitly assign licenses to devices. In Single Device mode, you can also assign a license if you happen to revoke it. In both modes, you must commit changes before the license takes effect.

When a feature license expires, you must replace it (which is called “renewing” the license), or you will not be able to use the feature controlled by the license. There is a grace period to give you time to replace the license.

Applying Licenses

The following procedure explains how to apply a feature license with an available license count to devices that currently have no license or whose license has expired.

Procedure

- Step 1** Select **Administration > Licenses**.
- Step 2** Select the license you are applying and click **Apply License**.
This opens the Apply License window, which shows the license type, device model, and the number of licenses still available for assignment.
- Step 3** Select the devices that should have this license.
The device selector will show only devices of the appropriate model that do not already have a valid license. You cannot select more devices than the available license count.

Devices configured for high availability are show once, using the logical name of the pair. These pairs use a single license, rather than two.
- Step 4** Click **Apply**.
-

Renewing Licenses

The following procedure explains how to renew a license by replacing it with another unused feature license. You would typically do this on licenses that are expiring or on evaluation licenses when you obtain a purchased license.

Procedure

Step 1 Select **Administration > Licenses**.

Step 2 Select the license you are replacing and click **Renew License**.

This opens the Renew License window, which shows the license type and device model. The **Selected Devices** box includes all devices that are currently using this license. You can delete devices from this list if you do not want to replace the license on certain devices.

The **Select Available License Files** list shows all unused licenses that are available to replace this license; if there are no available licenses based on feature and model, the list does not appear. The licenses are sorted with the nearest expiration dates at the top.

If there are no licenses, or no licenses that you want to use, you can upload licenses files in this window. You can drag files from your system into the box (if supported) or click the box to open a file selector.

Step 3 Click each license you want to apply until you have selected a sufficient number of licenses.

If there are available licenses, they are pre-selected to match the required count, which is all devices that you have selected. You can change the selection. Clicking a selected license deselects it.

High availability pairs use one license for the pair, not two.

You cannot continue until you have selected the required number of licenses.

Step 4 Click **Renew**.

Obtaining and Installing the 3DES/AES (K9) License for Strong Encryption

A 3DES/AES license, otherwise known as a K9 license, is required for strong encryption. If you do not have a K9 license, decryption processing with a server that requires strong encryption will fail. Any flow that requires decryption that the device cannot perform will be denied regardless of access policies. Although the K9 license is free, its availability is limited by export restrictions.

If you cannot use a K9 license, you should test decryption processing in a controlled environment to ensure that it satisfies your requirements before enabling decryption in your production network. Without a K9 license, your decryption policies will require careful testing and fine-tuning to ensure that desirable traffic is not blocked.

Procedure

Step 1 Obtain the serial number (SN) of your ASA CX device. You can obtain this number using the following techniques:

- If you are managing the device in PRSM, the device inventory page shows the serial number.
- If ASA CX is already operational, you can log into the CLI and use the show platform hardware info command; the PCB SN is the number you need.
- If the ASA CX hardware module is installed in an ASA 5585-X appliance, you can get the number through the ASA CLI using the show module 1 details command.

- If the ASA CX software module is installed in an ASA 5500-X series appliance, the ASA CX and the ASA share the same serial number. Use the show version command from the ASA CLI to get the number. If ASA CX is operational, you can also use the show module cxsc details command from the ASA CLI.

- Step 2** Go to <http://www.cisco.com/go/license> and obtain a new K9 Crypto license. Select **Get New > IPS, Crypto, or Other License** and select **Cisco ASA CX 3DES/AES License** under Security Products. Follow the wizard instructions to obtain the license. (Note that this procedure might have changed since the publication of this document.)
- Step 3** In the ASA CX/PRSM web interface, select **Administration > Licenses**, then **I want to > Upload license file**, to upload the K9 license. The license is tied to the SN, so as long as the SN for the license matches the device, it is applied immediately. In Multiple Device mode, the device must already be in the inventory.
-

Revoking Licenses

You can revoke a license from a device if you no longer want to use the features covered by the license. Revoking the license frees it for use by other devices.

You cannot revoke a license if the device is using hard-enforced features that require it. For example, if the device uses a policy set that includes application-based rules, you cannot revoke the Application Visibility and Control license. However, you can revoke a license if the only features that require it are soft enforced.

You cannot revoke a 3DES/AES (K9) license.

Procedure

- Step 1** Select **Administration > Licenses**.
- Step 2** Select the device within the license you want to revoke and click **Revoke License**. You are asked to confirm the revocation.
-

Deleting Licenses

If a license is not assigned to any device, you can delete it. You should delete expired licenses once you have removed all device assignments to them.

Procedure

- Step 1** Select **Administration > Licenses**.
- Step 2** Select the license you want to delete and click **Delete License**.
-



PART **I**

The Basics

- [Managing Devices, page 81](#)
- [Managing Policies, page 103](#)
- [Managing Policy Objects, page 115](#)



CHAPTER 6

Managing Devices



Tip

Device inventory management applies to PRSM in Multiple Device mode only. If you are configuring a CX device through a direct connection to the device, you do not need to add the device to the inventory to configure it. You will not see the device inventory page in Single Device mode.

You must identify the devices you want to manage by adding them to the inventory. Once in the device inventory, you can monitor device activity and make necessary changes to the configuration, and then deploy configuration changes back to the device.

The following sections explain the basics of managing the device inventory.

- [Managing CX Devices in Multiple Device Mode, page 81](#)
- [Preparing ASA Devices for Management, page 83](#)
- [Understanding Device Discovery, page 84](#)
- [Actions that Require You to Delete and Re-import a Device, page 87](#)
- [The Device Inventory, page 89](#)
- [Troubleshooting Device Communications, page 99](#)

Managing CX Devices in Multiple Device Mode

If you manage a CX device in PRSM Multiple Device mode, the device is placed in **managed mode**.

When a CX device is in managed mode, you cannot configure it directly through its web interface in Single Device mode. All configuration and monitoring must be done through PRSM Multiple Device mode. The only exception is that the local CLI is still available, where you can troubleshoot and fix basic configuration settings such as IP addressing, DNS, NTP, and passwords.

Putting a CX Device into Managed Mode

To put a CX device into managed mode, you add it to the device inventory. If you add an ASA that contains a CX to the inventory, you will also be adding the CX device. The device is placed in managed mode when you commit changes.

**Tip**

If the CX believes that it is already being managed by a different PRSM server, discovery will fail, because you cannot manage a single CX device from multiple PRSM servers. If this happens, log into the CX web interface in Single Device mode and click the link to unmanage the device. Then try again to add the device to the inventory (delete it first if necessary).

Implications of Managed Mode

Placing a CX device into managed mode has the following implications:

- Policies, policy objects, licenses, and some other parts of the configuration are discovered and added to the PRSM database. Going forward, you must use PRSM Multiple Device mode to change the policies, objects, and other settings that are defined through the web interface. However, not all device settings are discovered, and undiscovered settings are replaced with the settings currently defined in the database.
- The CX device maintains awareness of which PRSM server is managing it. You cannot push configuration changes from another PRSM server. If you ever need to move the management of a CX device from one PRSM server to another, delete the device and add it to the new server. Deleting the device puts it into unmanaged mode and the licenses currently installed on the device are retained.
- Events are automatically forwarded to the PRSM server. There are no settings to configure to get events forwarded to the correct server, it happens automatically.
- PRSM automatically collects dashboard data from all managed CX devices.
- If you open the web interface for the CX device in Single Device mode, most of the interface is disabled, but the home page informs you that the device is in managed mode, and includes a link to the PRSM server that is managing the device. Thus, if you ever lose track of which server is managing a particular CX device, you can always find out through the web interface.
- The CLI available through the CX management interface remains active and fully functional. Use it to troubleshooting and to maintain the basic device management settings. Making changes through the CLI does not affect the managed mode of the device.

Going Back to Unmanaged Mode

If you need to return a CX device to unmanaged mode, you have two choices:

- Preferred method—Delete the device from the device inventory. This action returns the device to unmanaged mode.
- Emergency method—If PRSM is not available for any reason, you can open the web interface for the CX device in Single Device mode and click the link to unmanage the device. This action breaks the connection with the PRSM server and enables the local web interface.

**Caution**

If you unmanage the device from the Single Device mode interface, if the device remains in the device inventory, you will get errors if you try to deploy to it. After unmanaging the device in this manner, if you want to continue managing the device from PRSM, you must delete it from the inventory, then add it back to the inventory. You will have to go through this process even if you mistakenly unmanage the device without making any changes to the local configuration.

**Note**

Switching to Single Device mode restarts services on the device. If the device is part of an ASA high-availability pair, this will cause the ASA to fail over.

What You Can Do From the Managed Mode Home Page

When you log into a CX device that is running in managed mode, you can do the following from the home page:

- **Redirect to Cisco Prime Security Manager Multiple Device mode**—The device knows which PRSM server is managing it, and you can click the link to get to the server. The address is shown.
- **Download logs**—Click the link to download system logs to help troubleshoot problems. You can also download the logs for each managed device through the PRSM server from the Device Configuration page for each managed device. Access the Device Configuration page from the device inventory.
- **Switch to single device mode**—Break the management connection with the PRSM server. See above for more information.
- **Re-synchronize the full configuration from Cisco Prime Security Manager**—If you recovered the database on the PRSM server, you need to bring the managed devices in line with the configuration stored on the PRSM server. You can click this link to reinitialize the device database and return it to the configuration defined on the PRSM server. Services are restarted after re-synchronizing the configuration. The address of the server is shown.

Preparing ASA Devices for Management

Before you can manage an ASA device, you must ensure that PRSM can communicate with the device to discover its configuration and to subsequently make modifications to that configuration based on your changes. Follow the procedures in the hardware installation guide for your ASA model to perform a basic configuration using ASDM or the device CLI.

PRSM uses SSL (HTTPS) to manage the ASA. Thus, you must ensure the following are configured:

The HTTP server must be enabled.

The configuration command is **http server enable**. The HTTP server is already enabled in the default ASA configuration.

The IP address of the PRSM server must be allowed to connect to the HTTP server.

You can identify the specific IP address of the server, or you can identify the subnet on which the server resides.

The command for enabling access to the HTTP server on the ASA is **http *IP_address subnet_mask interface_name***, where the parameters indicate the IP address or network address allowed to access the server, its subnet mask, and the ASA interface through which access is allowed. You can allow connections from all hosts through the management interface and depend on username and password to protect access to the HTTP server by specifying **http 0.0.0.0 0.0.0.0 management**.

The **http** command is included in the default configuration with the following settings. Adjust them as required.

http 192.168.1.0 255.255.255.0 management

The Management 0/0 interface is configured with the IP address 192.168.1.1. In the default configuration, the 192.168.1.0/24 network is the management network.

Tips

- In addition, you must ensure that the ASA is configured in single-context routed or transparent mode if you want to manage it. Ensure that the **mode single** command, which configures single-context mode, does not appear in the configuration; you can use the **show mode** command to verify the firewall mode. The default ASA configuration is single-context routed mode. If the ASA is in multiple-context mode, you can still manage a CX module contained in it.
- You cannot use the **password encryption aes** command in the ASA configuration.
- You cannot use an IPv6 address on the ASA management interface.
- Typically, you will also create an enable password for Privileged EXEC mode. You might also create a user account for logging into the device. If you create a user account to control log in, assign it privilege level 15.

Understanding Device Discovery

When you add a device to the PRSM Multiple Device mode inventory, the policies and settings currently configured on the device are added to the PRSM database and the device is considered to be managed by the PRSM server. To make changes to the device configuration, you would make the changes within PRSM and deploy the changes to the device.

During discovery, if there are naming conflicts between a discovered object and one that already exists in the PRSM database, you are prompted to resolve the conflict either by supplying a suffix for the discovered objects or by creating an override to customize the existing object's contents for the device you are adding. Thus, all unique objects are discovered, but a name change can occur. If the discovered object is the same as the same-named object in the database, the database object is simply reused. System-defined objects are never discovered, because they will always be identical.

It is important to understand the limitations of device discovery, which differ based on device type, as explained in the following sections.

CX Device Discovery

Policies, objects, directory realms, and settings are discovered with the following limitations:

Licenses

Valid licenses are imported. Invalid licenses, or licenses that are identical to ones already in the PRSM database, are replaced with the copies in the PRSM database. Evaluation licenses are not imported.

You must have sufficient licenses already in the PRSM server for any devices that you add. For example, if the device includes policies that use application, URL filtering, or web reputation, sufficient available licenses for those features must exist. If they do not exist, you cannot add the device until you add the licenses to the PRSM server.

Users

Users are not imported. The existing users are not removed, nor are users imported from the server. However, all existing users other than the **admin** user can no longer log into the managed device. The password for the **admin** user is not changed.

Backup Schedule

The backup schedule is removed when you add the device to the inventory, because the PRSM server will maintain the true source of the device's configuration. If you want to back up the device configuration anyway, you can use the CLI.

End User Notification Customizations

If all notification types in PRSM are the defaults, and the device has one or more custom page, the custom pages are imported and used for all managed devices. However, if any notification type in PRSM has a customized page, no pages are imported.

Undiscovered Settings

The following settings are never imported. After discovery, when you commit changes, the settings will be replaced with those defined on the PRSM server. Before adding the device, ensure that you are comfortable with how these settings will change.

- Signature update settings (frequency and proxy settings).
- Network participation.

ASA Device Discovery

When you add an ASA, you can elect whether to add it in managed mode or monitor-only mode. In monitor-only mode, the configuration is not discovered, because you will not manage it in PRSM. For fully-managed mode, configuration discovery is limited to those policies and settings that PRSM supports.

If you need to make changes to other device policies or settings, use the ASA CLI or another management application such as ASDM. However, do not use a management application that will also consider itself the owner of the policies or settings currently managed by PRSM. For example, do not attempt to manage ASA access lists with both PRSM and Cisco Security Manager.

When you add the device to the inventory, if there are aspects of the configuration that are problematic for PRSM, messages will explain the issues. In some cases, discovery will fail, in other cases, an otherwise supported policy will not be imported. There are also cases where an unsupported command for an otherwise supported feature will simply be ignored and left unchanged (and unmanaged).

Following are some tips and details about what is supported during discovery by general feature area.

Interface Configuration

An IPv6 address for the management interface is not supported. You cannot add an ASA to the inventory using an IPv6 address.

An IPv6 address for a bridge group interface is not supported. If you configure an IPv6 address, it will be ignored and left unmanaged.

The management interface must be configured with the **mgmt-only** attribute. Discovery will fail if this is not configured. If you get a discovery error related to this setting, and the ASA CLI does not allow you to apply it, you will need to back up your configuration and reset the ASA to get around the problem.

Policy Objects

If the configuration includes any of the following object commands, discovery fails. You must convert these objects to ordinary service or service group objects before importing this device, that is, the **object service** or **object-group service** (without qualifier) commands. Unsupported commands include: port-object, object-group service tcp, object-group service udp, object-group service tcp-udp, object-group icmp-type, object-group protocol.



Tip

Cisco provides an off-line tool that will convert the unsupported service object commands, and the ACLs that use them, to the required style. You can use the tool to convert an ASA configuration, then verify it yourself before you manually apply the changes to the ASA. You can then add the device to the PRSM inventory. The tool is called CSM to PRSM Migration Tool and is available as a download from the Cisco Prime Security Manager software download page. The readme file in the download includes instructions on using the tool.

The following objects will be imported: network, network object group, service, service object group, time range, and ASA identity user group object.



Note

Policy object names are case-sensitive in PRSM. Upon import “Object1” and “object1” will not be considered to have the same name.

Access Control Lists (ACLs) and access groups

Discovered interface and global extended ACLs are added to the access policies as policy sets. The name of the policy set is the ACL name; global ACLs are added to the Universal Bottom policy set.

Discovery creates a separate policy set for each interface that is assigned an ACL. For example, if you have ten interfaces, you should see ten ACLs. However, after import, you can create new policies for different interfaces in any policy set. During deployment, ACLs are generated for each interface based on all the rules, across policy sets, that apply to the interface.

Standard, EtherType, and Web ACLs are not supported. Unreferenced ACLs are not discovered, nor are they deleted.

Carefully consider the following restrictions:

- TrustSec security groups on extended ACLs are not supported. ACEs with TrustSec specifications will be removed from the access list on deployment.
- For access groups, the per-user-override and control-plane keywords are not supported. They will be removed on deployment.

Syslog Server and Logging Configuration

The **logging trap** command is not directly supported. Instead, the syslog level is supported. Upon first deployment, the **logging trap** setting will be overwritten.

Traffic Redirection to CX

Although you can configure the policy that redirects traffic to CX, PRSM does not support all possible configurations. If you import a device with an unsupported redirection policy, that policy is not imported, and you must use other means to maintain the policy.



Note

PRSM will not be able to recognize out-of-band changes to the traffic redirection policy.

High Availability Configuration

Active-Standby configurations are discovered. Active-Active is not supported.

Network Address Translation (NAT)

Both object-based and rule-based (twice) NAT are discovered. NAT44, NAT46, NAT64, and NAT66 rules are supported.

Actions that Require You to Delete and Re-import a Device

Some changes you make to a device cannot be supported through PRSM management. If you make these changes, and you want to continue managing the device in PRSM, you must delete the device from the inventory and re-import it, assuming the change does not make the device completely unsupported.

Unmanaging a CX device

If you log into a CX device and unmanage it from its home page, the relationship between the device and PRSM server is broken. You must delete and re-import the device to re-establish the relationship.

Upgrading or Downgrading an ASA to an unsupported release

You cannot upgrade ASA Software using PRSM. Thus, any upgrades you apply will be noticed by PRSM the next time you deploy configuration changes. At that time, the deployment results will indicate that the upgrade happened, you will see an information icon in the inventory that indicates the upgrade occurred, and the Software Version column will show the currently-running version. However, PRSM will build configurations based on the original software version that was running when you added the device to the inventory.

In contrast, if you upgrade (or downgrade) to a version PRSM does not support, the deployment job will fail, and the reason will indicate that the software version is not supported. To fix the problem, you must reinstall a supported version and retry the deployment. If you do not want to undo the upgrade, you need to delete the device from the inventory; you cannot manage it in PRSM.

Following is a summary of supported or unsupported software version changes:

- **Supported Changes**—Typically, you can upgrade between minor and point releases, for example, from 9.0.1 to 9.1.1, or from 9.1.1 to 9.1.2.
- **Unsupported Changes**—Upgrading or downgrading the major release number is not supported. For example, going from 9.x to 8.x. If PRSM supports the major release number, deleting and re-importing the ASA is required to handle the major version change.

Changing a management IP address

If you change the management IP address of a managed device, you break the connection between PRSM and the device. Before changing the address, delete the device from PRSM. Otherwise, for CX devices, you will have to both delete the device and go to the device's home page to switch to Single Device mode.

If you change the management address of the PRSM server, you must delete all managed devices. Delete devices before changing the address.

Security context and operational mode changes

If you change the security context and operational mode settings on an ASA device, you must delete and re-import the device if you want to continue managing it. Deployments after the following changes will fail.

- Single context to multiple context (or vice-versa).
- Routed mode to transparent mode (or vice-versa).

Replacing device hardware

If you replace a device, for example, replacing an ASA 5520 with a 5525, while configuring the new device with the same management IP address as the former device, you must delete the old device from the inventory and add the new one. PRSM cannot simply change the device model of the existing inventory record, because changes in hardware can change the available features and configuration limits associated with the managed device. Even if you are replacing a device with one of the same model, the serial number will change, and delete followed by re-import is the best option.

The Device Inventory

To view the device inventory, select **Configurations > Policies/Settings**, switch to Repository view, and open the **Overview** tab.

For each device, the inventory list summarizes device information such as the device name (the name by which the device is referred to in PRSM, not necessarily the host name), the features available (based on licenses), the operational mode (routed or transparent), the device type, last deployment information, the management IP address and port, the software version, and the device serial number.

Devices are listed as follows:

- Standalone devices are listed one per line.
- ASAs with CX devices are listed on a single row, with both the ASA and CX information displayed.
- ASAs configured as high-availability pairs have the second device in the pair shown beneath the primary device. Click the **Show Standby Device** link to view it.



Tip

If there is a warning icon in the list, mouse over the icon to see information about the current status of the device. The status might indicate a temporary situation, such as discovery in progress (when you first add a device), or an error condition that needs your attention.

The following topics explain how to work with the device inventory.

Adding Devices

To add a device to the inventory, select **Configurations > Policies/Settings**, then click the **Add Device** link in either Device or Repository view. The Add Device wizard walks you through the process.

The process for adding the device differs based on the following characteristics:

- **ASA plus CX**—Where you add an ASA device that includes a CX device. You can decide whether you want to manage the parent ASA in PRSM or to add it in monitor-only mode. In monitor-only mode, you can view events and dashboard statistics for the ASA, but you cannot change the device configuration.
- **Standalone ASA**—Where you add an ASA that does not contain a CX device.
- **ASA configured for high-availability**—Where you add an ASA that is configured in a high-availability pair with another ASA. The ASAs can contain CX devices, or they can be standalone.

The following topics provide details about these methods and restrictions.

Restrictions on Adding Devices

Devices must meet certain restrictions before you can add them to the inventory. In general, you must be running the minimum or higher software version as defined in *Cisco CX and Cisco Prime Security Manager Compatibility*, http://www.cisco.com/c/en/us/td/docs/security/asacx/compatibility/cx_prsm_comp.html. The device model must also be supported.

The following table and notes provide more detail about supported combinations.

Table 2: ASA and CX Supported Combinations

	No CX	CX	CX Unsupported Version	CX Monitor-only Mode	CX, PRSM Realm Conflict	CX Insufficient Licenses
ASA single-context mode, routed or transparent	Yes	Yes	ASA—Yes CX—No	ASA—Yes CX—No	ASA—Yes CX—No	ASA—Yes CX—No
ASA multiple-context mode	No	ASA— monitor only mode CX—Yes	No	No	No	No
ASA in high availability configuration	Yes	Both	ASA—Yes CX—No	ASA—Yes CX—No	ASA—Yes CX—No	ASA—Yes CX—No

Table Legend

- Yes—Fully supported, managed mode.
- No—Not supported, you cannot add this device.
- Both—Both the ASA and CX device are fully supported in managed mode.
- Monitor-only—You can add the ASA in monitor-only mode, where you will see events and dashboard data for the device, but you cannot change the device's configuration.
- N/A—This combination is not meaningful.

Notes

- If you are using third-party certificates, you must add the entire certificate chain (root and intermediates) into whichever device uses the third-party certificate (PRSM, CX, and ASA). Adding just an intermediate certificate will result in certificate verification failures during import. If the device certificate is not issued by a party PRSM recognizes, you will also have to add the chain to the supplemental certificate store in PRSM.
- If there is a Network Address Translation (NAT) boundary between the PRSM server and the device, and you apply NAT to the management IP addresses, you must keep 443 as the HTTPS port, you cannot translate the port to a different value. The NAT rule must translate both source and destination addresses for both inbound and outbound traffic.
- You cannot add a CX device that is configured in monitor-only mode.
- You cannot add a CX device that uses policies requiring a feature license if you do not have sufficient feature licenses available in PRSM. Although the CX might be operating normally with evaluation licenses, PRSM does not import evaluation licenses, so those are not considered to be valid licenses. Ensure that either the CX device, or PRSM, has sufficient feature licenses for the devices you add to the inventory.

- If an AD realm is defined on both the CX device and PRSM server, they must be identical, or you will be prevented from adding the CX device to the inventory.
- Active-Standby is the only supported high availability configuration.

Handling Object Naming Conflicts

When you add a device to the inventory, its configuration is discovered and objects, policies, and other configuration settings are added to the PRSM database. In this topic, we will call these discovered items “objects.” Because there are already objects in the database, it is possible that discovered objects have the same name as objects already defined in the database.

If an object in the discovered configuration has the same name as an object already in the database, but the content of the objects is identical, the object in the database is used and replaces the discovered object. For example, if two network objects have the same name and define the same addresses, they are not considered to be naming conflicts.

Naming conflicts occur when the content of the same named objects differ; for example, two network objects with the same name that include different addresses. All conflicts of this type are identified during discovery and listed in a table of naming conflicts.

To resolve the conflicts and complete the device import, you must elect how to handle them. You have the following options:

- Define a suffix to add to all conflicting names. The default is to use the device name of the discovered devices, but you can use any suffix that results in a unique name.
- Create a device-level override for the device you are adding. If an object allows device-level overrides, you can keep the same object name, but create an override that defines a different, custom value, for the device you are adding.

Adding an ASA and its CX

When you add an ASA that contains a CX device, you also have the option to add the ASA in monitor-only mode. In this mode, you use other methods to manage the ASA CLI. Monitor-only mode is useful if you manage the ASA with another application, such as ASDM or Cisco Security Manager. If you define the PRSM server as a syslog server, you can view events and dashboard data for monitor-only ASAs.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings**, then click the **Add Device** link in either Device or Repository view.
- Step 2** Fill in the following information to define the communication properties for the ASA device.
- **Device Name**—The name by which the device will appear in selectors in PRSM, typically the same as the device host name.
 - **Hostname/IP: Port**—The IP address or DNS hostname of the management interface or another interface that allows access to the internal HTTP server, and the port number used for HTTPS access. The default port is 443.
 - **Username, Password**—The user name for logging into the device and the user’s password.

For ASA devices, the user should have privilege level 15. If the device requires an enable password only to configure it, you can leave the Username and Password fields blank.

When you enter the hostname/IP address and port, PRSM tries to retrieve the certificate from the device. This step must be successful before you continue. You should see a green checkmark, and the Certificate field should contain a **View** link. Click the link to inspect the certificate.

Step 3 Click **Next**.

PRSM evaluates the ASA configuration and determines if it contains a CX device. If it does, but the ASA does not meet other requirements, you can add the ASA in monitor-only mode, where you can view events and dashboard information for the device but you cannot change its configuration. If PRSM supports this ASA for configuration, you have the option of managing it in PRSM or adding it in monitor-only mode.

Step 4 Select the mode you want to use for the ASA and click **Next**.

Step 5 Fill in the communication properties for the CX device.

Typically, you will simply need to enter the password for the **admin** user, the other information should be discovered correctly.

If you need to make changes, keep the following in mind:

- The **admin** username and password are required. The **admin** username is the only one allowed for device discovery.
- Keep the port number 443 unless an intervening NAT device is translating the traffic to a different port.
- The IP address is discovered through the parent ASA. If you configured both IPv4 and IPv6 management addresses, the IPv4 address is the one used. If you prefer, you can replace this with the global IPv6 address. You must enter correct address and port information, and get a green checkmark for certificate retrieval, before you can proceed.
- If there is a NAT boundary between the PRSM server and the device, be aware that the discovered address is the real IP address of the device. You must change it to the NAT address for discovery to succeed.

Step 6 Click **Next**.

PRSM imports the configuration and determines if there are any naming conflicts between discovered items and those that already exist in the database.

Be patient. Device discovery can take time, and the time required to complete the discovery increases with the size of the device's configuration.

Tip If there are object naming conflicts, you are asked how you want to handle them. You can add a suffix to imported objects, or in some cases, elect to keep the object name but create an override for the device you are adding. Make your selections and continue.

Step 7 On the summary page, evaluate the results and add descriptive information if desired.

The summary page shows the device models and the number of policies, realms, licenses, objects, object overrides, and renamed objects for the devices you are adding. You can also enter information about the device location, organization, and department. This descriptive information is for your management purposes only and does not affect the device configuration.

Step 8 Click **Commit Now** to complete the process.

You must commit changes to put the devices into managed mode. You can click **Commit Later** if you intend to add more devices or make some immediate configuration changes, but you should not leave a newly-added device in uncommitted state for a long time.

Adding a Standalone ASA

You can add a supported ASA even if it does not contain a CX device.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings**, then click the **Add Device** link in either Device or Repository view.
- Step 2** Fill in the following information to define the communication properties for the ASA device.
- **Device Name**—The name by which the device will appear in selectors in PRSM, typically the same as the device host name.
 - **Hostname/IP: Port**—The IP address or DNS hostname of the management interface or another interface that allows access to the internal HTTP server, and the port number used for HTTPS access. The default port is 443.
 - **Username, Password**—The user name for logging into the device and the user's password. For ASA devices, the user should have privilege level 15. If the device requires an enable password only to configure it, you can leave the Username and Password fields blank.
- When you enter the hostname/IP address and port, PRSM tries to retrieve the certificate from the device. This step must be successful before you continue. You should see a green checkmark, and the Certificate field should contain a **View** link. Click the link to inspect the certificate.
- Step 3** Click **Next**.
PRSM evaluates the ASA configuration to determine if it is supported. If it is, PRSM imports the configuration and determines if there are any naming conflicts between discovered items and those that already exist in the database.
- Be patient. Device discovery can take time, and the time required to complete the discovery increases with the size of the device's configuration.
- Tip** If there are object naming conflicts, you are asked how you want to handle them. You can add a suffix to imported objects, or in some cases, elect to keep the object name but create an override for the device you are adding. Make your selections and continue.
- Step 4** On the summary page, evaluate the results and add descriptive information if desired.
The summary page shows the device models and the number of policies, realms, licenses, objects, object overrides, and renamed objects for the devices you are adding. You can also enter information about the device location, organization, and department. This descriptive information is for your management purposes only and does not affect the device configuration.
- Step 5** Click **Commit Now** to complete the process.
You must commit changes to put the devices into managed mode. You can click **Commit Later** if you intend to add more devices or make some immediate configuration changes, but you should not leave a newly-added device in uncommitted state for a long time.
-

Adding an ASA High Availability Pair

You can manage ASAs that are configured for active-standby high availability (HA). These devices can optionally include CX devices, which will also fail over. You manage an HA pair as a unit.

You can also use this procedure to add CX devices as an HA pair if the devices reside in ASAs that are otherwise not supported, such as those configured in multiple-context mode.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings**, then click the **Add Device** link in either Device or Repository view.
- Step 2** Fill in the following information to define the communication properties for the ASA device.
- **Device Name**—The name by which the device will appear in selectors in PRSM, typically the same as the device host name.
 - **Hostname/IP: Port**—The IP address or DNS hostname of the management interface or another interface that allows access to the internal HTTP server, and the port number used for HTTPS access. The default port is 443.
 - **Username, Password**—The user name for logging into the device and the user's password. For ASA devices, the user should have privilege level 15. If the device requires an enable password only to configure it, you can leave the Username and Password fields blank.

When you enter the hostname/IP address and port, PRSM tries to retrieve the certificate from the device. This step must be successful before you continue. You should see a green checkmark, and the Certificate field should contain a **View** link. Click the link to inspect the certificate.

- Step 3** Click **Next**.
PRSM evaluates the ASA configuration and will notice that it is configured for HA, and whether the ASAs include CX devices. You are prompted to name the HA pair.
If the device includes a CX, you can elect to add the ASA in monitor-only mode.
- Step 4** Enter a name for the HA pair, adjust the connection information for the second ASA if necessary, and click **Next**.
- Step 5** If prompted, enter the CX connection information and admin password and click **Next**.
Because you do not explicitly configure CX devices as HA pairs, the configuration is imported from only one of the CX devices; select which device to use. PRSM will keep the configuration of these devices the same going forward.
PRSM imports the configuration and determines if there are any naming conflicts between discovered items and those that already exist in the database.
Be patient. Device discovery can take time, and the time required to complete the discovery increases with the size of the device's configuration.
- Tip** If there are object naming conflicts, you are asked how you want to handle them. You can add a suffix to imported objects, or in some cases, elect to keep the object name but create an override for the device you are adding. Make your selections and continue.
- Step 6** On the summary page, evaluate the results and add descriptive information if desired.
The summary page shows the device models and the number of policies, realms, licenses, objects, object overrides, and renamed objects for the devices you are adding. You can also enter information about the device

location, organization, and department. This descriptive information is for your management purposes only and does not affect the device configuration.

- Step 7** Click **Commit Now** to complete the process.
 You must commit changes to put the devices into managed mode. You can click **Commit Later** if you intend to add more devices or make some immediate configuration changes, but you should not leave a newly-added device in uncommitted state for a long time.
-

Troubleshooting Device Import

When you add a device into the PRSM inventory, PRSM contacts the device, reads the device's configuration, and loads the supported policies and settings into the configuration database. If something goes wrong during this process, you will see error messages; please read these carefully to understand the problem.

The main issues that you might encounter fall into the following categories.

Communication Problems

There must be a route between the PRSM server and all devices you are adding. For ASA devices configured for high availability, this means that both devices must be reachable.

Additionally, the devices must be configured to respond to HTTPS, as PRSM uses this type of secure communication for a discovery and deployment. Ensure the ASA is configured to allow HTTPS access; the CX is always configured for HTTPS. Ensure that the PRSM server is allowed access to the device's management port, and that you specify the correct HTTPS port.

Finally, HTTPS communications require a valid certificate. Following are some typical problems regarding certificates:

- If time settings are not consistent between the device and PRSM, the certificate might not be valid, for example, from PRSM's point of view, the device certificate might not be valid until some future time. Using NTP on all systems is the most reliable way to ensure consistent time settings.
- Both the PRSM and device certificate must allow both server and client authentication. If you use a certificate that allows one but not the other, device import will fail.
- If you are using third-party certificates, you must add the entire certificate chain (root and intermediates) into whichever device uses the third-party certificate (PRSM, CX, and ASA). Adding just an intermediate certificate will result in certificate verification failures during import. If the device certificate is not issued by a party PRSM recognizes, you will also have to add the chain to the supplemental certificate store in PRSM.

Once the device is successfully added to the inventory, any future change to a device or PRSM certificate will require you to refresh the certificate from the PRSM device inventory.



Tip

If you used self-signed certificates on the CX, and configured NTP after installing or upgrading the device, use the **config cert-reset** command in the CX CLI to regenerate the certificate.

Device Name Problems

Two CX devices cannot have the same name and be managed by the same PRSM server. Ensure that you configure unique names when running the setup command on each device. Duplicate names can lead to certificate problems, since the device name is typically included in the certificate.

Device Login Problems

If communication is successful, PRSM must be able to log into the device:

- If you specify a username for ASA devices, the user requires privilege level 15.
- If you enabled active authentication (for the CX) on the ASA, then local usernames might not work for logging into the ASA.
- You must use the admin user for CX devices, with the correct password.

Device Configuration Problems

PRSM does not support all ASA configurations. Although PRSM tries to ignore unsupported settings, certain settings cannot be ignored. You must change these settings before adding the device.

Error messages will indicate the first unsupported feature encountered. Use ASDM or the ASA CLI to change the configuration. Because the first error only is shown in the message, look for other instances of the same type of configuration before trying the import again.

Feature License Problems

CX devices come with evaluation licenses for the services that require them. However, these evaluation licenses are not imported. Thus, if you add a device that includes policies that use features that require them, but the device uses the evaluation licenses, the PRSM server must have enough available licenses of the right type.

If the device is using paid licenses, those licenses are imported with the device, and you should not encounter problems related to license counts.

Additionally, the PRSM device license must have sufficient unused licenses to accommodate the devices you are adding.

Device Health Problems

Devices that you add must be functioning correctly for device import to be successful. Health tests include the following:

- Ping the device from the PRSM CLI, assuming you do not block ping responses. Both devices of a high-availability pair must be reachable.
- Log into the CX CLI and use the **show services status** command to verify all processes are running.
- Log into the ASA that contains a CX, and use the **show module** command to verify the health and status of the CX module. No status should be “Unknown.”
- For high-availability devices, use the **show failover** command in the ASA CLI to verify that failover is on, that the LAN interface is configured and up, and that the active and standby management interfaces are shown and monitored in all the appropriate sections.

Converting Monitor-Only Devices to Full Management

If an ASA is in monitor-only mode, where you cannot configure the device using PRSM but you can see events and dashboard information, you can convert it to full management by importing the device configuration. You can do this without deleting the device from the inventory. However, you can import the configuration only if PRSM supports the device for full management.



Tip

This procedure does not work for devices configured in a high-availability pair. If the device is configured for high-availability, you must delete it from the inventory and add it again to re-import its configuration.

Procedure

- Step 1** Select **Configurations > Policies/Settings**, switch to Repository view, and select the **Overview** tab.
- Step 2** Look for an information icon in the Last Deployed column for the device and click the icon.
A popup message explains the state of the device. If the message includes an **Import** link, you can convert this device to managed mode.
- Step 3** Click **Import** in the popup message and follow the wizard instructions.
The wizard used to import the configuration is the same one used when adding devices. Read the instructions on adding devices for details.

Viewing Device License Assignments

You can view the list of licenses assigned to each device in the inventory.

Procedure

- Step 1** Select **Configurations > Policies/Settings**, switch to Repository view, and select the **Overview** tab.
- Step 2** Click the link in the License column.
This opens the License Information window, which lists each license assigned to the device and their expiration dates.

Updating Device Management Credentials

If you change the password that PRSM is using to connect to a device, you must update the inventory with the new password.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings**, switch to Device view if necessary, and select the device.
 - Step 2** Select the **Overview** tab.
 - Step 3** Click the **Change Device Login Credentials** link in the device profile.
 - Step 4** Make your changes and click **Save**.
You can change the username and password.
-

Changing the Management IP Address

The relationship between the PRSM server and managed devices is based on the management IP addresses of all systems. If you change the management IP address for either side of the relationship, you break the relationship, and PRSM cannot manage the device.

The only way to fix the broken relationship is to delete the device from the inventory and then add it back; for CX devices, you must also log into the web interface and manually switch it to Single Device mode before adding it back to the inventory.

Therefore, if you need to change the management IP address of any system, delete it from the inventory before making the change. This will allow PRSM to unmanage the device gracefully.

If you change the PRSM management address, delete all devices from the inventory before making the change.

For PRSM and CX, use the **setup** command in the CLI to change the management address. For an ASA, use the ASA CLI or ASDM.

Refreshing Certificates

You might need to refresh the SSL certificate associated with a device when you generate a new certificate on the device or the PRSM server, or when you otherwise have communication problems between PRSM and the device. When refreshing a CX device certificate, the PRSM server certificate is also updated on the CX device.



Note

If you use self-signed certificates on the ASA, whenever the ASA reboots, it generates a new certificate, which requires that you refresh the certificate in PRSM.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings**, switch to Repository view, and select the **Overview** tab.
 - Step 2** Select the device whose certificate you want to refresh.
 - Step 3** Click the **Refresh Certificate** button.
 - Step 4** The certificates are retrieved from all of the devices associated with the inventory item and presented to you. If the certificates look right, click **Accept** to save them.
-

Deleting Devices

If you no longer want to manage a device in PRSM, you can delete it from the inventory. Deleting a device does not change the device configuration in any way; the device continues to function using its current configuration and assigned licenses.

Additionally, any items created when you added the device to the inventory are not removed. For example, discovered policy objects remain in the database. Dashboard data for the device also remains and will be visible in the dashboards contingent upon whether the time range for the dashboard includes a period in which the device was still in the inventory.

When you delete a CX device, the device is placed in unmanaged mode. You can now add it to another PRSM server, or you can manage it directly through its web interface.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings**, switch to Repository view, and select the **Overview** tab.
 - Step 2** Select the device you want to delete.
All devices associated with the inventory item you select will be deleted, including child CX devices and all devices in a high-availability configuration.
 - Step 3** Click the **Delete** button.
You are asked to confirm the deletion. Read the message carefully before clicking **Delete** in the message window.
 - Step 4** Commit your changes to complete the deletion.
Tip If communication with a CX device fails for any reason, the system can fail to put it in unmanaged mode. If this happens, log into the CX device's home page and click the link to switch to Single Device mode.
-

Troubleshooting Device Communications

Whenever PRSM communicates with a device, problems can occur that prevent success. Communication is required during configuration discovery, when you commit changes to the device, or when monitoring data is collected for display in dashboards. You might see alerts related to communications in the network overview dashboard or the device inventory list or see error messages when adding devices or deploying to them.

Following are some common communication errors:

Unsupported device

You might have added a device of an unsupported type or operating system version.

Verify the device type and operating system version by logging into the device directly. Verify that you entered the IP address for the right device.

This error is usually caught when you are trying to add the device. You might also see the error if you reassign the IP address from a supported device to an unsupported device. If this is the case, delete the device from the inventory.

User authentication error, invalid username, password

The username or password for logging into the device was rejected by the device.

If this happens while you are adding the device to the inventory, simply correct the username and password. Log directly into the device (for example, using SSH) to verify that the username/password works.

If this happens after you have added the device, and have been successfully managing it, then you probably changed the password for the user that you identified when adding the device. Update the credentials from the device overview tab.

On the ASA, keep in mind that the device uses the enable password as the default password for the HTTP server if there is no user password.

Certificate is invalid, certificate out of date, refresh certificate, HTTPS (SSL) error, cannot negotiate SSL, communication error

Secure SSL (HTTPS) communications could not be established. SSL is always used for device communications.

If this occurs when adding a device, first verify that you specified the correct port number used for SSL communications with the device, and that the HTTP server is enabled on the ASA.

If the problem is an invalid certificate, the certificate has either expired, the start date of its valid period is in the future compared to the PRSM server's current time, or the certificate does not allow both client and server authentication. If the certificate is expired, log into the device and generate a new certificate. If the problem relates to time, correct the time settings on the system that has inaccurate time. Consider using NTP to maintain consistent time for all systems that you are managing with the server.

If the problem is an out of date certificate, or you get a message saying you need to refresh the certificate, go to the inventory list, select the device, and use the **Refresh Certificate** command.

If the problem is not the certificate, verify that the HTTP server is enabled on the ASA and that you did not change the SSL port after adding the device to the inventory. If you changed the port for SSL, you can change it back to the one identified in the inventory; otherwise, you must delete the device from the inventory and add it back using the new port number.

Finally, SSL communications can fail if there is a time mismatch between the systems. For example, if the validity period for the device certificate is outside the current time of the server. Best practice is to use NTP for all systems to ensure time synchronization.

PRSM certificate is invalid

This error means that there is a problem with the certificate on the PRSM server itself. Device discovery and deployment will not work until you correct the problem. The certificate might be expired, there might be timing issues between the time settings on the server and the managed devices, or the certificate does not allow for both client and server authentication. Ensure that your time settings are good, and obtain a new server certificate. To upload the certificate, select **Administration > Server Certificates**.

Unresponsive device, cannot connect to host, device is unavailable, deployment timed out, communication error

There might not be a route between the server and the device. It is also possible that you changed the IP address or host name for the device in the device configuration, or that you changed the port number for SSL communications. Additionally, there might be firewall rules denying traffic between the devices.



Tip You cannot manage two CX devices that have the same non-default name in the same PRSM server. Discovery can time out due to certificate verification errors because the certificate subject will be the same for the identically-named devices. Ensure you give each CX device a unique name if you do not want to use the default.

Check network connectivity. Keep in mind that the issue is the network connection between the device and the server; you might be able to connect to both from your workstation even when those devices cannot connect to each other. Try logging into the CLI on both systems and using **ping** or **traceroute** to check connectivity.

If there is a route, ensure that the HTTP server is enabled on the ASA.

If there is a route between the device and the server, and you changed the IP address, host name, or SSL port number, you need to delete the device from the inventory and add it back using the new addressing information.

If these actions do not resolve the problem, check the access rules on all firewall-capable network devices that are on the path between PRSM and the device; for CX devices, this includes the device in which it resides. Ensure that the existing rules allow HTTPS traffic on port 443 to go between the hosts; you need two allow rules, one where PRSM is the source, one where the unavailable device is the source. If you configured a different HTTPS port than 443, you must allow the port you configured. Ensure that all hops in the network path have the required access rules to allow communication.



Managing Policies

Policies define the security characteristics and requirements of your network, such as rules on who can access the network, what applications they can use, what web sites they can visit, and so forth. Policies implement your organization's network security policies.

Depending on whether you are managing multiple devices, or you are directly configuring a CX device, policies can be shared among many devices or local to a single device.

The following topics explain policy basics in more detail.

- [Policy Concepts, page 103](#)
- [Configuring the Device, page 104](#)
- [Policy Basics, page 107](#)

Policy Concepts

You should understand the following basic concepts to effectively use the application and configure your device. Some of these concepts apply to Multiple Device mode only.

Rule-Based Policies versus Configuration Settings

There is a fundamental difference between a rule-based policy, such as access policies, and configuration settings, such as authentication settings.

Rule-based policies are an ordered list of policies. A policy is a single rule that defines some aspect of your firewall security policy. For example, deny access to gambling web sites, or require users to authenticate. Incoming traffic is compared against each rule, starting from the top, until a match is found. When matched, the actions defined in the rule are applied to the traffic. Examples include access, identity, and decryption policies.

Configuration settings are simple. You either configure an option or not, and your settings apply to the device as a whole, or to all traffic as a whole. Examples include authentication settings and decryption settings.

Policy Sets

Rule-based policies are composed of policy sets. A policy set is a named container within which you organize the individual policies or rules. The order of the policies in a policy set matters. In Multiple Device mode, you can share a policy set among devices.

Policy object

A definition of some characteristic that you can use in a policy. For example, you use a URL object to define the URL category that you want to control access to in an access policy. Because policy objects are separate entities, you can reuse them in multiple policies. In Multiple Device mode, the objects are configured on a device only if a policy configured on the device uses the object.

Shared versus Local Policies or Settings

In Single Device mode, all policies and settings are local, that is, they apply to the device you are configuring only.

In Multiple Device mode, you have the option to share a policy or setting among devices. In this case, you can consider “policy” to generically apply to any shareable policy or configuration setting.

When you share a policy, each device to which the policy is assigned gets the same settings. For rule-based policies, you share policy sets, so that each device might use shared policies yet include a different collection of policy sets. For configuration settings, you share the entire page of settings.

You cannot share all types of policy. Some settings are global and apply to all devices. Other settings are always local to a single device. For devices configured as high availability pairs, you share policies based on the pair’s logical name, so that each member device gets the same configuration.

Shared versus Universal Policy Sets

There are two types of shared policy set: shared among specific devices and universal.

Policy sets shared among specific devices are applied to those devices only. Any devices you add to the inventory are not affected.

Universal policy sets are applied to every device (of the correct device type), even devices that you add to the inventory in the future. Thus, you can define a set of policies that should always be enforced (for example, you could always block finger traffic).

Universal policy sets apply to access policies only, and there are two pre-defined ones:

- **Universal Top**—These policies are always at the top of the ordered list of access policies. Traffic is always compared to the matching rules for these policies before any other shared or local policies.
- **Universal Bottom**—These policies are always at the bottom of the list. Traffic is not compared to these rules until all other access policies have been evaluated. This would be where you place a Deny All policy to cover any remaining traffic that is not explicitly allowed, for example.

Whenever you edit policies in a Universal policy set, you are editing them for all devices, whether you do it while configuring a specific device in Device view, or you do it in Repository view.

Configuring the Device

To configure most policies and device settings, select **Configurations > Policies/Settings**.

The Device Configuration page has a tabbed layout, with each tab representing a different rule-based or configuration settings policy. You can open and close tabs as you need them. If a tab is not already open, you can select it from the drop-down menu icon on the right side of the tabs. When you have a lot of tabs open, tab names might be truncated.

Use the **Overview** tab to get a general picture of the device's configuration.

The overall contents of the page itself differs depending on your mode. In Single Device mode, the page contains the tabs only. In Multiple Device mode, the tabs appear under two distinctly separate views.

Device View

In Device view, the left column shows the list of devices in the inventory. You select a device to see and edit its configuration. Use the filter box to help you find a device, or change the View By setting to see the inventory organized in different ways.

Mouse over a device in the selector to see details such as device types and model, management addresses, and mode.

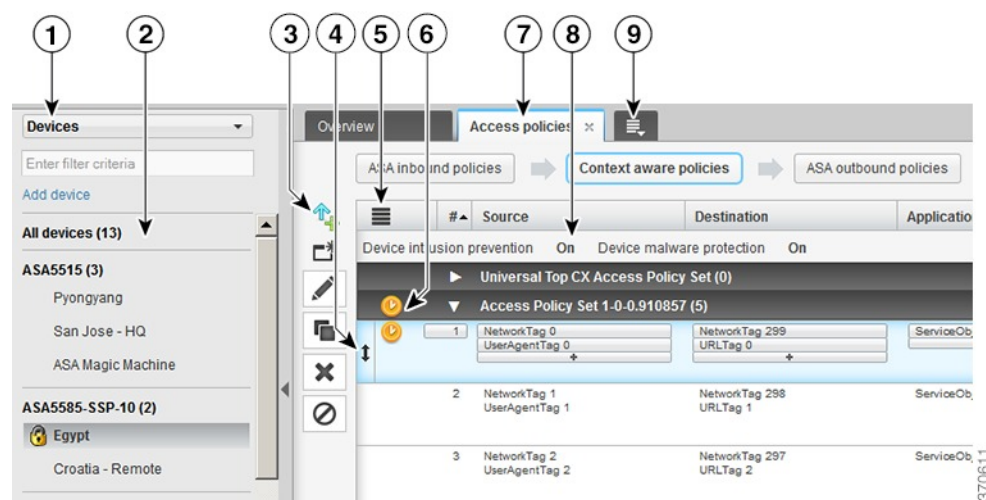
Repository View

In Repository view, you can see the device inventory with detailed information on the Overview tab.

On the policies tabs, you see a list of all policies in the system across all devices. Each policy is a separate expanding/collapsing folder, open it to see the policy contents. From here, you can find and change policies independently of the device, making it easy to change shared policies, or even to make across-the-board changes to a type of policy for many devices.

After making changes in Repository view, you can return to Device view and verify you are getting the desired configuration for each device.

The following graphic explains the various elements of the Device Configuration page. The image shows Multiple Device mode; in Single Device mode, the tabbed area is the entire page.



- 1 Device/Repository view toggle (Multiple Device mode).
- 2 Device Selector (Multiple Device mode).

- 3 Policy action buttons. For rule-based policies, select a rule or policy set to see action buttons related to your selection.
- 4 Move policy or policy set handle. For rule-based policies, click and hold this icon to drag the policy or policy set to the desired position.
- 5 Expand All/Collapse All button. For rule-based policies, this opens or closes all policy sets.
- 6 Notification icons. These identify pending changes, potential user editing conflicts, or other important information. Mouse over for detailed information. Clicking the icon can also provide information, but in the case of the Pending Changes icon, clicking performs an action, taking you to the Pending Changes page.
- 7 Policy and settings tabs. The Overview tab is always visible. If you have more tabs open than fit, tab scroll arrows appear, allowing you to scroll right and left.
- 8 Feature status: Shows whether intrusion prevention (Next Generation IPS filtering) and malware protection (web reputation) are on or off for the device. Mouse over the On/Off indication to see details about the device-level profile for each feature. There is an **Edit Settings** link in the popup to open the settings tab for the feature, where you can change the status and profile.
- 9 Tab menu. Open tabs from this menu.

The following topics provide an overview of the policies and settings available on the Device Configuration page.

Device Configuration Policies and Settings

You can configure the following policies and settings on the Device Configuration page. The available options differ between Single Device mode and Multiple Device mode and by device type.

Basic Policies

These policies control traffic passing through the device.

- **Access Policies**—Control access to the network. In Single Device mode, these are CX policies only. In Multiple Device mode, you can configure both CX and ASA access policies.
- **NAT Policies**—(ASA, Multiple Device mode only.) Translate network addresses between internal and external versions.

Logging

These policies control device logging.

- **ASA CX Logging**—(CX only.) Controls logging levels for CX devices.
- **Syslog Settings**—Configure syslog servers for ASA and CX, and logging settings for ASA devices. ASA options are available in Multiple Device mode only.

Basic Device Properties

These policies configure functional device settings.

- **Packet Capture**—(CX only.) Set packet capture options and perform global capture of dropped packets.
- **Interfaces**—(ASA, Multiple Device mode only.) Configure device interfaces.
- **High Availability**—(ASA, Multiple Device mode only.) Configure failover between devices to increase network reliability.
- **Traffic Redirection**—(ASA, Multiple Device mode only.) Configure traffic redirection from the ASA to its CX module.
- **Intrusion Prevention**—(CX only.) Enable Next Generation IPS filtering and configure device-level settings.
- **Malware Protection**—(CX only.) Enable web reputation filtering and configure device-level settings.

Decryption

These policies control SSL/TLS decryption.

- **Decryption Settings**—(CX only.) Enable decryption policies and identify the Certificate Authority (CA) certificate that the device will use to managed decrypted traffic flows.
- **Decryption Policies**—(CX only.) Determine whether to decrypt TLS/SSL traffic flows. Decrypting HTTPS and other TLS/SSL traffic flows provides greater visibility into the content of encrypted traffic flows, such as application behaviors, and more detailed threat analysis.

Authentication and Identity

These policies control user and group identification, which enables identity-based access control.

- **AD Agent**—(CX only.) If you are using Active Directory, you can install the Context Directory Agent (CDA) or Active Directory agent to provide passive user-to-IP address mappings based on Windows login authentications.
- **Auth Settings**—(CX only.) Control active authentication timeouts and refresh intervals.
- **Identity Policies**—(CX only.) Determine whether a user must authenticate. The purpose of authentication is to determine the user who is involved in a traffic flow, so that you can apply identity-based access policies to traffic flows.

Policy Basics

The following topics explain how to configure local (single device) or shared (multiple device) policies.

Configuring Policy Sets

Use policy sets to define a segment of a rule-based policy. The policy set appears as a heading row in the policy list, and you can open and close it to show or hide the policies it contains. The policy set header shows the number of policies contained in the set. In Multiple Device mode, you can share policy sets among devices.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and open the tab for the rule-based policy. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Select a policy set, then do one of the following:
- To create a new policy set, click the **Add Policy Set** button. You can also create a new policy set when a policy is selected.
 - To edit an existing policy set, click the **Edit Policy Set** button. You can also click into the policy set fields in the table and type your changes.
 - To create a copy of a policy set, click **Duplicate Policy Set** button. In Multiple Device mode, if you duplicate a Universal policy set, the copy is created as a local policy set.
- Step 3** Fill in the policy set properties:
- **Policy Set Name**—The name of the policy set.
 - **Policy Set Type**—The type of policies that will be included in this policy set.
 - **Description**—A description of the policy set.
 - **Devices**—(Multiple Device mode only.) The devices that should share this policy set. In Device view, this is initially set to include the device you are configuring; in Repository view, it is empty (“not installed”), and the policy set will not be assigned to any device unless you make a selection.
 - **Tags**—Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.
 - **Ticket ID**—A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)
- Step 4** Click **Save Policy Set**.
- Step 5** If necessary, move the policy set so that it is in priority order. Policies are applied on a first-match basis, and the order is defined not only by their order within a policy set but also by the order of the policy sets themselves.
-

Configuring Rule-Based Policies

Policies define the security characteristics and requirements of your network, such as rules on who can access the network, what applications they can use, what web sites they can visit, and so forth. Policies implement your organization's network security policies.

Policies are grouped into policy sets. Policies are evaluated on a first-match basis; incoming traffic is compared to the match criteria for each policy in a set from top to bottom, and the first policy whose traffic matching criteria is satisfied defines the security policy applied to the traffic. Thus, order within a policy set is critical. If there are multiple policy sets, the sets are evaluated in the same order.

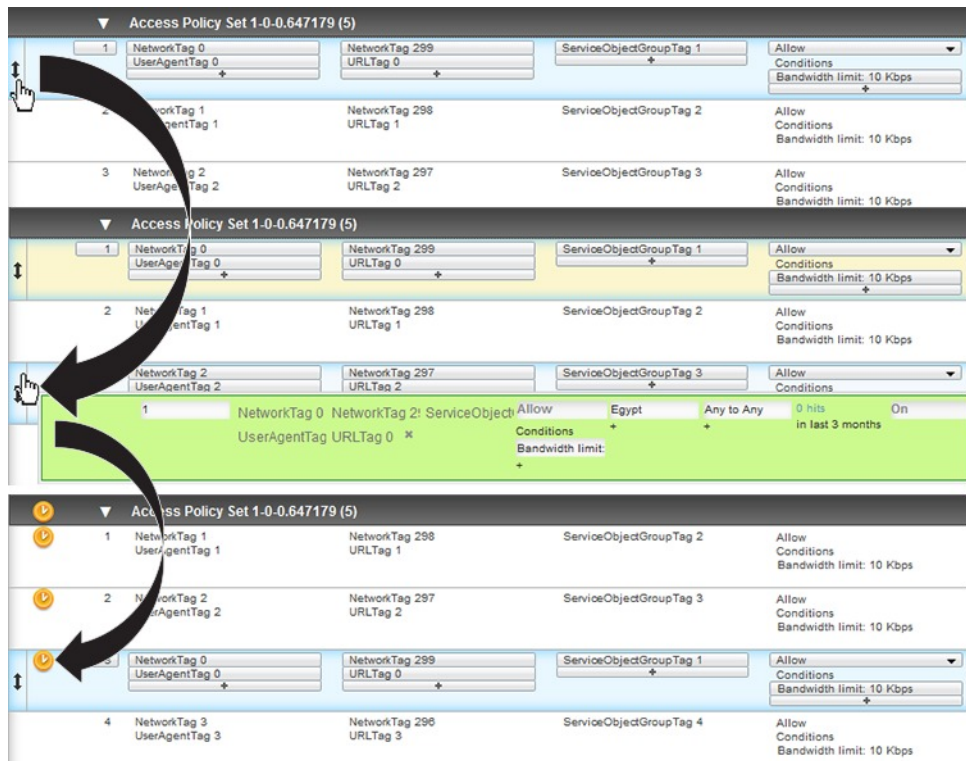
Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and open the tab for the rule-based policy. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Do any of the following:
- To add a new policy, use one of the **Add Policy** buttons. If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.
 - To edit an existing policy, select the policy and click the **Edit Policy** button.
 - To base a new policy on a similar existing policy, select the policy and click the **Duplicate Policy** button.
- A form opens with the policy properties for the type of policy you are creating or editing. For detailed information about these properties, click the Help link in the form or see the chapter for the policy in this guide.
- Step 3** Fill in the policy properties and click **Save Policy**.
- Step 4** If necessary, move the policy so that it is in priority order. Policies are applied on a first-match basis, so you must ensure that policies with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.
- To move a policy set or rule, you click and hold the Move icon (the vertical double-headed arrow on the left margin) and drag it to the policy after which you want to insert it. You can also simply edit the sequence number and change it to the desired value.
-

Moving Policy Sets and Rules

In rule-based policy sets, the order of the policy rules matters, because they are matched to traffic from top to bottom and the first match determines the policy applied to the traffic. Thus, you need to move policies and policy sets to ensure they are in the right order.

To move a policy set or rule, you click and hold the Move icon (the vertical double-headed arrow on the left margin) and drag it to the policy after which you want to insert it, as illustrated in the following graphic. You can also simply edit the sequence number and change it to the desired value.

**Tip**

You cannot move policies between policy sets. Instead, you must recreate the rule in the desired policy set.

Changing Policy Sharing Status

(Multiple Device mode only.) For policies and policy sets that allow sharing among devices, you can change the sharing settings, converting local policies to shared and vice versa.

In addition to using this procedure, you can adjust the devices that share a policy set when editing the policy set.

**Tip**

When you apply multiple policy sets of a particular type to the same device, they are evaluated in the same order in which they appear on the policy tab. Use Device view to verify the order for a particular device is the desired one.

Procedure

- Step 1** Select **Configurations > Policies/Settings** and open the tab for the rule-based policy. You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Step 2 Click the shared status link for the policy or policy set. The link is named **Device Name** for unshared policies, or **Shared** for those already shared.

A popup opens with the actions you can implement for this item. The available commands differ based on current sharing and policy type.

Step 3 In the popup, do any of the following:

- To share a local policy, click **Shared**, then select the devices that should share the policy. The device currently assigned to the policy is already selected, but you can delete it from the list.
- To change the devices for a shared policy, simply change the devices already listed. You can add or delete devices. Any device you remove is assigned a local policy with the same content.
- To make a shared policy local, click **Local**.

Step 4 Click **Apply**.

What to Do Next

When you initially share a policy set with a device, the policy set is added to the top of the policy list for the device; in the case of access rules, just below the universal top policy set. You need to go to the policy tab in Device view for each device you add to a policy set, and move the newly-shared policy set to the desired position.

Making Per-Device Exceptions for Shared Policy Sets

(Multiple Device mode only.) For rule-based policies, you can share policy sets among multiple devices so that the devices provide consistent services. However, it is not uncommon that a given device should implement the same policies as a group of other devices yet also have some unique requirements. For example, you might need to add more restrictive access to a network controlled by a certain device.

By creating per-device exceptions, you can share a common policy set among a group of devices yet also create a few device-specific policies within that otherwise shared policy set. These per-device exceptions can be for one device or for a subset of the devices assigned to the policy set. You cannot share these exceptions with devices that are not already sharing the policy set that contains the exception policy.



Note Per-device exceptions for rule-based policies are possible with ASA or CX access policies only.

Procedure

Step 1 Select **Configurations > Policies/Settings** and open the **Access Policies** tab.

You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Step 2 Do any of the following:

- If the policy does not yet exist, create it, and in the **Shared/Local** field, select the devices that should implement the policy.

- Edit an existing policy and select the devices that should implement the policy in the **Shared/Local** field.
- For existing policies, click the + button in the **Shared/Local** column and select the devices that should implement the policy.

Leave the **Shared/Local** field blank if you want all devices that share the policy set to implement the policy. If this field contains any specific device, the field defines the complete list of devices that will implement the policy.

Editing Rule-Based Policies and Policy Sets

After creating a policy set or a policy in the set, you can edit it.

Procedure

- Step 1** Select **Configurations > Policies/Settings** and open the tab for the rule-based policy. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** You then have two options for editing a rule-based policy or policy set. Do either of the following:
- Traditional—Select the policy or policy set, then click the **Edit Policy** or **Edit Policy Set** button. A window opens where you can make your changes; click the save button when finished.
 - Inline editing—If a policy supports inline editing, select the policy or policy set, then make changes directly in the table. Mouse over each column in the row to see possible actions. You can click the + button in a field to add to the column, delete items, change the policy action, click in edit fields and type in different text, and so forth. In access policies, if you select an application that supports behaviors, click the **Behaviors** button to configure them.
-

Disabling or Enabling Rule-Based Policies

You can disable a rule-based policy if you want to temporarily stop applying it to traffic. You do not need to delete the policy unless you really no longer need it.

You can also easily enable policies you had disabled.

When disabled, a policy is hashed out in the policy table.

Procedure

- Step 1** Select **Configurations > Policies/Settings** and open the tab for the rule-based policy. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Step 2 Select the policy, then do one of the following:

- Click the **Disable Policy** button.
- Click the **Enable Policy** button.

Step 3 Commit your changes.

Analyzing Shared Policy Assignments

(Multiple Device mode only.) When working in Repository view, you can analyze how your policies are shared among devices. To open Repository view, select **Configurations > Policies/Settings**, then select **Repository** above the device selector.

As you select policy tabs, the following links appear in the left pane if they apply to the tab. Use these links to filter and analyze policy assignments:

- **All**—View all policies regardless of assignments.
- **Local**—View only those policies that are local to a device. That is, policies that are not shared.
- **Shared**—View only those policies that are defined as shared, including Universal policy sets. You can click the **Shared** link in the policy heading row to see the list of devices using the policy.
- **Not Installed**—View only those policies that are defined but not yet assigned to any device. You can click the **Not Installed** link in the policy heading row to assign the policy.

Deleting Policies or Policy Sets

Delete policies or policy sets when you no longer need them. However, before you delete a policy or policy set, consider these methods of temporarily disabling them:

- **Policies**—You can temporarily disable a policy by disabling it. When you commit changes, devices assigned the policy will no longer enforce it.
- **Policy Sets**—(Multiple Device mode only.) Unassign the policy set from any device that references it. When you commit changes, the entire policy set is removed from the device and replaced with whatever new policy sets you assigned.

Procedure

- Step 1** Select **Configurations > Policies/Settings** and open the tab for the rule-based policy. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Do any of the following:
- To delete a policy, select it and click the **Delete Policy** button.

- To delete a policy set, select it and click the **Delete Policy Set** button.
-



Managing Policy Objects

Policy objects are reusable containers that define criteria that you want to use in policies. The following topics explain policy objects in more detail.

- [Policy Objects, page 115](#)
- [Policy Object Reference, page 121](#)

Policy Objects

Policy objects are reusable containers that define criteria that you want to use in policies. Some objects define traffic matching criteria, such as network groups, which can identify hosts or networks for which you want to control access or to define identity policies. Other objects define profiles, which apply specific types of services to matching traffic.

Policy objects let you define proposition criteria so that you can easily reuse the same criteria in different policies. When you update a policy object, all policies that use the object are automatically updated.

CX policies require that you use policy objects; you cannot enter traffic matching or profile settings directly in a policy. You have the flexibility of creating objects independently on the Policy Objects page, or you can create them while you are configuring a policy.

To open the Policy Objects page, where you can create, edit, delete, and view objects, select **Components > Objects**. You have the flexibility of creating objects independently on the Policy Objects page, or you can create them while you are configuring a policy.

The Policy Objects page includes the following items:

I want to

This list includes the following commands:

- **Add *Object Type***—To create a new object of this type. For an overview of the available objects, see [Policy Object Types, on page 116](#).
- **Import External Objects**—(Multiple Device mode only.) To import objects exported from a network management application. See the [release notes](#) for a list of supported applications and object types.

List of Policy Objects

All policy objects are presented in a single list.

Each object shows the object name, a summary of the content of the object, and on the right side, the object type and a summary of the policies and objects in which the object is used, if any. If a Pending Commit banner appears on the right, the object has not yet been committed to the device database.

To see the commands related to an object, mouse over the object; the following commands appear along the bottom of the object row:

- **Delete Object**—To delete the object. You cannot delete an object if it is currently being used in a policy or another object, or if the object was created by the system (a pre-defined system object).
- **Edit Object**—To edit the object.
- **View Object**—(Pre-defined system objects only.) To view the object contents.

The following topics explain object management in more detail.

Policy Object Types

You can divide policy objects into the following types:

- Those that you can use in CX policies only.
- Those that you can use in both ASA and CX policies, and which are available in both Single Device mode and Multiple Device mode.
- Those that you can use in both ASA and CX policies, but which are available in Multiple Device mode only. These objects are typically native to the ASA; the ability to use them in CX policies is a convenience.
- Those that you can use in ASA policies only. These objects are available in Multiple Device mode only.

The following lists summarize the objects you can create. See the reference topics for detailed information.



Note

Availability of CX objects differs based on the CX platform and the feature licenses you have purchased. These lists are complete; your platform or license might not support all object types.

CX-only Policy Objects

The following objects are available for use in CX policies only.

- **CX Network Group**—IP addresses to identify hosts and networks.
- **CX Identity Object**—User identity, including user names and user group names.
- **URL Object**—Web domains or servers (such as example.com, www.example.com) Web URL resources (HTTP or HTTPS only, such as http://example.com/games), and web (URL) categories.
- **User Agent Object**—Types of agents used to make HTTP requests, as identified in the user agent field in HTTP packet headers. For example, browser types (Internet Explorer, Firefox, and so forth).
- **Application Object**—Applications or application types or tags, which can be identified regardless of port used during any particular connection session.

- **Secure Mobility Object**—Client platforms (operating systems) used in an AnyConnect Secure Mobility remote access VPN connection, which identify the type of device that is connecting to your network.
- **Application Service**—Define an application based on a combination of service group objects (traditional protocol and port specifications), application specifications, or application objects. You can create multiple combinations that are OR'ed, so that a single application service object can define a very exact traffic pattern.
- **Destination Object Group**—Define a potentially complex destination traffic match criterion using the objects allowed in the destination field of a policy. You can create a definition of network group and URL objects that are AND'ed so that all objects must be satisfied for traffic to match the policy. You can create multiple combinations that are OR'ed, so that a single destination object group can define a very exact traffic destination pattern.
- **Source Object Group**—Define a potentially complex source traffic match criterion using the objects allowed in the source field of a policy. You can create a definition of network group, identity, user agent, and Secure Mobility objects that are AND'ed so that all objects must be satisfied for traffic to match the policy (you cannot create this relationship directly within the access policy). You can create multiple combinations that are OR'ed, so that a single source object group can define a very exact traffic source pattern.
- **File Filtering Profile**—An action profile that controls the types of files that users are allowed to upload or download.
- **Web Reputation Profile**—An action profile that controls which parts of an otherwise allowed web page can be returned to the user based on the public reputation of the web site.
- **NG IPS Profile**—An action profile that applies Next Generation IPS filtering, which can drop otherwise allowed traffic.
- **Header-Injection Profile**—An action profile that inserts a header into HTTP Request messages directed to web sites that support the header. This can provide special processing of requests for web pages.

ASA and CX Policy Objects (Single Device mode, Multiple Device mode)

The following objects are available for use in both ASA and CX policies and are available in all operational modes.

- **Interface Role**—A group of name patterns that identify interfaces on the device.
- **Service Group**—Protocol and port definitions, such as TCP/80 for TCP traffic on port 80.
- **Time range**—Defines time ranges to limit the effective life of a policy or to define the times of day and days of the week when a policy should be in effect.

ASA and CX Policy Objects (Multiple Device mode only)

The following objects are available for use in both ASA and CX policies. These objects are available in Multiple Device mode only; however, if you use these objects in a CX policy, and return the CX to Single Device mode, these objects will be available on the device, where you can edit and delete them, but not create new ones.

- **Network object group**—One or more IP addresses to identify hosts and networks. You can also refer to other objects.

- **Network**—A single value that defines a host, network, or range of addresses. The value can be addresses or a fully-qualified domain name (FQDN). You can define object NAT on these objects.
- **Service**—A single value that defines a service, such as a protocol or protocol/port.

ASA-only Policy Objects (Multiple Device mode only)

The following objects are available for use in ASA policies only.

- **ASA Identity Object**—Defines user or group names to use in identity-based firewall rules.

Configuring Policy Objects

You can configure policy objects directly through the Policy Objects page, or you can configure them while configuring policies. Either method yields the same results, a new or updated object, so use the technique that suits your needs at the time.



Note

You cannot edit the contents of a pre-defined system object, although you can view them.

Procedure

- Step 1** To open the form for creating or editing an object, do one of the following:
- To create an object directly, select **Components > Objects**, then select **I want to > Add Object Type**.
 - To edit an object directly, select **Components > Objects**, then mouse over the object and click **Edit Object**.
 - To create an object while creating or editing a policy, click in the field to which you are adding the object and select **Create New Object** at the bottom of the drop-down list. If the field accepts more than one type of object, select the type in the **Object Type** field before filling in the object properties.
 - To edit an object while editing a policy, you need to open the details form for the object, where you can click the **Edit Object** button in the form to edit the object definition.
 - If the object is already specified in the policy, click the object name.
 - If the object is not specified, click in a blank area in the field in which you are adding the object to open the list of available objects, find the object in the list, and click the **View Details** link next to the object.
- Step 2** Fill in the object properties, which differ based on object type. See the reference topics for the object types for details.
- At the very least, enter a name for the object. The name must be unique among objects of all types, not just objects of the selected type. If you change the name of an existing object, the object name is also changed in every policy object or policy that refers to the object.
- If an object has both include and exclude lists, the exclude lists relate solely to the contents of the include list, excluding items that would otherwise match criteria in the include list. The typical default for the include list, Any, is used only if you do not specify anything in any include properties. Once you specify an item in a

single include property, the default for the other properties is removed and those properties are ignored unless you explicitly enter a value.

Tip You can enter multiple values in the object, and these values are considered to be in an OR relationship unless an explicit AND is shown. That is, traffic will match the object if the traffic matches any item specified. Typically, objects have multiple fields that allow you to enter values or nest other existing objects. For example, in a URL object, you can enter a combination of specific URLs, web categories, and other URL objects. Any fields that you leave blank are ignored.

Step 3 Click **Save Object** to save your changes.

Customizing Object Contents for a Device

(Multiple Device mode only.) You can create object overrides so that a single object defines different values for different devices.

Thus, you can create an object whose definition works for most devices, and then create modifications to the object for the few devices that need slightly different definitions. Object overrides make it possible for you to create a smaller set of shared policies for use across your devices without giving up the ability to alter policies when needed for individual devices.

For example, you might want to enforce more restrictive access requirements for your management network at each site. If the network address of this network differs by site, you can create a single network object called Management Network, and create overrides for each device to specify the local management network address. Thus, you can have a single object, and single policy, that provides the same service to each site's management network.

Not all objects can be customized by device. If the Overrides section does not appear in an object, you must create separate objects and policies to define different values for a device.

Procedure

Step 1 Select **Components > Objects**.

Step 2 Mouse over the object and click **Edit Object**.
You can also define overrides when creating new objects.

Step 3 In the Overrides section, do any of the following:

- To add a new override, click the Add + button, select the device for which you are defining the override, and enter the desired values.
- To edit an existing override, open it in the list and make your changes.
- To delete an override, click the trash can icon to the right of the override.

Step 4 Click **Save Object**.

Importing Objects

(Multiple Device mode only.) You can import certain types of objects that you export from a supported network management application. For information on the specific applications and object types supported, see the release notes at <http://www.cisco.com/c/en/us/support/security/asa-next-generation-firewall-services/products-release-notes-list.html>.

Whether imported objects update existing objects in the configuration database, based on object name only, depends on the following complex factors:

- If an object of the same name does not exist in the database, the object is imported. Internally, the object is marked as an imported object.
- If an object of the same name exists in the database, and that object is still marked as an imported object, the object's definition is replaced with the imported definition. Thus, if you update the object in the other application, and export it to PRSM, you can update the PRSM version of the object to align with the definition in the other application.
- If an object of the same name exists in the database, but you have previously edited the object in PRSM, the imported object is considered to conflict with the existing object. You are prompted to add a suffix to the imported object or if supported, to create a device-level override; the object in the PRSM database is not changed.
- If an imported object has defined device-level overrides, those overrides are not preserved in PRSM. Instead, unique objects are created for each override.

This behavior is summarized in the following table.

Imported object name exists in PRSM	You have edited the object in PRSM	Action
No	N/A	Object is imported.
Yes	No	PRSM object is updated with the contents of the imported object.
Yes	Yes	You are prompted for a suffix to add to the imported object name. The PRSM object is not changed.

Before You Begin

Export the objects using the capabilities of the supported application.

In Cisco Security Manager, you must enable the option to include the object type column, **-g true**. For service objects, you must also include the option to flatten port list objects to their contents, because PRSM does not support port lists; **-e true**. For example, you could export service objects using the following command (see the CSM user guide for complete and up-to-date usage information):

```
C:\CSCOpX\bin> perl PolicyObjectImportExport.pl -u admin -p admin -o export
-t Service -e true -g true -f C:\csmServices.csv
```

You might be able to access PRSM directly from the other application when exporting then importing objects; see the documentation for the other application for details. Depending on the application, you will export the objects in CSV or JSON format. Cisco Security Manager uses CSV (comma-separated values).

Procedure

-
- Step 1** Select **Components > Objects**.
- Step 2** Select **I want to > Import external objects**
If there are pending changes that you have not yet committed, you must commit them before continuing. Click **Go to Pending Changes** to open the Commit and Deploy changes page, and commit your changes. You can then return to this page to restart the process.
- Step 3** In the Import Objects window, click **Browse** and select the file that contains the exported objects.
- Step 4** Click **Import**.
PRSM evaluates the content of the file and compares the objects to those already defined in the database. If there are any conflicts, where an object you are importing has the same name as one in the database, but with different content, you are shown the conflicts. Select how to handle the conflicts and continue.
If all objects have already been imported, you are told so. No changes will be made, you can close the wizard.
- Step 5** To complete the process, click **Commit**.
If you do not want to immediately commit your changes, click **Commit Later**.
-

Deleting Policy Objects

If you no longer need a policy object, you can delete it, with the following restrictions:

- You cannot delete pre-defined system objects.
- You cannot delete an object that is currently in use, for example, in a policy or a policy object. You must first remove all references to the object before you can delete it. Examine the Object Usage list for the object to identify any policies or objects that use the object.

Procedure

-
- Step 1** Select **Components > Objects**.
- Step 2** Mouse over the object you want to delete and click **Delete Object**.
-

Policy Object Reference

The following topics describe the various types of policy object.

Common Policy Object Properties

The following table describes properties that appear in most policy objects. See the reference information for individual policy objects for information on properties unique to that object.

Table 3: Common Policy Object Properties

Property	Description
Name	The name of the object. If you change the name while editing the object, the name is automatically changed in any policy or object that refers to the object.
Object Type	The type of object. If you create the object while editing a policy, you can select the desired object type from among the types supported in the associated field. Otherwise, this information is read-only.
Description	A description of the object.
Ticket ID	A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)
Tags	Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.
Object Information	Information about the object usually appears on the right side of the object window and can include the following information: • Status—The current status of the object: • Pending (New)—The object is new and has never before been committed. • Pending (Modified)—The object has been changed since the last commit. • Committed—The object has been committed to the device configuration and no changes have been made since the last commit. • Created—The date when the object was created and the user ID of the user who created it. The System user indicates the object is a pre-defined system object. You cannot change or delete system objects.

Property	Description
Object Type Objects	One or more existing objects of the same object type. Click in the field to open a drop-down list of existing objects; typing scrolls and filters the list. The default, Any, applies if you do not specify objects or other properties in the object. The default for exclude lists is None, excluding no objects. If you can include more than one type of object, you can pre-filter the list by selecting the object type from the drop-down arrow list.
Overrides (Multiple Device mode only.)	Some objects let you create overrides to the object contents for specific devices. Thus, you can have a single object that defines different content for different devices. Not all objects allow you to create overrides. To create overrides, open this section and click the + Add button, select the device for which you are defining the override, and enter the desired values. You can delete overrides by clicking the trash can icon to the right of the override. You can add as many overrides as desired for applicable devices, but only a single override per device.
Usage	Information about the policies and objects that use this object. There are separate folders for policies and other objects; the folder heading includes the number of policies or other objects that use this object. Within the folder you can see detailed information about each policy or object.

Network Group and Network Objects

Use network group and network objects (collectively referred to as network objects) to define the addresses of hosts or networks for purposes of defining traffic matching criteria for policies. Network objects come in the following types:

- CX network group—You can use these objects in CX policies or objects only.
- Network group or Network object—(Multiple Device mode only.) You can use these objects in both ASA and CX policies or objects. These objects are available in Multiple Device mode only; however, if you use these objects in a CX policy, and return the CX to Single Device mode, these objects will be available on the device, where you can edit and delete them, but not create new ones.

The following topics describe the various network objects.

CX Network Groups

Use CX network group objects to define the addresses of hosts or networks for purposes of defining traffic matching criteria for CX policies.

CX network group objects include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Include, Exclude lists

You can configure two lists of properties, an include list and an exclude list. The exclude list is always related to the include list, excluding items that are included in the list. The scope of the exclude list is strictly within the object and does not apply to any other objects that might be selected in the same policy. Consider the following tips:

- If you allow all properties within the include list to default to Any, you can still specify items in the exclude list. The resulting object applies to “everything of this object type except for these excluded items.”
- If you specify any property in the include list, for example, selecting a policy object, the exclude list is limited to those selections. The exclude fields are not exclusively related to the same-named fields in the include list.
- Objects are simply a container of the items defined within them. Including or excluding an object is equivalent to manually typing in the content of the object into the containing object.

IP Addresses

A list of IP addresses. You must specify at least one IP address or network group object.

You can enter addresses in the following formats:

- Host IP address, any of the following:
 - Standard IPv4 address, for example, 10.100.10.10.
 - IPv6 address in compressed format, where you replace a series of fields of 0's with two colons (::), for example, 2001:DB8::0DB8:800:200C:417A.
 - IPv6 address in uncompressed format, for example, 2001:DB8:0:0:0DB8:800:200C:417A. These addresses are converted to compressed format.
- Network address, any of the following:
 - IPv4 network including subnet mask, for example, 10.100.10.0/24 or 10.100.10.0/255.255.255.0.
 - IPv6 network including prefix, for example, 2001:DB8:0:CD30::/60.
- IPv4 address ranges, with the first and last address in the range separated by a hyphen, for example, 10.100.10.5-10.100.10.10. The first address must be a lower number than the second.

Network Objects

The objects to include in the group object, if any. CX network groups can include these types of objects: CX network group, network group, and network object.

Navigation Path

- To create a CX network group object, select **Components > Objects**, then select **I want to > Add CX Network Group**.
- To edit a CX network group object, select **Components > Objects**, then mouse over the object and click **Edit Object**.

**Tip**

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

Network Object Groups

Use network object groups to define the addresses of hosts or networks for purposes of defining traffic matching criteria for both ASA and CX policies.

Network object groups include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Hosts/Networks

The IPv4 or IPv6 addresses of hosts or networks. You cannot include address ranges. You can enter addresses in the following formats:

- Host IP address, any of the following:
 - Standard IPv4 address, for example, 10.100.10.10.
 - IPv6 address in compressed format, where you replace a series of fields of 0's with two colons (::), for example, 2001:DB8::0DB8:800:200C:417A.
 - IPv6 address in uncompressed format, for example, 2001:DB8:0:0:0DB8:800:200C:417A. These addresses are converted to compressed format.
- Network address, any of the following:
 - IPv4 network including subnet mask, for example, 10.100.10.0/24 or 10.100.10.0/255.255.255.0.
 - IPv6 network including prefix, for example, 2001:DB8:0:CD30::/60.

Network Objects/Groups

The objects to include in the group, if any. Network object groups can include these types of objects: network object group and network object. They cannot include CX network group objects.

Navigation Path

- To create a network object group, select **Components > Objects**, then select **I want to > Add Network Object Group**.
- To edit a network object group, select **Components > Objects**, then mouse over the object and click **Edit Object**.

**Tip**

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX
- ASA

Network Objects

Use network objects to define the addresses of hosts or networks for purposes of defining traffic matching criteria for both ASA and CX policies.

**Note**

You cannot use a network object in CX policies if it includes an fully-qualified domain name (FQDN) or an IPv6 address range. If you already are using a network object in a CX policy, you cannot edit it to include an FQDN or IPv6 range.

Basic Object Contents

Network objects include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties, on page 122](#).

IP Address / FQDN

A single address value, any of the following:

- Host IP address, any of the following:
 - Standard IPv4 address, for example, 10.100.10.10.
 - IPv6 address in compressed format, where you replace a series of fields of 0's with ::, for example, 2001:DB8::0DB8:800:200C:417A.
 - IPv6 address in uncompressed format, for example, 2001:DB8:0:0:0DB8:800:200C:417A. These addresses are converted to compressed format.
- Network address, any of the following:
 - IPv4 network including subnet mask, for example, 10.100.10.0/24 or 10.100.10.0/255.255.255.0.
 - IPv6 network including prefix, for example, 2001:DB8:0:CD30::/60.
- IPv4 or IPv6 address ranges, with the first and last address in the range separated by a hyphen. The first address must be a lower number than the second. For example, 10.100.10.5-10.100.10.10 or 2001:DB8:0:CD30::1-2001:DB8:0:CD30::FFFF.
- Fully-qualified domain name (FQDN), a DNS hostname such as server.example.com.

Navigation Path

- To create a network object, select **Components > Objects**, then select **I want to > Add Network Object**.
- To edit a network object, select **Components > Objects**, then mouse over the object and click **Edit Object**.



Tip

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX
- ASA

Service Group Objects

Use service group objects to define traffic patterns based on protocol and port or ICMP service. Use these objects when you specifically want to target a port or range of ports, or an ICMP service. Consider using application objects if you really want to target a specific application regardless of the ports used by any given connection session. Service groups provide the more traditional port-based match criteria for firewall rules.

There are two types of service object:

- Service group—You can use these objects in ASA or CX policies or objects.
- Service object—(Multiple Device mode only.) You can use these objects in ASA or CX policies or objects. These objects are available in Multiple Device mode only; however, if you use these objects in a CX policy, and return the CX to Single Device mode, these objects will be available on the device, where you can edit and delete them, but not create new ones.

Service objects include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties, on page 122](#).

Service

A list of services. The default, Any, applies if you do not specify any services or service objects. The default for exclude lists is None, excluding no services. See below for details on how to specify services.

Service Objects (service group objects only.)

The service objects to include in the object group, if any. In Multiple Device mode, you can also select a service object.

Specifying Services

You can enter services in the following formats:

TCP or UDP Ports

One of:

- **{TCP| UDP}**[/*destination_port_or_range*]
- **{TCP| UDP}**[/*source_port_or_range/destination_port_or_range*]

where

- Protocols are **TCP** or **UDP**. You must specify TCP and UDP ports separately.
- *destination_port_or_range* is either a single port, such as 80, or a range of ports, such as 80-100, and defines the port to which the traffic is destined. If you do not specify a destination port, the object applies to any traffic that satisfies the source port requirements, regardless of destination port. For example, tcp/80.
- *source_port_or_range* is either a single port, such as 80, or a range of ports, such as 80-100, and defines the port used by the traffic source. You must specify a destination port to specify a source port. If you do not specify a port, the object applies to all traffic for the protocol regardless of port. For example, tcp/8080/80.
- You can include an operator with the port number: **lt** (less than), **gt** (greater than), **eq** (equal to), **range start end** (not equal to), or **range start end**. For example, TCP/lt 400.

IP protocol

{IP| protocol}

where you enter a well-known protocol name, such as IP, GRE, AH, ESP, and so forth, or the number associated with the protocol, such as 51 for AH. When you enter a number, it is translated to the well-known protocol name or **protocol number** after you save the object. You can also enter the number as IP/protocol. For information on IP protocol numbers, see *Protocol Numbers* at <http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml>.

ICMP services

{ICMP| ICMP6}[/*message_number*]

where

- Protocol is **ICMP** or **ICMP6** (for IPv6).
- *message_number* is the ICMP message type, 1-255. Consult an ICMP reference to determine the number associated with common ICMP commands such as echo request.

Pre-Defined Service Groups

There are many pre-defined service groups that cover common protocols and ICMP and ICMPv6 messages.. You might find that the system objects cover all of the services that you care about.

Navigation Path

- To create a service group object, select **Components > Objects**, then select **I want to > Add Service Group**.
- To edit a service object, select **Components > Objects**, then mouse over the object and click **Edit Object**.



Tip

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX
- ASA

TCP and UDP Port Keywords

When specifying services based on TCP and UDP ports, you can enter the port number directly, such as tcp/80, or you can use a keyword, such as tcp/www. The following table lists the keywords available for well-known ports.

Although you can enter the keywords in lowercase, after saving your changes, they are shown in uppercase. You must include the correct protocol to use a keyword; for example, tcp/www works, but you cannot use udp/www to indicate udp/80.

For more information about port numbers, see the IANA website: <http://www.iana.org/assignments/port-numbers>.

Keyword	Port Number	Protocol	Description
ECHO	7	TCP, UDP	Echo.
DISCARD	9	TCP, UDP	Discard.
DAYTIME	13	TCP	Day time, RFC 867.
CHARGEN	19	TCP	Character Generator.
FTPDATA	20	TCP	File Transfer Protocol (data port).
FTP	21	TCP	File Transfer Protocol (control port).
SSH	22	TCP	Secure Shell.
TELNET	23	TCP	RFC 854 Telnet.
SMTP	25	TCP	Simple Mail Transport Protocol.

Keyword	Port Number	Protocol	Description
TIME	37	UDP	Time.
NAMESERVER	42	UDP	Host Name Server.
WHOIS	43	TCP	Who Is.
TACACS	49	TCP, UDP	Terminal Access Controller Access Control System Plus.
DOMAIN	53	TCP, UDP	DNS (Domain Name System).
BOOTPS	67	UDP	Bootstrap Protocol Server.
BOOTPC	68	UDP	Bootstrap Protocol Client.
TFTP	69	UDP	Trivial File Transfer Protocol.
GOPHER	70	TCP	Gopher.
FINGER	79	TCP	Finger.
WWW	80	TCP	World Wide Web.
HOSTNAME	101	TCP	NIC Host Name Server.
POP2	109	TCP	Post Office Protocol - Version 2.
POP3	110	TCP	Post Office Protocol - Version 3.
SUNRPC	111	TCP, UDP	Sun Remote Procedure Call.
IDENT	113	TCP	Ident authentication service.
NNTP	119	TCP	Network News Transfer Protocol.
NTP	123	UDP	Network Time Protocol.
NETBIOSNS	137	UDP	NetBIOS Name Service.
NETBIOSDGM	138	UDP	NetBIOS Datagram Service.
NETBIOSSSN	139	TCP	NetBIOS Session Service.
IMAP4	143	TCP	Internet Message Access Protocol, version 4.
SNMP	161	UDP	Simple Network Management Protocol.
SNMPTRAP	162	UDP	Simple Network Management Protocol - Trap.

Keyword	Port Number	Protocol	Description
XDMCP	177	UDP	X Display Manager Control Protocol.
BGP	179	TCP	Border Gateway Protocol, RFC 1163.
IRC	194	TCP	Internet Relay Chat protocol.
DNSIX	195	UDP	DNSIX Session Management Module Audit Redirector.
LDAP	389	TCP	Lightweight Directory Access Protocol.
MOBILEIP	434	UDP	MobileIP-Agent.
HTTPS	443	TCP	HTTP over SSL.
PIMAUTORP	496	TCP, UDP	Protocol Independent Multicast, reverse path flooding, dense mode.
ISAKMP	500	UDP	Internet Security Association and Key Management Protocol.
EXEC	512	TCP	Remote process execution.
BIFF	512	UDP	Used by mail system to notify users that new mail is received.
LOGIN	513	TCP	Remote login.
WHO	513	UDP	Who.
CMD	514	TCP	Similar to exec except that cmd has automatic authentication.
SYSLOG	514	UDP	System Log.
LPD	515	TCP	Line Printer Daemon - printer spooler.
TALK	517	TCP, UDP	Talk.
RIP	520	UDP	Routing Information Protocol.
UUCP	540	TCP	UNIX-to-UNIX Copy Program.
KLOGIN	543	TCP	KLOGIN.
KSHELL	544	TCP	Korn Shell.
LDAPS	636	TCP	Lightweight Directory Access Protocol (SSL).

Keyword	Port Number	Protocol	Description
KERBEROS	750	TCP, UDP	Kerberos.
LOTUSNOTES	1352	TCP	IBM Lotus Notes.
CITRIXICA	1494	TCP	Citrix Independent Computing Architecture (ICA) protocol.
SQLNET	1521	TCP	Structured Query Language Network.
RADIUS	1645	UDP	Remote Authentication Dial-In User Service.
RADIUSACCT	1646	UDP	Remote Authentication Dial-In User Service (accounting).
H323	1720	TCP	H.323 call signaling.
PPTP	1723	TCP	Point-to-Point Tunneling Protocol.
CTIQBE	2748	TCP	Computer Telephony Interface Quick Buffer Encoding.
AOL	5190	TCP	America Online.
SECUREIDUDP	5510	UDP	SecureID over UDP.
PCANYWHERE DATA	5631	TCP	pcAnywhere data.
PCANYWHERE STATUS	5632	UDP	pcAnywhere status.

CX Identity Objects

Use CX identity objects to identify individual users, user groups, or a combination of users and groups.

As you type user or group names to enter into the object, queries are made to help automatically complete your entry and the list of matching user or group names is retrieved from the directories configured for all realms defined on the system. Select the desired name from the retrieved list. You must define a realm before you can create CX identity objects.

CX identity objects include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Include, Exclude lists

You can configure two lists of properties, an include list and an exclude list. The exclude list is always related to the include list, excluding items that are included in the list. The scope of the exclude list is strictly within the object and does not apply to any other objects that might be selected in the same policy. Consider the following tips:

- If you allow all properties within the include list to default to Any, you can still specify items in the exclude list. The resulting object applies to “everything of this object type except for these excluded items.”
- If you specify any property in the include list, for example, selecting a policy object, the exclude list is limited to those selections. The exclude fields are not exclusively related to the same-named fields in the include list.
- Objects are simply a container of the items defined within them. Including or excluding an object is equivalent to manually typing in the content of the object into the containing object.

Groups

A list of user group names. The default, Any, applies if you do not specify any users or identity objects. The default for exclude lists is None, excluding no groups.

Group names are not case-sensitive but must include the realm name in the format `Realm\group_name`. For example, if the group is called Marketing, and the group is defined in the directories defined in the system as the Corporate realm, you would specify `Corporate\Marketing`.

Users

A list of user names. The default, Any, applies if you do not specify any names or identity objects. The default for exclude lists is None, excluding no users.

User names are not case-sensitive but must include the realm name in the format `Realm\user_name`. For example, `Corporate\user1`.

Pre-Defined System Objects

The following pre-defined system objects are available:

- **Guest Users**—This object matches any user who failed active authentication on an identity policy for which you enabled guest access. Guest users is a subset of unknown users
- **Known Users**—This object matches any user for whom identity is available, either because the user actively authenticated, or because there is a passive mapping for the user’s IP address obtained from CDA or AD agent.
- **Unknown Users**—This object matches users who do not match the Known Users object, in other words, IP addresses for which a user mapping is not available.

Navigation Path

- To create a CX identity object, select **Components > Objects**, then select **I want to > Add CX Identity Object**.
- To edit a CX identity object, select **Components > Objects**, then mouse over the object and click **Edit Object**.

**Tip**

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

URL Objects

Use URL objects to identify web domains or servers (such as example.com, www.example.com) Web URL resources (HTTP or HTTPS only, such as http://example.com/games), and web (URL) categories. Use these objects to impose acceptable use policies for web browsing.

URL objects include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Include, Exclude lists

You can configure two lists of properties, an include list and an exclude list. The exclude list is always related to the include list, excluding items that are included in the list. The scope of the exclude list is strictly within the object and does not apply to any other objects that might be selected in the same policy. Consider the following tips:

- If you allow all properties within the include list to default to Any, you can still specify items in the exclude list. The resulting object applies to “everything of this object type except for these excluded items.”
- If you specify any property in the include list, for example, selecting a policy object, the exclude list is limited to those selections. The exclude fields are not exclusively related to the same-named fields in the include list.
- Objects are simply a container of the items defined within them. Including or excluding an object is equivalent to manually typing in the content of the object into the containing object.

URL

A list of individual web-based URLs. The default, Any, applies if you do not specify any categories or URL objects. The default for exclude lists is None, excluding no URLs. You can specify URLs that include just the domain or server name, so that they apply to all pages available on the all servers on a domain or at the specified server, or you can include paths to specific web pages to differentiate between pages hosted at the same site. Do not include the protocol; for example, enter `www.example.com` or `example.com`, not `http://www.example.com`. HTTP and HTTPS are the only protocols that will match these URLs.

If you want to treat all servers in a domain the same, enter just the domain name, such as `example.com`. The object would then apply to `www.example.com`, `games.example.com`, `photos.example.com`, and so forth.

For more information on entering specific URLs, see the Tips below.



Tip

When configuring URL objects for use in decryption policies, do not include path information. When evaluating whether traffic matches a URL object, the decryption policy completely ignores any URLs that include path information. If the object contains a mix of URLs with domain name only and URLs that include paths, the decryption policy treats the object as containing only those URLs that specify just a domain name. When configuring URL objects for access policies, be aware that paths cannot be matched for encrypted traffic (where a decryption policy did not decrypt the flow) or for any decrypted flow that is not HTTPS; in these cases, the access policy matches URLs that specify a domain name only.

Web Category

A list of web categories. Select all desired categories from the list of categories.

Including or excluding a category includes or excludes all web sites that belong to the category. The default, Any, applies if you do not specify any URLs or URL objects. The default for exclude lists is None, excluding no categories.

Select **Uncategorized** to match URLs that are not yet categorized.

Tips on Entering URLs

The software differentiates between the domain name and the path of a URL. The path is any string of characters to the right of the first slash "/" in a URL, for example, `www.example.com/us/` has the path "`us/`". The distinction between domain-only and domain-plus-path URLs is significant, because decryption policies will never match URLs that include paths. The following specifications are equivalent and none are considered to include path information:

```
www.example.com
www.example.com/
www.example.com/*
```

You can use the following wildcards to create URL patterns that apply to multiple pages on the web:

- * (asterisk)—To match zero or more characters. For example, `www.example.com/us/*` matches all web pages on the `www.example.com/us/` web server space.

- **^ (caret)**—Placed at the beginning of a URL, indicates a URL that starts with the following string. For example, `^www.example.com` matches all web pages that start with `www.example.com`. The difference between `^www.example.com` and `www.example.com` is that `www.example.com` will also match `server1.www.example.com` and any other sites that have modifiers prior to “`www.example.com`.”
- **\$ (dollar sign)**—Placed at the end of a URL, indicates a URL that ends with the preceding string. For example, `/index.html$` matches all URLs that point to a page named `index.html`.

Following are tips on how to accomplish likely matching goals:

- **To match all hosts at a given domain**—Enter the domain name, not the fully-qualified host name. For example, `example.com` matches `www.example.com`, `photos.example.com`, `finance.example.com`, and so forth, as well as just `example.com`. Note that `example.com$` also provides the same matching; the scope of the `$` is limited to the domain name and does not mean that requests for specific paths on the `example.com` site would bypass the match.
- **To match exactly one host**—Start the URL entry with a `^`, such as `^finance.example.com`. This will match the `finance.example.com` host only; it will not match `games.example.com`, `quotes.finance.example.com`, or `example.com`.
- **To match a group of similarly named hosts**—Use the asterisk to indicate that additional characters are allowed. For example, `example.co.*` will match any server that includes the “`example.co`.” string, including `www.example.co.us`, `example.co.uk`, and so forth. In this case, additional qualifiers are allowed at the beginning of the site name, and an unlimited string of additional qualifiers are allowed at the end of the string. Be careful when using asterisk in this way, because you might match more than you desire. For example, `example.co*` would match `example.commercialbank.com`.

Pre-Defined System Objects

The following pre-defined system objects are available:

- **YouTube for Schools**—Defines the domains used by YouTube for Schools for delivering educational materials. Use this object when creating a header-injection profile to insert your school or district ID.

Navigation Path

- To create a URL object, select **Components > Objects**, then select **I want to > Add URL Object**.
- To edit a URL object, select **Components > Objects**, then mouse over the object and click **Edit Object**.



Tip

You can also create or edit objects when you are creating or editing policies.

License Requirements

The device must have a valid Web Security Essentials license to use this type of object.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

User Agent Objects

Use user agent objects to identify types of agents used to make HTTP requests as identified in the user agent field in HTTP packet headers. For example, browser types (Internet Explorer, Firefox, and so forth). Use these objects to tailor policies based on the device being used to access the network; for example, you can explicitly exclude user agents that cannot respond to active authentication prompts from an identity policy that otherwise requires authentication.

User agent objects include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Include, Exclude lists

You can configure two lists of properties, an include list and an exclude list. The exclude list is always related to the include list, excluding items that are included in the list. The scope of the exclude list is strictly within the object and does not apply to any other objects that might be selected in the same policy. Consider the following tips:

- If you allow all properties within the include list to default to Any, you can still specify items in the exclude list. The resulting object applies to “everything of this object type except for these excluded items.”
- If you specify any property in the include list, for example, selecting a policy object, the exclude list is limited to those selections. The exclude fields are not exclusively related to the same-named fields in the include list.
- Objects are simply a container of the items defined within them. Including or excluding an object is equivalent to manually typing in the content of the object into the containing object.

User Agent

A list of user agents. The string you enter can match any part of the user agent field of the HTTP packet header. The default, Any, applies if you do not specify any user agent objects. The default for exclude lists is None, excluding no user agents.

You can use the * (asterisk) as a wildcard character to match zero or more characters. For example, Mozilla/* Gecko/* Firefox/ matches all versions of the Firefox browser.

Pre-Defined System Objects

There are many pre-defined user agent objects. You might find that the system objects cover all of the agents that you care about. Use these existing objects as building blocks to create your own user agent objects that apply to multiple types of user agent.

The NTLM Browsers pre-defined object identifies the main browsers that can respond to NTLM authentication requests.

Navigation Path

- To create a user agent object, select **Components > Objects**, then select **I want to > Add User Agent Object**.
- To edit a user agent object, select **Components > Objects**, then mouse over the object and click **Edit Object**.

**Tip**

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

Application Objects

Use application objects to identify individual applications or types of applications. Traffic inspection can identify an application regardless of the port used during any particular connection session. Use these objects to tailor policies based on the application being used during a session in place of a traditional service definition based on protocol and port.

Application objects include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Include, Exclude lists

You can configure two lists of properties, an include list and an exclude list. The exclude list is always related to the include list, excluding items that are included in the list. The scope of the exclude list is strictly within the object and does not apply to any other objects that might be selected in the same policy. Consider the following tips:

- If you allow all properties within the include list to default to Any, you can still specify items in the exclude list. The resulting object applies to “everything of this object type except for these excluded items.”
- If you specify any property in the include list, for example, selecting a policy object, the exclude list is limited to those selections. The exclude fields are not exclusively related to the same-named fields in the include list.
- Objects are simply a container of the items defined within them. Including or excluding an object is equivalent to manually typing in the content of the object into the containing object.

Application Name

A list of individual applications. Select the desired applications from the list of applications that the inspector can identify. If the application you want is not listed, try finding it under an alternate name. Otherwise, you will need to use a service group object to define the application using the traditional protocol and port specification. The default, Any, applies if you do not make selections in any of the other fields. The default for exclude lists is None, excluding no applications.

Select **Uncategorized Application** to match unknown applications.

Application Type

A list of application types. An application will map to a single application type. Select all desired types from the list of application types.

Including or excluding an application type includes or excludes all applications that belong to the type. The default, Any, applies if you do not make selections in any of the other fields. The default for exclude lists is None, excluding no types.

Select **Uncategorized App Type** to match applications whose application type is unknown.

Application Tag

A list of application tags, which provide additional categorization of applications. Select all desired tags from the list of application types. Note that an application can map to more than one application tag, and some tags and types might be similar.

Including or excluding an application tag includes or excludes all applications that belong to the tag. The default, Any, applies if you do not make selections in any of the other fields. The default for exclude lists is None, excluding no tags.

Navigation Path

- To create an application object, select **Components > Objects**, then select **I want to > Add Application Object**.
- To edit an application object, select **Components > Objects**, then mouse over the object and click **Edit Object**.



Tip

You can also create or edit objects when you are creating or editing policies.

License Requirements

The device must have a valid Application Visibility and Control license to use this type of object.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

Secure Mobility Objects

Use Secure Mobility objects to identify types of clients used to make remote access VPN connections as reported by the AnyConnect Secure Mobility application. Use these objects to tailor policies based on the device being used to access the network through a remote access VPN connection.

Secure Mobility objects include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Include, Exclude lists

You can configure two lists of properties, an include list and an exclude list. The exclude list is always related to the include list, excluding items that are included in the list. The scope of the exclude list is strictly within the object and does not apply to any other objects that might be selected in the same policy. Consider the following tips:

- If you allow all properties within the include list to default to Any, you can still specify items in the exclude list. The resulting object applies to “everything of this object type except for these excluded items.”
- If you specify any property in the include list, for example, selecting a policy object, the exclude list is limited to those selections. The exclude fields are not exclusively related to the same-named fields in the include list.
- Objects are simply a container of the items defined within them. Including or excluding an object is equivalent to manually typing in the content of the object into the containing object.

Device Type

A list of device types based on the operating system (OS) running on the device. Select a type from the list. The default, Any, applies if you do not specify any Secure Mobility objects. The default for exclude lists is None, excluding no device types.

Pre-Defined System Objects

There is a pre-defined system object named All Remote Devices. This object matches any device used in a remote access VPN connection.

Navigation Path

- To create a Secure Mobility object, select **Components > Objects**, then select **I want to > Add Secure Mobility Object**.
- To edit a Secure Mobility object, select **Components > Objects**, then mouse over the object and click **Edit Object**.



Tip

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

Application Service Objects

Use application service objects to define an application based on a combination of service groups (traditional protocol and port specifications), application specifications, or application objects. You can create multiple combinations that are OR'ed, so that a single application service object can define a very exact traffic pattern.

Application service objects include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Multiple OR'ed rows of AND'ed conditions

You can create one or more rows of traffic matching conditions. To add a row, click the **Add Another Entry** link. To remove a row, click the **Delete Entry** link for the row.

Matching criteria are evaluated as follows:

- Multiple items within a single field are OR'ed. For example, if you specify two service groups, the traffic must match object 1 or object 2. The traffic does not need to match all objects within the field (although that is also allowed).
- Multiple fields within a single row are AND'ed. For example, if you specify a service group and an application object in a single row, the traffic must match the service group and it must match the application object for the row to be considered matched.
- Multiple rows are OR'ed. For example, if you specify two separate rows of conditions, the traffic must match row 1 or row 2. The traffic does not need to match all rows (although that is also allowed). A traffic flow matches the object if at least one row is matched.

Service Objects

The service group objects, if any, for the traffic matching definition in a row. Service groups specify protocol and port, or ICMP message type, for a traffic flow.



Note (Multiple Device mode.) When using PRSM in Multiple Device mode, you can also use service objects defined on the ASA. The service group object can be used on both ASA and CX devices.

Application Objects, Types, or Names

The application objects, or other application specifications, if any, for the traffic matching definition in a row. You can pre-filter the list to items of a single type only by selecting the type from the drop-down arrow.

Navigation Path

- To create an application service object, select **Components > Objects**, then select **I want to > Add Application Service Object**.
- To edit an application service object, select **Components > Objects**, then mouse over the object and click **Edit Object**.



Tip

You can also create or edit objects when you are creating or editing policies.

License Requirements

The device must have a valid Application Visibility and Control license to use this type of object.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

Destination Object Groups

Use destination object groups to define a potentially complex destination traffic matching criterion using the objects allowed in the destination field of a policy. You can create a definition of network group and URL objects that are AND'ed so that all objects must be satisfied for traffic to match the policy. You can create multiple combinations that are OR'ed, so that a single destination object can define a very exact traffic destination pattern.

Destination object groups include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties, on page 122](#).

Multiple OR'ed rows of AND'ed conditions

You can create one or more rows of traffic matching conditions. To add a row, click the **Add Another Entry** link. To remove a row, click the **Delete Entry** link for the row.

Matching criteria are evaluated as follows:

- Multiple items within a single field are OR'ed. For example, if you specify two network groups, the traffic must match object 1 or object 2. The traffic does not need to match all objects within the field (although that is also allowed).
- Multiple fields within a single row are AND'ed. For example, if you specify a network group and a URL object in a single row, the traffic must match the network group and it must match the URL object for the row to be considered matched.
- Multiple rows are OR'ed. For example, if you specify two separate rows of conditions, the traffic must match row 1 or row 2. The traffic does not need to match all rows (although that is also allowed). A traffic flow matches the object if at least one row is matched.

Network Objects

The network groups, if any, for the traffic matching definition in a row. Network groups specify the IP addresses associated with a traffic flow.



Note

(Multiple Device mode.) When using PRSM in Multiple Device mode, you can also use network objects or groups defined on the device that contains the CX device. The network group objects come in two types: one that can be used on both ASA and CX device, and one that can be used on CX devices only, which is explicitly called CX network group.

URL Objects

The URL objects, if any, for the traffic matching definition in a row. URL objects specify the URLs or URL categories targeted in an HTTP request.

Navigation Path

- To create a destination object group, select **Components > Objects**, then select **I want to > Add Destination Object Group**.
- To edit a destination object group, select **Components > Objects**, then mouse over the object and click **Edit Object**.



Tip

You can also create or edit objects when you are creating or editing policies.

License Requirements

The device must have a valid Web Security Essentials license to include URL objects in this type of object.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

Source Object Groups

Use source object groups to define a potentially complex source traffic match criterion using the objects allowed in the source field of a policy. You can create a definition of objects that are AND'ed so that all objects must be satisfied for traffic to match the policy (you cannot create this relationship directly within the access policy). You can create multiple combinations that are OR'ed, so that a single source object group can define a very exact traffic source pattern.

Source object groups include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Multiple OR'ed rows of AND'ed conditions

You can create one or more rows of traffic matching conditions. To add a row, click the **Add Another Entry** link. To remove a row, click the **Delete Entry** link for the row.

Matching criteria are evaluated as follows:

- Multiple items within a single field are OR'ed. For example, if you specify two network groups, the traffic must match object 1 or object 2. The traffic does not need to match all objects within the field (although that is also allowed).
- Multiple fields within a single row are AND'ed. For example, if you specify a network groups and a user agent object in a single row, the traffic must match the network group and it must match the user agent object for the row to be considered matched. If you select objects in all four fields, the traffic flow must match at least one object specified in each field.
- Multiple rows are OR'ed. For example, if you specify two separate rows of conditions, the traffic must match row 1 or row 2. The traffic does not need to match all rows (although that is also allowed). A traffic flow matches the object if at least one row is matched.

Network Objects

The network groups, if any, for the traffic matching definition in a row. Network objects specify the IP addresses associated with a traffic flow.



Note

(Multiple Device mode.) When using PRSM in Multiple Device mode, you can also use network objects or groups defined on the device that contains the CX device. The network group objects come in two types: one that can be used on both ASA and CX device, and one that can be used on CX devices only, which is explicitly called CX network group.

CX Identity Objects

The identity objects, if any, for the traffic matching definition in a row. Identity objects specify user names, or user groups to which a user belongs, associated with a traffic flow.

User Agents Objects

The user agent objects, if any, for the traffic matching definition in a row. User agent objects define the agents, such as browsers, used to make an HTTP request.

Secure Mobility Objects

The Secure Mobility objects, if any, for the traffic matching definition in a row. Secure Mobility objects identify types of clients used to make remote access VPN connections using the AnyConnect Secure Mobility application.

Navigation Path

- To create a source object, select **Components > Objects**, then select **I want to > Add Source Object Group**.
- To edit a source object, select **Components > Objects**, then mouse over the object and click **Edit Object**.



Tip

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

File Filtering Profile Objects

Use file filtering profile objects to specify the types of file uploads or downloads that should be blocked. Use the profile in an access policy that otherwise allows network access to enforce file transfer acceptable use policies. For example, you could allow all downloads, but prevent all uploads, to ensure that company files are not transferred out of network.

If you do not specify a file filtering profile in an access rule, all file uploads and downloads are allowed.

File filtering profile objects include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Specifying MIME Types

The **Block file downloads** and **Block file uploads** lists contain the MIME type (Multipurpose Internet Mail Extensions, or in general, Internet Media Type) of files that users should be prevented from downloading or uploading. Select a general category, such as application/*, or a specific type, such as application/pdf. The default is blank, which allows all file downloads and uploads.

The selection list includes all supported MIME types; you cannot specify other types.

About MIME Types

The MIME type, also known as Media Type, identifies the type of file currently being dealt with and is identified in the Content Type header. There are a large number of MIME types, and you can find more detailed information about each type in sources such as Wikipedia or the IANA, with whom these types are registered (for official types, see <http://www.iana.org/assignments/media-types/index.html>). The purpose of MIME types is to identify non-ASCII files so that applications handling the file, such as E-mail clients or browsers, know which applications to use to open the file.

When specifying a MIME type in this object, you can target an entire MIME type, or you can target a specific type/sub-type. The main types are:

- application/*—Discrete data that does not fit into the other categories and which is typically processed by some type of application program before it is viewable or usable. The application category can include languages for computational material, which opens potential security holes if the transferred code is malware. Examples include application/pdf (Adobe Acrobat files), application/java, and application/postscript.
- audio/*—Audio files, such as audio/mp4 and audio/mpeg. If the file includes motion pictures, the type would be video instead of audio.
- image/*—Image or graphic files, such as image/gif and image/jpeg.
- message/*—Encapsulated mail messages, such as message/news.
- model/*—3D model files, such as model/vrml.
- text/*—Textual files, including plain and rich text, such as text/plain, text/html, text/rtf, text/javascript.
- video/*—Video files, such as video/quicktime and video/mpeg. This media type can contain synchronized audio. For example, a typical MPEG video file that includes motion pictures and sound would be a video/mpeg file.

Navigation Path

- To create a file filtering profile object, select **Components > Objects**, then select **I want to > Add File Filtering Profile**.
- To edit a file filtering profile object, select **Components > Objects**, then mouse over the object and click **Edit Object**.

**Tip**

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

Web Reputation Profile Objects

Use web reputation profile objects to define a low reputation zone so that you can apply special processing to web traffic whose reputation falls into the low reputation zone.

The Cisco Threat Operations Center uses dynamic updates and actionable intelligence obtained from ASAs, IPSs, Email security appliances, web security appliances, and system administrators to calculate a web reputation score for web sites. Web reputation is a statistical assessment based on context and past behavior and combines many factors of varying significance into one correlated metric. Similar to a person's credit score, web reputation is a continuous value along a graduated scale from -10 to 10. By defining a low reputation zone, you can implement predictive, zero-day protection against low reputation sites, the ones that are most likely to serve malware to your users.

To implement reputation-based processing, you apply a web reputation profile to the following types of policy:

- Access policies that allow traffic. By adding a web reputation profile, the policy will in general allow matching traffic, but drop any traffic from a low reputation site. You can apply the profile to any or all access policies that have the Allow action.
- Decryption policies whose action is Decrypt Potentially Malicious Traffic. By adding a web reputation profile, any low reputation sites that match the policy will be decrypted, so that access policies have knowledge of the content of the traffic. The access policies can then drop the traffic if configured to do so. Even if you do not have a matching access policy that drops the traffic, decrypting the low reputation traffic provides data for reports that is otherwise unavailable for encrypted TLS/SSL traffic flows.

For access policies, you can configure a device-level profile and have the policy use that profile. You can then easily change your default filtering policy by editing the **Malware Protection** settings.

To set the allowed and denied zones of web reputations, move the slider to the desired position; all reputations to the left of the slider are in the low reputation zone, all to the right are considered high reputation and do not receive special processing. Note that the analysis of reputation applies to all independent elements on a web page, so that users might see a page that has some elements blocked, such as a page with some blocked ads that were provided by sites whose reputation falls into the low reputation zone.

Following is a general guideline to the scores:

-10 to -6

Sites in the lowest reputation zone are dedicated or hijacked sites that persistently distribute key loggers, root-kits, and other malware. Also included are phishing sites, bots, and drive-by installers. Sites in this reputation range are almost guaranteed to be malicious.

The pre-defined default web reputation profile defines this zone as the low reputation zone.

-6 to -3

Sites in this zone tend to be aggressive ad syndication and user tracking networks. These sites are suspected of being malicious, but maliciousness has not been confirmed.

-3 to 3

Sites in this zone tend to be well managed, responsible content syndication networks and user generated content sites.

0 to 5

Sites in this zone have some history of responsible behavior or third party validation.

5 to 10

Sites in this zone have a long history of responsible behavior, have significant traffic volume, and are widely accessed.

**Tip**

To look up the reputation of a site, select **Components > Web Filtering Categories**, then select **I want to > Look up web reputation score**.

For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Pre-Defined Web Reputation Objects

The **Default web reputation profile** pre-defined object implements the recommended low reputation zone.

Navigation Path

- To create a web reputation profile object, select **Components > Objects**, then select **I want to > Add Web Reputation Profile**.
- To edit a web reputation profile object, select **Components > Objects**, then mouse over the object and click **Edit Object**.

**Tip**

You can also create or edit objects when you are creating or editing policies.

License Requirements

The device must have a valid Web Security Essentials license to use this type of object.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

NG IPS Profile Objects

Use NG IPS profile objects to define how to handle traffic that matches a Next Generation IPS threat. You can use these objects to define your filtering policy using these methods:

- **Intrusion Prevention** settings—Select a single profile that defines your default policy. You also must configure the access policy to use the device-level object.
- **Access policy**—Select a profile within an access policy, or specify that the device-level profile should be used. This defines the Next Generation IPS filtering that you want to apply to traffic that matches the access policy. If an access policy does not specify an NG IPS profile, no filtering is applied.

NG IPS profiles include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Threat Zone Sliders

The sliders define three separate threat zones. The slider is based on the threat score, with 100 being worst (on the left) and 0 being least dangerous (on the right). Move the sliders to define the following zones:

- **Block and Monitor** (Deny)—Traffic that includes threats in this zone is dropped, and you will see events for the connections in Event Viewer.
- **Allow and Monitor** (Alert)—Traffic that includes threats in this zone is allowed, but events are generated for the connections. You can use the dashboards and Event Viewer to monitor these connections.
- **Allow and Do Not Monitor** (Ignore)—Traffic that includes threats in this zone is allowed and no events are generated.

Advanced Threat Settings

This table defines exceptions to the zones defined in the slider. For example, you can identify a threat that should always be blocked regardless of its threat score. Or, you can identify a threat you believe is benign and that you want to ignore.

- To add a threat, select it from the Exceptions list, select the action you want for the threat, and click **Apply**. The exception is added to the table.
- To edit an existing exception, find it in the table and select a different action for that entry.
- To delete an existing exception, find it in the table and click **Remove** for that entry.

Pre-Defined NG IPS Profile Objects

The **Default NG IPS profile** pre-defined object implements the recommended zones.

Navigation Path

- To create an NG IPS profile object, select **Components > Objects**, then select **I want to > Add NG IPS Profile**.
- To edit an NG IPS profile object, select **Components > Objects**, then mouse over the object and click **Edit Object**.

**Tip**

You can also create or edit objects when you are creating or editing policies.

License Requirements

The device must have a valid Next Generation IPS license to use this type of object.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

Header-Injection Profile

Use the header-injection profile object to insert headers into HTTP Request messages.

Injecting a header can provide you with specialized handling of requests to sites that support the header.

Header-Injection profile objects include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Domain Match

A URL object that defines the web sites you are targeting. Headers are injected into messages sent to supported sites only, so the object can include more than just the targeted sites. The default is the YouTube for Schools object.

Header Name

The name of the header you are injecting. The YouTube for Schools header, X-YouTube-Edu-Filter, is automatically selected. You cannot insert other headers.

Header Value

The value to insert into the header. For X-YouTube-Edu-Filter, enter the school or district ID issued by YouTube for Schools.

Navigation Path

- To create a header-injection profile object, select **Components > Objects**, then select **I want to > Add Header-Injection Profile**.
- To edit a header-injection profile object, select **Components > Objects**, then mouse over the object and click **Edit Object**.

**Tip**

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

Interface Role Objects

Use interface role objects to identify interfaces on the device through which traffic passes. You can use interface roles in policies to limit the application of the policy to traffic passing through the identified interfaces only.



Tip

If you specify interface roles in a policy, and no interfaces on the device match the interface names defined in the role, the policy will never apply to any traffic on the device.

Interface roles include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Include, Exclude lists

You can configure two lists of properties, an include list and an exclude list. The exclude list is always related to the include list, excluding items that are included in the list. The scope of the exclude list is strictly within the object and does not apply to any other objects that might be selected in the same policy. Consider the following tips:

- If you allow all properties within the include list to default to Any, you can still specify items in the exclude list. The resulting object applies to “everything of this object type except for these excluded items.”
- If you specify any property in the include list, for example, selecting a policy object, the exclude list is limited to those selections. The exclude fields are not exclusively related to the same-named fields in the include list.
- Objects are simply a container of the items defined within them. Including or excluding an object is equivalent to manually typing in the content of the object into the containing object.

Interface Name Pattern

A list of interface names. You can use the asterisk (*) as a wildcard to indicate zero or more characters. For example, **outside** matches an interface named outside only, whereas ***outside*** matches any interface that includes the string “outside” somewhere within the interface name.

View Matching Interfaces

The actual interfaces that match the interface name pattern. The list refreshes when you open the section or click **Refresh**. The matches are organized in folders by device.

Navigation Path

- To create an interface role object, select **Components > Objects**, then select **I want to > Add Interface Role**.

- To edit an interface role object, select **Components > Objects**, then mouse over the object and click **Edit Object**.

**Tip**

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX
- ASA

**Note**

For CX devices, the interface names are those that exist on the host, or parent, device.

ASA Identity Objects

You can create ASA identity objects to identify individual users, user groups, or a combination of users and groups for use in identity-based ASA policies. These users and groups must be defined in Active Directory (AD), or locally on the ASA, you cannot define other types of users.

**Tip**

ASA identity objects are defined on the ASA as identity user group objects. You do not need to create these groups to duplicate groups that are already defined in AD. You can directly specify AD groups in firewall rules. Identity objects are needed only to define collections of users and user groups that do not otherwise exist in AD.

As you type user or group names to enter into the object, queries are made to help automatically complete your entry and the list of matching user or group names is retrieved from the directories configured for the AD realm defined on the system for CX policies, or from domain names used in other ASA identity objects. You can select one of these, and if a partial match, edit the selection. You can also enter free-form names.

ASA identity objects include the following primary properties. For information on properties common to most policy objects, see [Common Policy Object Properties](#), on page 122.

Groups

A list of user group names. The default, Any, applies if you do not specify any users or identity objects.

Enter groups in the *DOMAIN\group* format, where you enter the AD domain plus the group name, separated by a single \ mark.

This format differs from the one used in access rules, where a double \\ is required when specifying group names.

Users

A list of user names. The default, Any, applies if you do not specify any names or identity objects.

Enter user names in the *DOMAIN\name* format, where you enter the AD domain plus the user name, separated by a single \ mark. For users defined on the ASA, use LOCAL as the domain name.

Navigation Path

- To create an ASA identity object, select **Components > Objects**, then select **I want to > Add ASA Identity Object**.
- To edit an ASA identity object, select **Components > Objects**, then mouse over the object and click **Edit Object**.



Tip

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA

Time Range Objects

Use time range objects to limit a policy to specific times of the day and days of the week.

You can create time range objects for use when creating time-based access rules. Time-based access rules allow for access control based on time considerations. The time range applies to specific rules and makes those rules active for the specific time period defined in the range. For example, you can implement a rule for typical work hours to allow or prevent certain types of access. Traffic does not match the policy for periods outside the time range, so subsequent rules determine how the traffic is handled.

The time used for determining rule applicability is the local time on the device. Thus, a time range object when deployed defines the same relative time, but from a global perspective, that might be different times based on UTC.

Effective From, Effective To

The overall starting and ending time for the object. When you create a new object, the default is no start time and no end time, which would define a permanent time range for any policy in which you use the object.

If you want to limit the effective time frame for the object, so that its implementation is delayed to a specific date, or expires after a specific date (or both), click the calendar icons and select the desired date, then enter the time using 12-hour clock format.

Recurrences

Recurring time periods that happen within the overall start and end times, if any. For example, if you want to create a time range object that defines work hours, you could select no start or end date for the overall range, and enter a recurring range of weekdays from 08:00 AM to 06:00 PM. You can enter more than one recurrence to define all applicable times.

- To add a recurrence, click **Add Recurrence** and fill in the options:
 - **Series/Range**—Whether the recurrence is a set of discontinuous days (series) or a range of days. You can also model a range as a series.
 - **From, To**—The time period in 12-hour clock format.
 - **Every** (Series only)—Select the days of the week for this recurrence.
 - **On** (Range only)—Select the start and end days of the week to define the range.
- To delete a recurrence, click the trash can icon on the right side of the recurrence.

Navigation Path

- To create a time range object, select **Components > Objects**, then select **I want to > Add Time Range Object**.
- To edit a time range object, select **Components > Objects**, then mouse over the object and click **Edit Object**.



Tip

You can also create or edit objects when you are creating or editing policies.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX
- ASA



PART II

Monitoring Devices

- [Viewing Dashboards and Reports, page 157](#)
- [Viewing Events, page 183](#)



Viewing Dashboards and Reports

You can view dashboards or reports on a variety of items for various time periods. Dashboards can include a variety of dashboards and tables and include information on device health and performance and network usage. The following topics explain dashboards and reports.

- [Overview of Dashboards, page 157](#)
- [Dashboard Basics, page 162](#)
- [Interpreting the Network Overview Dashboard, page 173](#)
- [Interpreting the Malware Traffic Dashboard, page 179](#)
- [Interpreting the NG Intrusion Prevention Dashboard, page 180](#)
- [Interpreting the ASA Traffic Dashboard, page 181](#)

Overview of Dashboards

Dashboards aggregate information on various aspects of your network traffic. You can view dashboards on various time periods to analyze the traffic on your network. In most cases, you can drill down from general information to specific information, for example, you can view a dashboard on all users, then view details about specific users.

The following illustration shows the network overview dashboard for Single Device mode. In Multiple Device mode, there is a selector letting you pick the device and toggle between the ASA and the ASA CX.

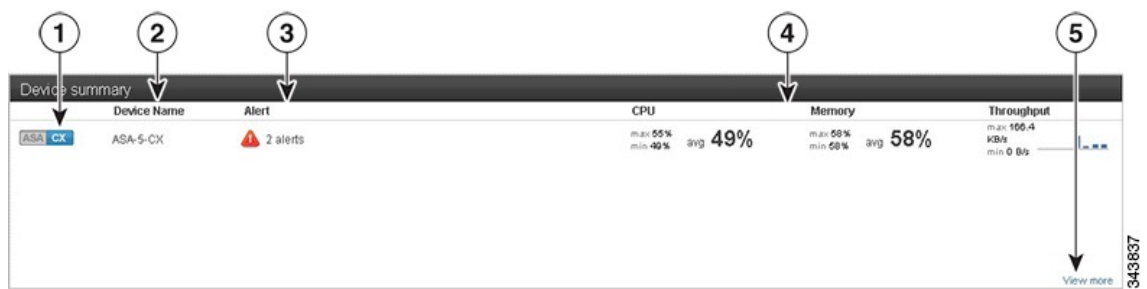
Figure 6: Network Overview Dashboard, Single Device mode



1	Device summary dashboard.	4	Health and Performance dashboard. The overview dashboard includes dashboards for several items.
2	Time selector to determine the range of data in the dashboard.	5	Mouse over graphs to see pop up details about individual data points.
3	Toggle between viewing data based on transaction count or throughput (bits per second).	6	Toggle the display to show all transactions, allowed transactions, or denied transactions.

In Multiple Device mode, the network overview device summary has a selector letting you pick the device and toggle between the ASA and the ASA CX, as shown in the following illustration. There is no toggle for independent devices.

Figure 7: Device Summary Dashboard, Multiple Device mode



1	Toggle between the ASA and the ASA CX.	4	CPU, memory, and throughput usage for the selected device over the selected time period.
2	The device display name.	5	View More link. Click this link to go to the device summary dashboard to see all managed devices, not just the top five.
3	Alerts for the device. If there is a single alert, the full text is shown; otherwise, you see a summary account of the number of alerts. Click the text to go to the device dashboard that displays the specific alerts.		

Overview and detail dashboards include multiple dashboard components such as Top Sources and Top Destinations. These dashboards show the most often occurring items of that type for the dashboard you are viewing. For example, if you are viewing the detail dashboard for a specific user, the top destinations show the most visited destinations for that user.

Figure 8: Top Destinations Dashboard



1	Dashboard title.	4	View More link. Click this link to go to the summary dashboard for that reportable item.

2	Toggle between viewing data based on transaction count or data usage (total bytes sent and received). For Next Generation IPS dashboards, the toggle is between threat hits and data usage. Threat hits can be greater than the transaction count.	5	Toggle the display to show all transactions, allowed transactions, or denied transactions. For Next Generation IPS dashboards, the toggle is for threat hits, not transactions.
3	A dashboard can contain multiple reporting items. For top destinations, you can see as many as four items: web categories, web destinations, applications, and application types. Although a dashboard might appear in multiple dashboard types, the actual content of the dashboard can vary, and the items shown are always specific to the dashboard you are viewing. Click a name to go to a detail dashboard on that item.		

Available Dashboards

The following are the main dashboards available in the product. You can open these from the **Dashboard** menu.

In general, you can click on many items, including names, icons, and View More links, to get more detailed information about individual items or about the monitored category as a whole. In Multiple Device mode, statistics are a summary of all managed devices.

Network Overview

This dashboard shows summary information about the traffic in the network and the health and performance of the device. In Multiple Device mode, health and performance information is available for all managed devices, including the ASA and its ASA CX; in Single Device mode, information is available for the CX device only. Use this information to help identify areas that need deeper analysis, or to verify that the network is behaving within general expectations.

Malware Traffic

This dashboard shows the results of transactions based on the web reputation of the web servers visited. A transaction is considered to be malicious if the web reputation of the site is -6 or lower. Use this information to help identify areas that need deeper analysis or changes to existing policies, or to verify that reputation filtering is performing within general expectations.

You can also view this dashboard by clicking **View All** in the Malicious Transactions dashboard on the network overview .

NG Intrusion Prevention

This dashboard shows the results of Next Generation IPS filtering. The dashboard will show data only if you enable IPS filtering and apply an NG IPS profile to one or more access policy. Use this information to help identify areas that need deeper analysis or changes to existing policies, or to verify that Next Generation IPS filtering is performing within general expectations.

You can also view this dashboard by clicking **View All** in the CX IPS Threats dashboard on the network overview .

ASA Traffic (Multiple Device mode only.)

This dashboard shows the top sources, destinations, and services for connections through the ASA device. From drill-down reports, you can see denied traffic information, which indicates the application of ASA firewall deny rules. For allowed traffic, keep in mind that if the device includes a CX module, traffic allowed by the ASA might be ultimately denied by CX policies. Use this information to evaluate the types of traffic going through your network.

Users

This shows the top users of your network based on total transactions, allowed transactions, blocked transactions, data usage, and bytes sent and received. Usernames are in the format `Realm\username`. Users who fail active authentication are represented in user dashboards under the username `Realm\ANONYMOUS`, unless you enabled guest access, in which case the username is Guest. Users who simply do not have a mapping because they were not required to authenticate are shown as their IP address. Use this information to help identify anomalous activity for a user.



Tip User names are available only when user identity information is associated with traffic flows. At minimum, you must define a directory realm and create an identity policy for the realm. If you want to ensure that user identity is available in dashboards for the majority of traffic, the identity policy should use active authentication. In addition, you can configure a CDA or AD agent to supply passive authentication and optionally use active authentication as a backup method.

Web Destinations

This dashboard shows which servers, such as `www.cisco.com`, are being visited. Use this information to help identify the top destinations and to determine whether additional access controls are needed to reduce the usage of undesired servers. If a domain name for a server is not available, the IP address is used.

Web Categories

This dashboard shows which categories of web sites, such as Gambling, Advertisements, or Search Engines and Portals, are being used in the network based on the categorization of web sites visited. Use this information to help identify the top categories visited by users and to determine whether your access controls are sufficiently blocking undesired categories.

Policies

This dashboard shows how the access policies have been applied to traffic in the network. If you deleted the policy, the name is appended with “- DELETED.” Use this information to help evaluate policy efficacy.

User Devices

This dashboard shows the type of user devices that are making remote access VPN connections to the network. VPN user device information is obtained through the AnyConnect Secure Mobility client during remote-access VPN connections. Use this information to help evaluate the types of client connecting to your network.

Applications

This dashboard shows which applications, such as Facebook, are being used in the network based on the Application Visibility and Control (AVC) engine's analysis of the traffic in the network. Use this information to help identify the top applications used in the network and to determine whether additional access controls are needed to reduce the usage of unwanted applications.

Application Types

This dashboard shows which application types, such as Search Engine or Instant Messaging, are being used in the network based on the Application Visibility and Control (AVC) engine's analysis of the traffic in the network. Use this information to help identify the top application types used in the network and to determine whether additional access controls are needed to reduce the usage of unwanted application types.

Cloud

This dashboard shows which applications that are tagged as being cloud-based services are being used in the network based on the Application Visibility and Control (AVC) engine's analysis of the traffic in the network. Use this information to help identify the top cloud-based applications used in the network and to determine whether additional access controls are needed to reduce the usage of unwanted applications.

Devices (Multiple Device mode only.)

This dashboard shows summary information for each device that is managed by this PRSM server. From the device detail drill-down report, you can also view information about the interfaces on the device. Use this information to help analyze the differences in usage and policy application for the different devices in your network as well as the health and performance of the device.



Note

If you delete a device from the inventory, its data remains available for historical periods. The device name is appended with "DELETED."

Dashboard Basics

The following sections explain the basics of using dashboards. These topics apply to dashboards in general and not to any single specific dashboard.

Understanding Dashboard and Report Data

Dashboard data is collected immediately from the device, so there is little lag time between the data reflected in a dashboard and network activity. However, keep the following points in mind when analyzing the data:

- Data is collected for traffic that matches an access policy in which you select **Eventing: On** only, which is the default setting for access policies. If you turn off eventing for an access policy, any traffic that matches the policy will not be represented in dashboards and will not generate events in Event Viewer.
- For Next Generation IPS dashboards, data collection is further constrained to those threats that you are monitoring. Threats that you are ignoring do not show up in threat signature hit counts.

- Data is aggregated into 5 minute buckets, and 30 minute and one hour graphs show data points in 5 minute increments. At the end of the hour, the 5 minute buckets are aggregated into one hour buckets, which are subsequently aggregated into day and week buckets. The 5 minute buckets are kept for 7 days, the one hour buckets for 31 days, and the day buckets for up to 365 days. The farther back you look, the more aggregated the data. When you query for old data, you get the best results if you align your queries to the availability of these data buckets. All day calculations are based on UTC time; the time on the server or your client is ignored.



Note If a data point is missing, for example, because the device was unreachable for longer than 5 minutes, there will be gaps in line charts.

- The “Top N” dashboards are limited to a certain number of data points. If there are more data points than the limit in a 5 minute bucket, only the data points within the limit are counted; data points outside the limit are ignored (although the events for these items persist). Thus, as data is aggregated from the 5 minute buckets, items that appear in the top N in one bucket, but not in another, will have incomplete metrics.

For example, consider the Top Users report. During the first 5 minute window, user John Doe is in the Top N users. During the next 5 minute bucket, John Doe is still generating some network traffic, but he is not in the Top N for that time window. Then, when the hourly summary is calculated from the twelve 5-minute buckets that comprise that hour, the entry for user John Doe in that summary will include the data from the first 5-minutes, but it will not include anything of John Doe's traffic from the second 5-minutes because John Doe was not in the Top-N for that time period.

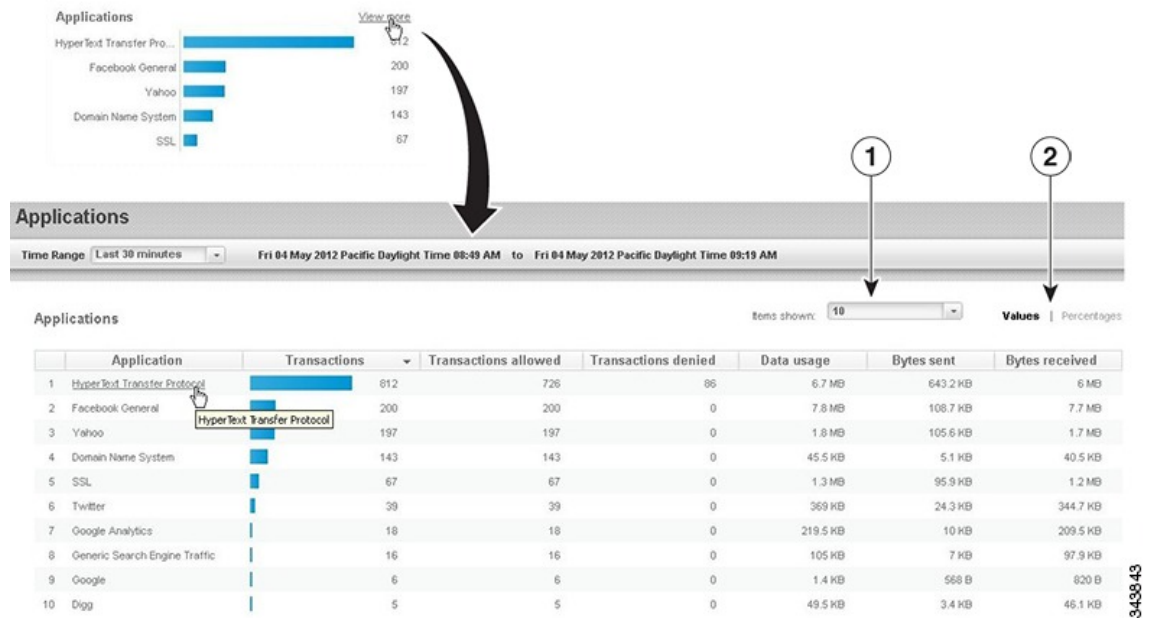
- As the storage area for event and report data is filled, the system automatically deletes older data to make room for new data. Thus, the amount of historical data available depends on the event rate and storage capacity of the system.
- (Multiple Device mode only.) If there is a break in retrieving data from a device, you can see an alert in the Time Range bar above a dashboard. This alert appears only if you select a time range that includes a break in the data for at least one device shown in the dashboard. The message indicates that “Report data may be missing due to connectivity lapses.” You can click the link to open Event Viewer to see the related system events. The Event Receiver Disconnected, Event Receiver Connected messages indicate the gaps.
- When viewing dashboards in PRSM Multiple Device mode, data is aggregated from all managed devices. To view information specific to a single device, use the Devices dashboard.
- (Multiple Device mode only.) The quality of application-based data can deteriorate if the AVC signature set used by reporting devices is more recent than the PRSM server's set. If the signature sets remain out of synchronization for a long time, data can include an increasing number of unrecognized applications. Lack of synchronization can occur if the PRSM server is persistently unable to download updates while managed devices successfully download updates, or if you disable updates when the signature sets are already out of synchronization. You get best results when all devices use the same signature set.
- (Multiple Device mode only.) ASA data is retrieved from the device and syslog events. For multiple-context mode devices, data is from the system context. If you do not define the PRSM server as a syslog server for the ASA, connection data is derived from health and performance monitoring data obtained from the device, and you cannot view statistics for allowed or denied connections. Set the syslog logging level at 6 or higher.
- (Multiple Device mode only.) High availability pairs are shown under the logical name for the pair.

Drilling Into Dashboards

Dashboards include many links to help you drill down to the information that you need. Mouse over items to see which ones might take you to more information about the item.

For example, in a typical dashboard reporting item, such as the top five applications list shown in the following graphic, you can click the View More link to go to the summary Dashboard for that item.

Figure 9: Going from top five dashboard to full summary dashboard



1

Items shown, select how many items to display in the dashboard.

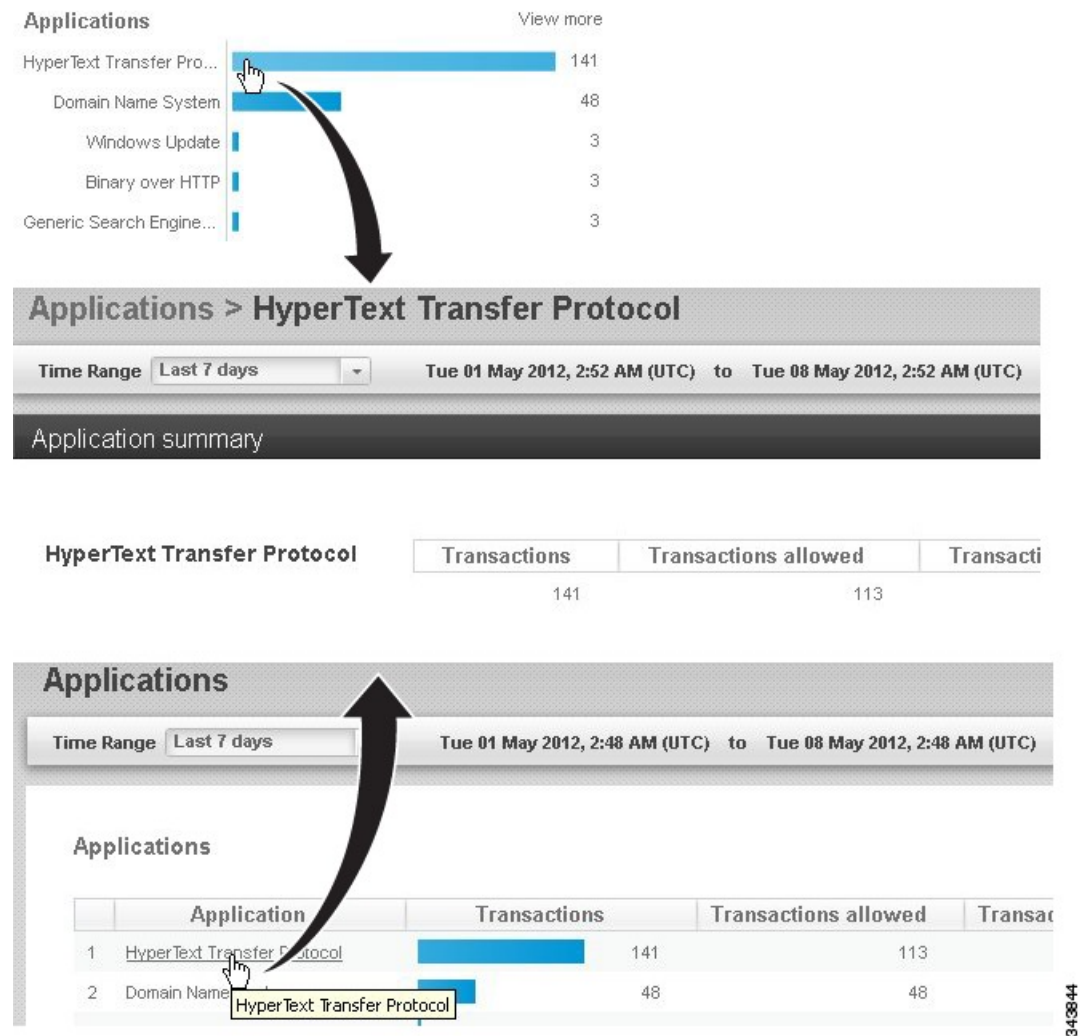
2

Toggle between showing data in raw values and as a percentage of overall traffic volume.

You can also get to a detail dashboard on a specific item by clicking the item in the top five dashboard or in a summary dashboard. As shown in the following illustration, clicking Hypertext Transfer Protocol in either

the top five applications dashboard or the applications summary dashboard takes you to the applications detail dashboard for HTTP.

Figure 10: Going from top five dashboard or summary dashboard to detail dashboard

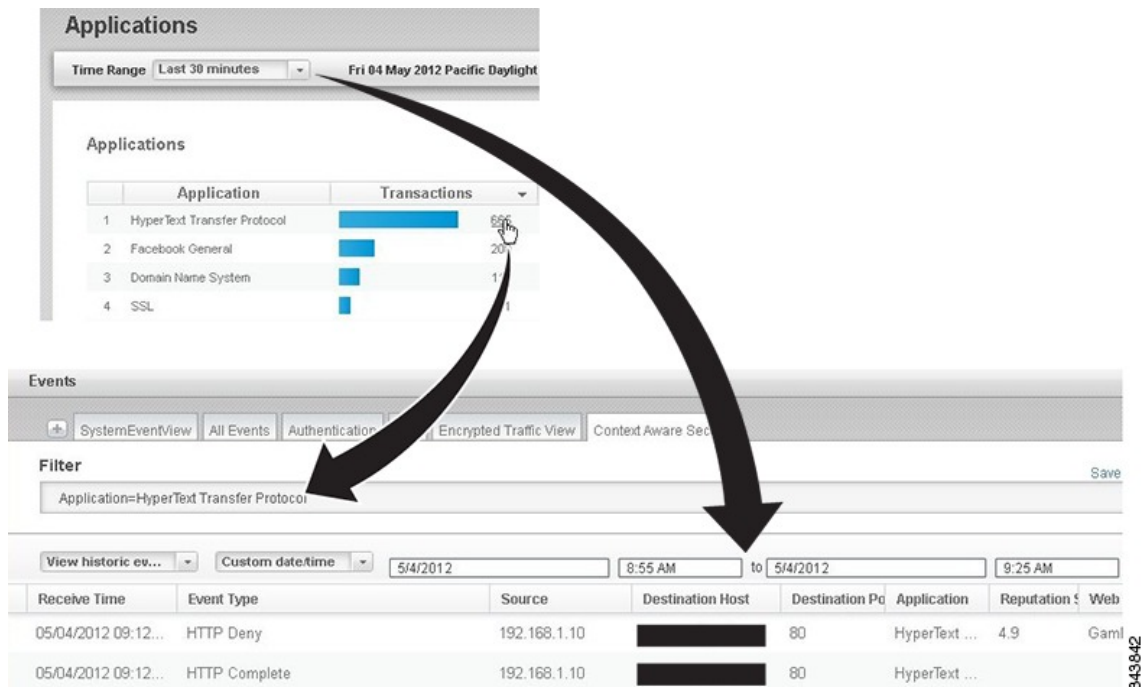


You can also go from a summary dashboard to Event Viewer to see the events that were used to collect the data by clicking the transactions count. Event Viewer is automatically filtered based on the dashboard item and the time range selected for the dashboard, as shown in the following illustration.

**Note**

The number of events shown can differ from the transaction count, especially for queries of older time periods, because events are removed from storage as disk space is depleted and new events arrive. Queries of time periods over 30 days ago might return no matching events. Conversely, you might see more events than transactions, if the item was not one of the top N in each 5 minute bucket covered by the time range, because transaction counts do not include these periods.

Figure 11: Going from summary dashboard to Event Viewer through transactions link



Changing the Dashboard Time Range

When you view a dashboard, you can change the time range that defines the information to include in the dashboard using the Time Range list. The time range list is at the top of each dashboard, and allows you to select predefined time ranges, such as the last hour or week, or to define a custom time range with specific start and end times. The time range you select is carried over to any other dashboard that you view until you change the selection.

Dashboards automatically update every 10 minutes.

**Note**

The time is based on the time zone defined on the device, not the zone configured on your workstation.

The following table explains the time range options.

Table 4: Time Ranges for Dashboards

Time Range	Data Returned In
Last 30 minutes	Thirty (30) complete minutes in 5 minute intervals, plus up to 5 additional minutes.
Last Hour	Sixty (60) complete minutes in 5 minute intervals, plus up to 5 additional minutes.
Last 24 Hours	One hour intervals for the last 24 hours rounded to the previous hour boundary. For example, if the current time is 13:45, the Last 24 Hour period is from 13:00 yesterday to 13:00 today.
Last 7 Days	One hour intervals for the last 7 days rounded to the previous hour boundary.
Last 30 Days	One day intervals for the last 30 days starting from the previous midnight.
Custom Range	The time range you define. Edit boxes are displayed for start date, start time, end date, and end time; click in each box and select the desired value. Click Apply to update the dashboard when you are finished. When constructing a custom time range, you should align your range with the availability of data buckets. For ranges 7-31 days in the past, align your query on the hour. For older ranges, align them on the day; for ranges over a year, align them on the week. In all cases, use UTC time to determine the day boundaries; the time zone of the query, server, and client do not relate to the data bucket. For example, if the time zone is Pacific Daylight Time (PDT), and you are querying data from 40 days ago, use 4PM on day 1 and 4PM on day 2 to align with UTC (8 hour offset to PDT).

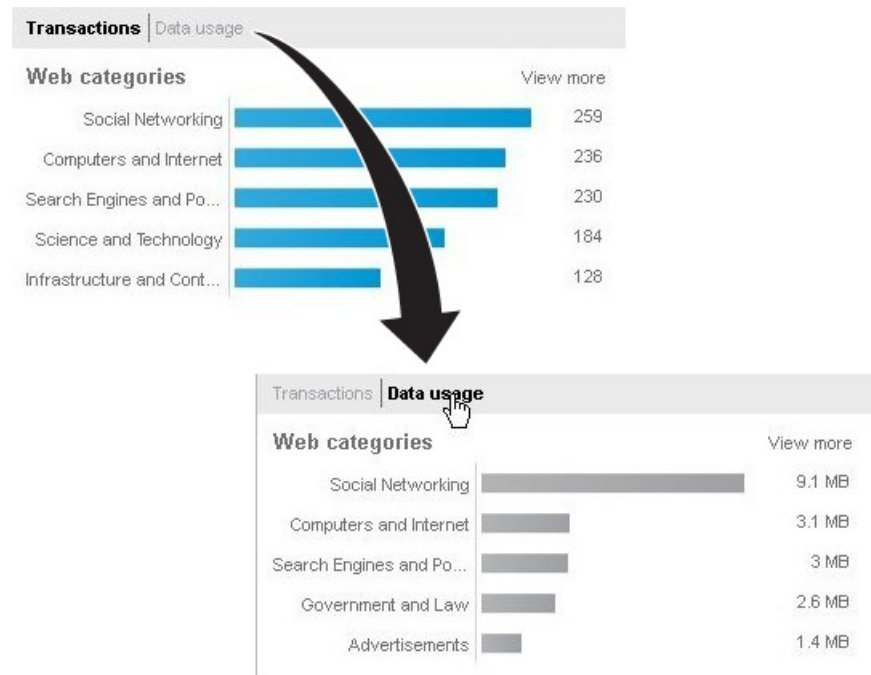
Controlling the Data Displayed in Dashboards

Overview and detail dashboards include several subordinate dashboards such as Top Sources and Top Destinations. Each dashboard panel includes controls that let you view different aspects of the data. You can use the following controls.

Transactions or Threats, Data Usage

Click these links to view charts based on the number of transactions or the amount of data in the transactions. For Next Generation IPS dashboards, **Transactions** is replaced by **Threats**, which is hit counts for those threats you are monitoring. A single transaction can match more than one threat, so the threat count can be higher than the count of matching transactions.

Figure 12: Toggling between transactions and data usage



343841

All, Denied, Allowed

The unlabeled drop-down list in the upper right of each dashboard includes these options. Use them to change whether you see denied connections only, allowed connections only, or all connections whether denied or allowed.

For Next Generation IPS dashboards, these numbers are hit counts for those threats you are monitoring, and the data usage for transactions related to those hits.

For ASA dashboards, these options are available only if you define the PRSM server as a syslog server for the ASA.

Figure 13: Toggling between all transactions and denied transactions (denied site names have been blanked out)



343839

View More

Click the View More link to go to the dashboard for the item you are viewing. For example, clicking **View More** in the Web Destinations chart of the Top Destinations dashboard takes you to the Web Destinations dashboard. If you are viewing the dashboard in a detailed dashboard, you go to the detailed Web Destinations dashboard for the item you are viewing details about.

Dashboard Columns

Dashboards typically contain one or more tables to present information in addition to the information displayed in graphical format.

- The meaning of many columns is modified by the dashboard in which they are included. For example, the transactions column shows the number of transactions for the type of item reported on, such as reputation. You can also toggle the values between raw numbers and as a percentage of the total reported raw values for the item.

- You can change the sort order of the columns by clicking the column heading.

The following table explains all of the columns that you can find in the various dashboards. The standard columns are in all dashboards, the variable columns appear in the dashboards for those items only.

PDF reports include many of the same columns.

Table 5: Dashboard Columns

Column	Description
Standard Columns	
Transactions	The total number of transactions for the reported item. In top-level dashboards, the number is a link; click it to open the Event Viewer with the events table filtered based on the item you are viewing. The number of events shown can differ from the transaction count, especially for queries of older time periods, because events are removed from storage as disk space is depleted and new events arrive. Queries of time periods over 30 days ago might return no matching events. Conversely, you might see more events than transactions, if the item was not one of the top N in each 5 minute bucket covered by the time range, because transaction counts do not include these periods.
Transactions allowed	The number of transactions that were allowed for the reported item.
Transactions denied	The number of transactions that were blocked (based on policy) for the reported item.
Data Usage	The sum of bytes sent and received for the reported item.
Bytes sent	The number of bytes sent for the reported item.
Bytes received	The number of bytes received for the reported item.
Variable Columns	
Application	The name of the application in the transaction as determined by the AVC engine.
Application type	The name of the application type for the application used in the transaction as determined by the AVC engine.
Attacker	The traffic source of a transaction that matches a Next Generation IPS threat.
Device Name	(Multiple Device mode.) The name or IP address of a managed device. If you deleted the device from the inventory, the name is appended with "- DELETED."
Domain name	The DNS name or IP address of the web site involved in the transaction.
Policy name	The name of the context-aware access policy that matched the transaction. If you deleted the policy, the name is appended with "- DELETED."

Column	Description
Target	The traffic destination of a transaction that matches a Next Generation IPS threat.
Theat	The name of the Next Generation IPS threat that matches the transaction.
User device	The name of the operating system or device used by the remote access VPN client making the transaction.
User name	The user ID of the user making the transaction. Usernames are in the format Realm\username. Users who fail active authentication are represented in user dashboards under the username <i>Realm\ANONYMOUS</i> , unless you enabled guest access, in which case the username is Guest. Users who simply do not have a mapping because they were not required to authenticate are shown as their IP address.
Web category	The name of the web (URL) category. Information for a category is the summary for all URLs that fall within the category.

Creating Reports

You can create reports to capture a snapshot of the data displayed in the dashboards. The following topics explain reports.

Generating Reports

You can generate reports to capture a snapshot of the data displayed in the dashboards. Reports are in PDF format, so you must have Adobe Acrobat Reader to view them.

Procedure

-
- Step 1** Select any dashboard from the **Dashboard** menu.
 - Step 2** Click **Generate Report** on the far right side of the dashboard title line.
 - Step 3** Select the type of report you want and the desired time range.
You can also upload a logo to use in the report. For detailed information on report properties, see [Report Properties](#), on page 171.
 - Step 4** Click **Generate**.
The system opens the report when it is ready.
-

Report Properties

To generate a report, you must configure the following properties. After selecting the desired properties, click **Generate**.

Report Type

Which report you want to generate. For detailed information, see [Report Types](#), on page 172.

Time Range

The range that defines which data should appear in the report. You can select the past 30 minutes, 1 hour, 24 hours, 7 days, or 30 days, or you can select **Custom** and select a start and end date in the displayed boxes.

Report Logo

Click **Upload Logo** to add your own organization's logo. The page explains the image limits.

Report Types

You can generate the following types of report. For each report:

- Transaction data shows the total number of transactions, the number that were allowed, and the number that were denied.
- Byte data shows transactions based on the total bytes in the transaction, and also shows the number of bytes for allowed transactions and the number for denied transactions.
- The “Top 5 by transactions” columns include both the item name (for example, user or web category) and the number of transactions for that item.

The following report types are available:

Administrative Report

Includes the following tables and charts:

- Policy changes, showing change history information. Each row indicates the user who made the change, the policy name, the ticket number, the date/time, the devices changed, and the change details, including the field changed, type of change (action), and the old and new data. The “old” column is blank for new items, the “new” column is blank for deleted items.
- Top policy hits by transactions, including the top users, web categories, and application types for each access policy.
- Traffic totals by transactions and data, showing the breakdown between local users and remote access VPN users on the network.

Application and Web Destination Analysis Report

Includes the following tables:

- Top applications by transactions, including the top users and web destinations for each application.
- Top web destinations by transactions, including the top users, devices, and web categories for each web destination.
- Top application types by transactions, including the top applications and users for each application type.
- Top web categories by transactions, including the top users and web destinations for each web category.

Threat Analysis Report

Includes the following tables:

- Top threats by transactions, including the average threat score and top attackers, targets, and access policies hit for each Next Generation IPS threat.
- Top attackers by transactions, including the top threats generated by each attacker, their targets, and the access policies most hit by the traffic.
- Top targets by transactions, including the top threats, attackers, and policies hit.
- Top policies detecting maximum threats by transactions, including the top threats, attackers, and targets.

User and Device Analysis Report

Includes the following tables:

- Top users by transactions, including the top applications, web categories, and user devices per user.
- Top user devices by transactions.

Interpreting the Network Overview Dashboard

The network overview shows summary information about the traffic in the network and the health and performance of the device. In Multiple Device mode, health and performance information is available for all managed devices, including the ASA and its ASA CX; in Single Device mode, information is available for the CX device only.

To view the network overview, select **Dashboard > Network Overview**.

You can toggle the various dashboards between transaction and data usage views, and filter on all, denied, or allowed transactions. You can click on many items, including names, icons, and View More links, to get more detailed information about individual items or about the monitored category as a whole. In Multiple Device mode, statistics are a summary of all managed devices. Use this information to help identify areas that need deeper analysis, or to verify that the network is behaving within general expectations.

The following dashboards are available on the network overview dashboard and drill-down reports:

- On-box summary, device summary—Information about the device (in Single Device mode) or managed devices (in Multiple Device mode). For more information, see [Monitoring Health and Performance](#), on page 174 and [Resolving Device Alerts](#), on page 176.
- Health and Performance—Information about CPU and memory usage. For more information, see [Monitoring Health and Performance](#), on page 174.
- Malicious transactions—The transactions detected with sites of low web reputation, -6 or below, compared to total transactions handled. For the detected malicious transactions, you are also shown the number that was allowed. Click **View More** to open the Malware Traffic dashboard and see [Interpreting the Malware Traffic Dashboard](#), on page 179.
- CX IPS Threats—A pie chart that provides a big picture view of the number of matches to monitored Next Generation IPS threats, by the number allowed verses blocked. You can toggle the view to data usage, which shows bytes sent and received. Click **View More** to open the NG Intrusion Prevention dashboard and see [Interpreting the NG Intrusion Prevention Dashboard](#), on page 180.
- Top policies—The access policies that matched the most traffic flows, by transactions or data usage.
- Top Sources—Information about the users, and if applicable, their remote access VPN user devices, who generated the most traffic, by transactions or data usage.
- Top CX—(Multiple Device mode only.) The CX devices that processed the most traffic by transactions or data usage.
- Traffic by location—A pie chart that shows the relationship between local (non-VPN) and remote access VPN connections, by transactions or data usage.
- Top destinations—Information about characteristics of the traffic destinations or applications, by transactions or data usage.
- Top cloud service applications—Information about applications that are tagged as cloud-based applications, by transactions or data usage.

Monitoring Health and Performance

You can use the network overview dashboard to view basic system health and performance information for a device. In Multiple Device mode, you can also use the devices dashboard.

The following features are available for health and performance monitoring:

On-Box Summary, Network Overview (Single Device mode only.)

Summary information about the CX device you are logged into, including any alerts that need to be addressed. The summary includes the following information:

- The list on the left shows the software version running on the device, the device model, and the last deployed date, which is the last time configuration changes were committed to the device.
- The chart and table on the right shows the amount of network activity passing through the system; use the links above the graph to toggle between transactions (raw number of connections) and throughput (data rate). Use the drop-down list to view denied, allowed, or all transactions. Mouse over the graph to see the time and value of specific data points.

Device Summary, Network Overview (Multiple Device mode only.)

Summary information about each ASA and CX device you are managing using this PRSM server. The ASA|CX icon is a toggle; click each side of the toggle to switch the data display between the ASA and the CX contained in it. Use the device name column to verify which device you are looking at.

The summary includes the following for each device:

- Alerts about current problems with the device, if any. If there is more than one alert, a summary count is shown instead of the specific alert; click the link to get to the detailed dashboard, which will list all the alerts. For more information on alerts, see [Resolving Device Alerts, on page 176](#).
- Current CPU and memory usage, and data throughput, for the device, including minimum, maximum, and average metrics.
- If you are managing more devices than fit into the summary, click **View More** to see the complete list.

Health and Performance, Network Overview and Device Detail

Separate charts for aggregate CPU and memory utilization, which provide insight into the load on the device. The charts differ based on operational mode:

Single Device mode

Mouse over the line to see the specific time and value of the data points in the chart. If a data point was not available, you will see gaps in the line. If the utilization is over 85%, it is marked as being high.

Multiple Device mode

The bar chart shows the number of devices that fit into pre-defined usage ranges. Click a range to see the device dashboard for the devices that fit into the range. If a single device is in the range, you are taken directly to the detail dashboard for the device. If there is more than one, you see the list of devices in the range, click a device to see details.

In the device details view, there are separate lines for the ASA and the CX; you can add or remove lines by clicking the device types in the legend. Mouse over the lines to see the specific time and value of the data points in the chart. If a data point was not available, you will see gaps in the line. If the utilization is over 85%, it is marked as being high. For high availability devices, you can toggle between the active and standby device.

Device Summary, Device Detail Dashboard (Multiple Device mode only.)

Summary information about the managed devices, including any alerts that need to be addressed. The summary includes the following information:

- The list on the left shows the software version running on each device, the device model, and the last deployed date, which is the last time configuration changes were committed to the device. There is also a graphical display of the network interfaces available on the device and their current status: red means down, green means up and functional, no color indicates that the interface is not configured. Click a port to view detailed information about the interface.
- For high availability devices, you can toggle between the active and standby device using the links above the device information.
- The chart and table on the right shows the amount of network activity passing through the system based on transactions/connections (raw number of connections), throughput (data rate), and translates (for the ASA). Use the links above the graph to toggle between the ASA and the CX. Use the drop-down list to view denied, allowed, or all transactions. Mouse over the graph to see the time and value of specific data points.

You can add or remove lines by clicking on **Transactions**, **Connections**, **Translates**, or **Throughput** in the chart legend.

Interfaces Dashboard (Multiple Device mode only.)

The interface dashboard shows detailed information for an interface configured on a device, including VLANs. For CX devices, the interfaces reside on the device hosting the CX device. Use this information to help analyze and troubleshoot interface performance.

To view the interface dashboard, you click on a port icon in the device detail dashboard. To get to the detail dashboard, select **Dashboard > Devices**, then click the name of the device whose interfaces you want to view. You can then click on a configured port; unconfigured ports do not have an interface dashboard available.

The dashboard includes the following main information:

- Traffic Usage chart—Shows traffic rates. Mouse over the lines to see the time and value of specific data points. You can manipulate the chart to show data rates for a specific VLAN, packets per second rates, throughput in bits per second, average packet size in bytes, and the dropped packet count. For packet rates, there are separate lines for input and output, which you can remove by clicking those labels in the legend.
- Troubleshooting chart—Shows various error rates. Mouse over the lines to see the time and value of specific data points. In most charts, you can add or remove lines by clicking the labels in the legend. Click **Refresh** to update the charts with new data. You can manipulate the chart to view packet errors (CRC and frame), buffer resources (overrun and under-run), collision count, and other (broadcast packets).

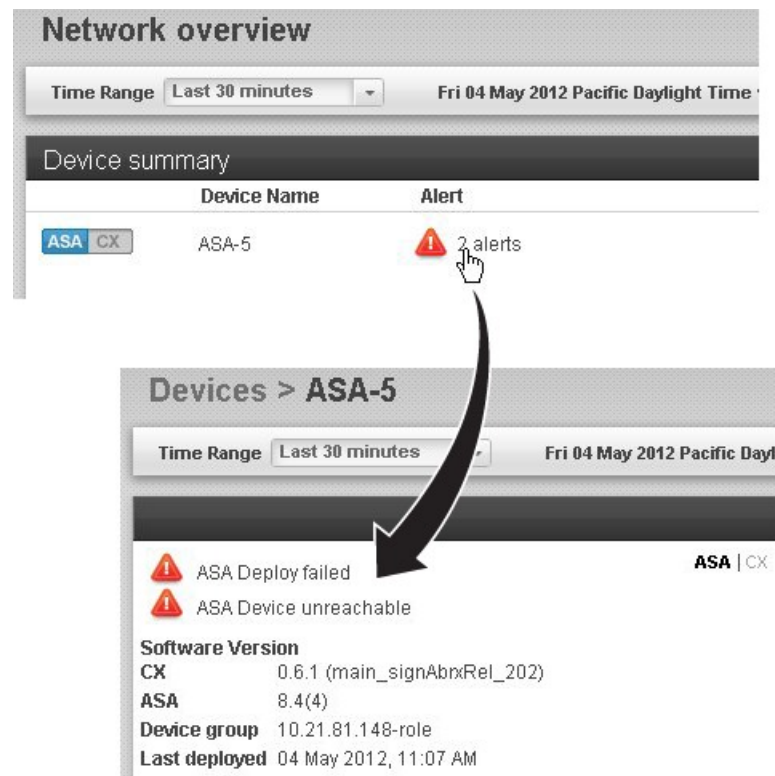
Resolving Device Alerts

The Network Overview displays alerts in the device summary if certain types of problems arise with a device. In Multiple Device mode, these alerts are also visible in the device detail dashboards. Additionally, the device inventory page in Multiple Device mode might display some alerts. Alerts are updated every five minutes.

To see if there are alerts for any managed device, do the following:

- Select **Dashboard > Network Overview** and look at the device summary. In Multiple Device mode, if there are more alerts for a device than can easily be shown, you see a summary of the number of alerts; click the alert summary to view the device detail dashboard, which shows the specific alerts. The illustration below shows this.
- (Multiple Device mode only.) Select **Dashboard > Devices**, then click a device name. Alerts appear in the device detail dashboard only.
- (Multiple Device mode only.) Select **Configurations > Policies/Settings**, switch to Repository view, and open the **Overview** tab. Look for alerts in the inventory table.

Figure 14: Going from summarized alerts to specific alerts



Following is a comprehensive list of the alerts you might see; many of these alerts do not apply to Single Device mode.

CX Config Version Out-dated

The difference between the configuration version running on the CX device differs from the one stored in the PRSM database by too great a degree. This might happen if you recover an old backup, or if many consecutive deployments failed for a long time. If you get this alert, log into the CX home page and select the option to re-synchronize the database on the device with the one in PRSM. If instead you want to preserve the CX configuration as is, you need to delete the device from the PRSM inventory, then add it back to update the PRSM database.

Delete failed

The deletion of this device from the inventory could not be completed. Log into the CX device and click the link to switch to single device mode.

Device Failed Over

The active device in a high availability pair failed and the standby device took over. Evaluate the problems with the failed device and bring it back online.

Device_type Deploy failed

A deployment job for the device failed. To evaluate the problem, select **Administration > Change History** and use the filter controls to get the latest jobs related to the device. If the failure is due to timeout or device unavailable, you should check whether there is a connection problem to the device (see the description for the Device Unavailable alert). Fix any problems you uncover.

To retry the deployment, click the **Changes Pending** link in the menu bar, then select the **Deployment Status** tab. Decide which devices to attempt redeployment, then click the **Redeploy** button.

Device_type Device unreachable

Communication between the PRSM server and the device is failing. There are several possible causes:

- The device is down. Try logging directly into the device to determine if it is functioning correctly. For ASA CX, you can log into the parent ASA and use the following commands:
 - **show module**—The status of the ASA CX module should be Up. The other statuses, Down, Init, or Unresponsive, indicate a problem with the module.
 - **show service-policy**—If you are directing traffic to ASA CX, look for packets coming back from the ASA CX module.
- There is a problem with the network path between the server and the device. Log into the server and use the **ping** and **traceroute** commands to check the connection. Problems can be logical, such as misconfigured routers, or physical, such as disconnected or broken wires.
- The TLS/SSL certificate expired. To retrieve a new certificate, select the device in the inventory list and use the **Refresh Certificate** command.
- You changed the password for the user account specified when adding the device to the inventory. If this is the cause of the problem, update the credentials on the device overview tab.

Discovery failed

This alert appears in the device inventory if you add a device and device configuration discovery failed. Mouse over the device and click **Delete Device**. Check the state of the device, including network connectivity, and try again.

Discovery in progress

This alert appears in the device inventory if you add a device and PRSM is in the process of discovering its configuration. Wait until discovery is completed before trying to deploy changes to the device.

Interface *interface_name* down

The indicated interfaces are down. This situation could be intentional or it could indicate a problem. To determine if an interface is administratively down, go to the device detail dashboard (click the device name from the Network Overview), then click the red interface to open the interface dashboard. If the alert indicates that the administrator shut down the interface, then the condition is intentional. Otherwise, log into the ASA and evaluate the problem. Keep in mind that the problem could be physical, for example, a removed or broken network cable.

N license expired

The indicated number of licenses expired. You need to upload a new license and apply it to the device to ensure uninterrupted service. To upload and apply licenses, select **Administration > Licenses**.

N license expiring in *nn* days

The indicated number of licenses are expiring in the indicated number of days. You need to ensure that new licenses are available in a timely fashion to ensure uninterrupted service.

No Events Processed

The system is not receiving events from the device. This might be reasonable if the device is not processing traffic, or in the case of ASA, if you have not configured PRSM as a syslog server for the ASA. If you should be getting events from the device:

- CX Device—Log into the CLI and use **show services status** to verify that processes are functioning normally. Try stopping and starting processes, or as a last resort, reboot the system.
- ASA—Verify that you have configured PRSM as a syslog server with the correct ports and settings, and that the ASA is functioning normally.

PRSM-CX Version mismatch

These alerts indicate that a managed CX device is running a different configuration than the one defined in the PRSM database. You must correct the mismatch. Either log into each CX home page and click the resynchronize link to revert to the old configuration, or remove the device from the inventory and rediscover it to preserve the current configuration.

Interpreting the Malware Traffic Dashboard

The malware traffic dashboard shows the results of web reputation filtering.

To view the dashboard, select **Dashboard > Malware Traffic**. You can also view the dashboard by clicking **View All** in the Malicious Transactions dashboard on the network overview.

The malware traffic dashboard shows the transactions detected with sites of low web reputation, -6 or below, compared to total transactions handled. For the detected malicious transactions, you are also shown the number that was allowed. The number of allowed transactions can be non-zero for any of the following reasons:

- You have not enabled web reputation services.
- There are some access policies without web reputation profiles.
- You are using web reputation profiles that allow traffic for reputations lower than -6. This dashboard always uses -6 as the cutoff for low reputation metrics.

To see events for allowed traffic, open the Event Viewer and use the following query elements:

- Reputation Score<-5.9
- Event Type=HTTP Complete
- Event Type=TLS Complete



Tip

To look up the reputation of a site, select **Components > Web Filtering Categories**, then select **I want to > Look up web reputation score**.

You can click on View More links and on some names and icons to get more detailed information about individual items or about the monitored category as a whole. In Multiple Device mode, statistics are a summary of all managed devices. Use this information to help identify areas that need deeper analysis or changes to existing policies, or to verify that reputation filtering is performing within general expectations.

The dashboard also shows the malware types detected in reputation filtering. Potential malware types include the following:

- Adware
- Conficker
- Not Malicious. Although the reputation score is low, the traffic is not considered malicious.
- Related to Phishing
- Related to Spam
- Spyware
- Suspected Malware
- Trojan

Interpreting the NG Intrusion Prevention Dashboard

The NG intrusion prevention dashboard shows the results of Next Generation IPS filtering. The dashboard will show data only if you enable IPS filtering and apply an NG IPS profile to one or more access policy.

To view the dashboard, select **Dashboard > NG Intrusion Prevention**.

The Dashboard includes several graphs to show the top policies that detected threats, the top attackers and their targets, and the threats encountered. In Multiple Device mode, statistics are a summary of all managed devices and you also see the top devices encountering these threats.

The metrics used in Next Generation IPS dashboards differ slightly from the other reports. Rather than showing transactions, these dashboards show hits for those threats you are monitoring. Because a single transaction can match more than one threat, the threat count need not equal the transaction count; it might be greater than the number of transactions.

You can toggle the various dashboards between monitored threat hits and data usage views, and filter on all, denied, or allowed threats. Click **View More** in any graph to see a complete report on that metric. From these reports you can drill down to detailed information on a specific report item.

The following dashboards are available on the NG intrusion prevention dashboard and drill-down reports:

- CX IPS Threats pie chart—This dashboard is also available on the network overview. It provides a big picture view of the number of transactions that match Next Generation IPS threats, by the number allowed or blocked. You can toggle the view to data usage, which shows bytes sent and received.
- Policies detecting maximum threats—The name of the policies these transactions matched.
- Top Attackers—The traffic source for these transactions.
- Top Victims—The traffic destination for these transactions.
- Top Threats—The most frequently encountered threats by name.

Interpreting the ASA Traffic Dashboard

(Multiple Device mode only.) The ASA traffic dashboard shows connection statistics from ASA devices. The dashboard will show data from a device only if you define the PRSM server as a syslog server for the device. In addition, statistics are not shown for an ASA that is configured in multiple-context mode, that is running an unsupported software version, or that is running in failover mode. Statistics are derived from syslog messages 302013, 302015, and 106023.

To view the dashboard, select **Dashboard > ASA Traffic**. You can also see the information in the device detail dashboards.

The Top ASA Traffic dashboard includes several graphs to show the top sources, destinations, and services. This dashboard is also available on other dashboards such as the device details.

You can toggle the various dashboards between connections and data usage views, and filter on all, denied, or allowed transactions. Click **View More** in any graph to see a complete report on that metric. From these reports you can drill down to detailed information on a specific report item.



Tip

Keep in mind that the Allowed connection statistics are based on the initial application of ASA firewall rules prior to redirecting traffic to CX. Thus, “allowed” connections might have subsequently been denied by CX policies. Also, the options to view data based on allowed or denied connections are available only if you define the PRSM server as a syslog server for the ASA.



Viewing Events

Use the Event Viewer to monitor and examine events from the devices you are managing. Events are organized into views that you can filter or search to find events that interest you. You can create customized views and filters to fit your needs or use the predefined views included in the application.

- [Overview of Event Viewer, page 183](#)
- [Using Event Views, page 187](#)
- [Configuring Syslog, page 192](#)
- [Event Messages, page 196](#)

Overview of Event Viewer

Use Event Viewer to view events collected from monitored devices:

- **Multiple Device mode**—Events are collected from all managed CX and ASA devices. For ASA, you must define the PRSM server as a syslog server to see events from the device. Managed CX devices automatically redirect events to the server.
- **Single Device mode**—When you are logged into an unmanaged CX device, you can see events from that device only.

As the storage area for event and report data is filled, the system automatically deletes older data to make room for new data. Thus, the amount of historical data available depends on the event rate and storage capacity of the system.

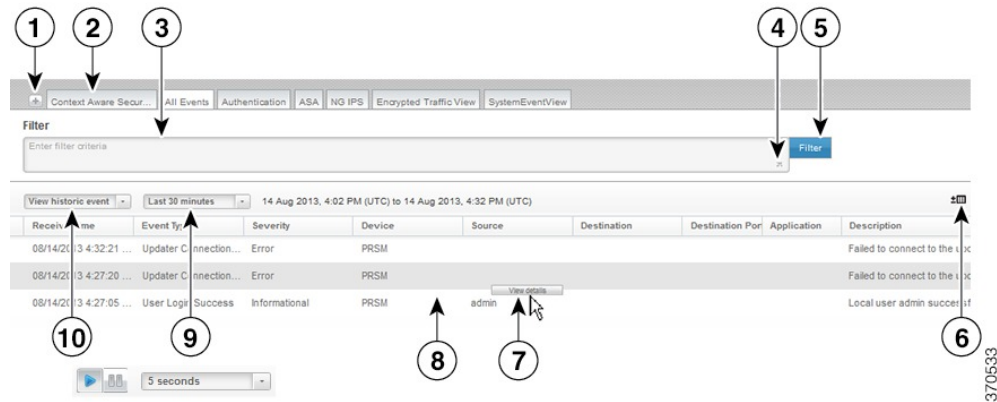


Tip

Event Viewer is useful for operational monitoring and troubleshooting of the managed devices. Event Viewer does not provide extensive event correlation, compliance reporting, long term forensics, or the integrated monitoring of both Cisco and non-Cisco devices.

Select **Events** > **Events** to open Event Viewer.

Figure 15: Event Viewer



1	Add view (+) button.	6	Add/Change columns button.
2	View tabs.	7	View Details button (mouse-over).
3	Event filter.	8	Events table.
4	Clear Filter (X) button.	9	Time range (historical); Play/Pause and refresh rate (real-time).
5	Filter button.	10	View type (historical, real-time).

The Event Viewer window includes the following items:

View Tabs

Each tab represents a different view, including the pre-defined views that come with the application and any custom views you created yourself. You can create custom views so that the table includes the columns you are most interested in, if the pre-defined views do not fit your needs.

Click the + button on the left to create a new view based on the general characteristics of the one you are currently viewing. For example, if the active view is System Events, your new view will show system events only. A new view is automatically created if you change the column selection while using a pre-defined view. To rename the view, click the tab name, type in the new name, and press Enter.

If there are more views than can be displayed in the tab area, the last tab on the right is **More**; click the tab to select one of the hidden views.

Click the **X** button in a tab to delete the view. You cannot delete any of the pre-defined views.

For more information about the pre-defined views and how to create, edit, or delete custom views, see:

- [Using Event Views, on page 187](#)
- [Configuring Custom Views, on page 187](#)

Filter

Use this field to create filters based on event attributes.

You can build a filter expression by:

- Clicking a cell that contains the value on which you want to filter.
- Selecting the atomic element from the drop-down list and typing in the value. The element includes an operator that defines the relationship with the value: = (equals), > (greater than), or < (less than). You can type in != to create a not-equals relationship.

If you include multiple elements in the filter, there is an AND relationship among elements of different types and an OR relationship among elements of the same type. For example, "Source=10.100.10.10 Source=10.100.10.11 Destination Port=80" is interpreted as "(Source=10.100.10.10 OR Source=10.100.10.11) AND Destination Port=80."

For more information on event filters, see [Filtering Events, on page 188](#) and [Event Filter Rules, on page 189](#).

To the right of the filter edit box are the following controls:

- **Filter** button—Click this button to apply the filter to the table. Simply building the filter expression, or deleting it, does not apply it to the events table. If the view is currently a paused real time view, the mode is automatically changed to play.
- **X**—Click this character in the far right of the **Filter** field to clear all elements in the filter.

If you want delete just one of several elements in a filter, mouse over the element and click the **X** for that element.

View Type and Time Controls

Above the events table are two or three unlabeled controls that define the time range of the events shown in the table. The second or third control changes purpose based on the selection in the first control. From left to right:

- **View Type**—Whether you are viewing events that occurred during a past time period (**View Historic Events**) or you want to view events as they occur (**Real Time Eventing**).
- **Time Period**—(Historic views.) The time window for the events. Most options are from the current time into the past; these views are refreshed to show new events that fit into the window. You can view events from the past 30 minutes, 1 hour, 4 hours, 12 hours, or 24 hours. The time is based on the time zone defined on the device, not the zone configured on your workstation.



Note You can also select **Custom Date/Time** and specify the exact starting and ending date and time that you want to view. Edit boxes are displayed for start date, start time, end date, and end time; click in each box and select the desired value. Click **Apply** to update the table when you are finished.

- **Play/Pause buttons**—(Real time views.) An additional control is inserted between the drop-down list controls when you are using real time viewing. Use the **Play** (arrow) and **Pause** (double hash) buttons to start and stop event table updates. You need to pause the view if you see an event that you want analyze; otherwise, the event will quickly get away from you as new events are added to the table.
- **Refresh Rate**—(Real time views.) The rate at which the events table updates. You can refresh the table every 5, 10, 20, or 60 seconds.

Events Table

The events received from monitored devices appear in the table, new events being added to the top of the table. You can do the following actions with the events table.

- To change the columns displayed, or their order, click the **Add/Remove Columns** icon button above the table to the right. The Customize Columns window includes two lists: available but unused columns on the left, selected columns on the right. Click and drag columns between the lists to add or remove them. To change their order, click and drag columns in the selected list to the desired location.

Click **OK** when finished.

If you make any changes to a pre-defined view, a new custom view is created. Rename the view as desired. Any changes to a custom view simply update the view.

- To change the width of a column, click and drag the column heading divider to the desired width.
- To view detailed information about an event, mouse over the event and click the **View Details** button that appears. A details window opens to show event information, including the policies related to an event, if any. If you have the appropriate privileges, you can edit the policy from the details window. Click the **Close** link to close the window and return to the events table.

Using Event Views

When you view events in Event Viewer, you open a view. A *view* defines a set of columns, including their arrangement and width. Views help organize the events list so that you can more easily find what you are looking for.

To open a view, click the view's tab. If the view you are looking for is not visible, click the **More** tab and select the view from the list of hidden views. (Select **Events** > **Events** to open Event Viewer.)

Event Viewer includes a number of predefined views:

- **All Events**—In Single Device mode, shows all events for the device. In Multiple Device mode, shows all events from all monitored ASA and managed CX devices.
- **ASA**—(Multiple Device mode only.) Shows all events from all monitored ASA devices.
- **Authentication**—Shows Context-Aware Security authentication events.
- **Context Aware Security**—Shows all events from CX devices.
- **Encrypted Traffic View**—Shows encrypted traffic events, which are related to Context-Aware Security decryption policies.
- **System Event View**—Shows all system events, such as signature updates.
- **NG IPS**—Shows events for potential threats as identified by the Next Generation IPS service.

In addition to the pre-defined views, you can create custom views.

Configuring Custom Views

You can create your own custom views so that you can easily see the columns you want when viewing events. You can also edit or delete custom views, although you cannot edit or delete the pre-defined views.



Tip

The base characteristics of a new view are defined by whichever view you were looking at when you created the new view. For example, if you create a view while looking at the System Events view, the new view will show system events only. Thus, ensure that you select a view that shows the appropriate event types.

Procedure

Step 1 Select **Events** > **Events** to open Event Viewer.

Step 2 Do one of the following:

- To create a new view based on an existing pre-defined view, click the tab for the pre-defined view. For example, if you want a view that shows Context-Aware Security traffic events only, select the predefined Context Aware Security view.
- To create a new view based on an existing custom (or pre-defined) view, click the tab for the view, then click the + button to the left of the view tabs. A new view is created with the new tab name highlighted; type in the desired view name.

- To edit an existing custom view, click the tab for the view.

Note To delete a custom view, simply click the **X** button in the view's tab. You cannot undo a delete.

Step 3 Click the **Add/Remove Columns** icon button above the events table on the right, and select or deselect columns until the selected list includes only those columns to include in the view. Click and drag columns between the available (but not used) and selected lists. You can also click and drag columns in the selected list to change the left-to-right order of the columns in the table.

When finished, click **OK** to save your column changes.

Note If you change column selection while viewing a pre-defined view, a new view is created. Click the name in the tab and type in the desired view name.

Step 4 If necessary, change column widths by clicking and dragging the column separators.

Switching Between Real Time and Historical Views

With Event Viewer, you can either watch events as they happen or view an historical time range when analyzing events. Event Viewer shows the current date and time range for the events shown in the table.

You can switch any view between real time and historical using the unnamed **View Type** control above the events table on the far left. The options are:

Real Time Eventing

To view events in real time as they happen. Select the refresh rate for updating the table with new events in 5, 10, 20, or 60 second intervals.

Use the **Play** (arrow) and **Pause** (double hash) buttons to start and stop event table updates. Pause the view when you want to analyze a particular event.

View Historic Events

To view events in a previous time period. Select the time window for the events. Most options are from the current time into the past; these views are refreshed to show new events that fit into the window. You can view events from the past 30 minutes, 1 hour, 4 hours, 12 hours, or 24 hours. The time is based on the time zone defined on the device, not the zone configured on your workstation.

You can also select **Custom Date/Time** and specify the exact starting and ending date and time that you want to view. Edit boxes are displayed for start date, start time, end date, and end time; click in each box and select the desired value. Click **Apply** to update the table when you are finished.

Filtering Events

You can create filters to limit the events listed in the events table based on various event attributes. Filters apply within the scope of the time range. That is, the events shown are limited to those within the selected historical time range or real time.

Procedure

-
- Step 1** Select **Events > Events** to open Event Viewer.
- Step 2** Click the view tab to select the desired view.
- Step 3** Create a filter in the **Filter** field.
 To create a new filter, either manually type in the filter by selecting atomic elements from the drop-down list and entering the filter value, or build a filter by clicking a cell in the events table that includes a value on which you want to filter. You can click multiple cells in the same column to create an OR condition among the values, or click cells in different columns to create an AND condition among the columns. If you build the filter by clicking cells, you can also edit the resulting filter to fine-tune it. For detailed information about creating filter rules, see [Event Filter Rules, on page 189](#).
- Step 4** Do any of the following:
- To apply the filter and update the table to show only those events that match the filter, click the **Filter** button.
 - To clear an entire filter that you have applied and return the table to a non-filtered state, click the **X** button in the far right of the **Filter** box.
 - To clear one of the atomic elements of a filter, mouse over the element and click the **X** for the element. Then, click the **Filter** button.
-

Event Filter Rules

You can create complex filters to limit the events table to the events that currently interest you. You can use the following techniques, alone or in combination, to build a filter:

Clicking columns

The easiest way to build a filter is to click on cells in the events table that contain the values on which you intend to filter. Clicking a cell updates the **Filter** field with a correctly-formulated rule for that value and field combination. However, using this technique requires that the existing list of events contains the desired values.

You cannot filter on all columns. If you can filter on the contents of a cell, it is underlined when you mouse over it.

Selecting atomic elements

You can also build a filter by clicking in the **Filter** field and selecting the desired atomic element from the drop-down list, then typing in the match value. These elements include event fields that are not available as columns in the events table. They also include operators to define the relationship between the value you type in and the events to display. Whereas clicking columns always results in an “equals (=)” filter, when you select an element, you can also select “greater than (>)” or “less than (<)” for numeric fields.

Regardless of how you add an element to the **Filter** field, you can type into the field to adjust the operator or value.

Operators for Event Filters

You can use the following operators in an event filter:

=	Equals. The event matches the specified value. You cannot use wildcards.
!=	Not equals. The event does not match the specified value. You must type in the ! (exclamation point) to build a not-equals expression.
>	Greater than. The event contains a value that is greater than the specified value. This operator is available for numeric values only, such as port and IP address.
<	Less than. The event contains a value that is less than the specified value. This operator is available for numeric values only.

Rules for Complex Event Filters

When building a complex filter that contains more than one atomic element, keep the following rules in mind:

- Elements of the same type have an OR relationship between all values for that type. For example, including Source=10.100.10.10 and Source=10.100.10.11 matches events that have either of these addresses as the source.
- Elements of different types have an AND relationship. For example, including Source=10.100.10.10 and Destination Port=80 matches events that have this source address AND destination port only. Events from 10.100.10.10 to a different destination port are not shown.
- Numeric elements, including IPv4 and IPv6 addresses, can specify ranges. For example, you could specify Destination Port=50-80 to capture all traffic for ports within this range. Use a hyphen to separate the start and end numbers. Ranges are not allowed for all numeric fields, for example, you cannot specify an IP address range in the Source element.
- You cannot use wildcards or regular expressions.

Improving Historical Event Filter Performance

When filtering historical views, you can filter on any field in the Event Viewer. However, certain fields are indexed, so searching on those fields instead of unindexed fields can provide better performance. The difference can be profound when filtering a large number of events, cutting minutes from your search.

The following fields are indexed; consider limiting your historical filters to these fields.

- Action
- Application
- Client OS
- Destination Host
- Destination IP
- Destination Port
- Destination Service

- Device
- Event Type
- Identity Source
- Policy Name
- Protocol
- Receive Time
- Reputation Score
- Request MIME File Type
- Response MIME File Type
- Source Host
- Source IP
- Source Port
- Severity
- Threat
- TLS Flow Decrypted
- TLS Protocol Version
- Username

Working with Individual Events

The events list shows a summary of the events that match your time range and filter criteria. When looking at the events summary, you can do the following with individual events.

- Mouse over an event and click the **View Details** button see the full contents of the event as described below.
- Build a filter by clicking on cells in an event. A filter rule is added to the **Filter** field with the contents of the cell used as the filter criteria. Click multiple cells to build a complex filter. You can also edit the contents of the **Filter** field to refine the filter. You must click the **Filter** button to apply the filter to the table.



Tip

If an event is for a device or policy that you have since deleted from the database, the name of the device or policy remains in the event but “Deleted” is added to the device or policy name cell contents.

Viewing Event Details

When you find an event that needs more detailed analysis, mouse over the event and click the **View Details** button that appears. A details window opens to show event information; click the **Close** link to close the window when you are finished.

When open, the event can provide the following information and features:

- Complete details about the event, including information not shown in the table. Even if you do not include a particular column in your view, if the event contains data for an attribute, you can see that information if you open the event.
- The policies, including policy sets, that were involved in this event. For example, if the event was generated by a traffic flow that matched an access policy, the access policy is shown. If you want to make changes to the policy or policy set, mouse over it and click **Edit Policy** or **Edit Policy Set**.
- If the event includes authentication information for CX devices, you can click the realm name to go to the directory realm configuration.

Configuring Syslog

You can configure syslog (system log) settings to forward events from a device to a syslog server. This makes it possible for you to use sophisticated Security Information and Event Management (SIEM) systems to collect and analyze events from a variety of devices in your network.

Configuring syslog servers does not prevent you from seeing events in the PRSM Event Viewer. Events remain available in both Single Device mode and Multiple Device mode.



Note

(Multiple Device mode.) For ASA devices, you must configure the PRSM server as a syslog server to see events from the ASA in the PRSM Event Viewer. All CX devices automatically send their events to PRSM; you need to configure syslog servers only if you want events sent to a separate event management server.

The following topics explain how to configure syslog.

Configuring Syslog Settings for CX Devices

Configure syslog settings for CX devices if you want to export a copy of events to an external syslog server.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and open the **Syslog Settings** tab. If necessary, open the **Syslog Settings** folder.
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Do any of the following:
- Select **CX Syslog Server: Enabled** or **Disabled** to change whether events are sent to an already-configured syslog server. You can disable sending events to a server without removing your settings.
 - Configure a new server by selecting **Enabled** and filling in the server attributes. You can configure up to two syslog servers. The properties are described in [CX Syslog Settings](#), on page 193.
- Step 3** Click **Save**.
-

CX Syslog Settings

Syslog servers used for exporting CX events have the following properties. You must select **Enabled** to see and configure them.

Protocol

The protocol used for transporting events to the server:

- **UDP**—Events are sent without notification that the transmission was successful.
- **TLS over TCP**—Events are sent encrypted with reliable transmission. If failures occur, the transmission is retried, thus increasing the likelihood that the syslog server receives all events. For TLS to work, the device must accept the syslog server's CA certificate, so the device must either already trust the CA authority that issued the certificate, or you must upload the certificate on the supplemental certificates page (**Configurations > Certificates**).
- **Unsecured TCP**—Events are sent unencrypted with reliable transmission. If failures occur, the transmission is retried.

Hostname/IP: Port

The hostname or IP address of the syslog server, and the port on which the server receives events. Default ports are 514 for UDP and Unsecured TCP, and 6514 for TLS over TCP.

If you are using TLS over TCP, you must ensure that the name or address matches one in the certificate that the syslog server presents. If there is a mismatch, a TLS connection cannot be made and events will not be transmitted to the server.

Minimum Severity to Export

The message severity to export to the syslog server. All traffic events are Informational; system events can be Informational or the other levels. In order from least number of messages to most, the levels are Error, Warning, Notification, and Informational. Select Informational to get all events.

Syslog Facility Code

The syslog facility code that the device includes in messages destined for syslog servers. You can select a facility between LOCAL0 and LOCAL7.

Syslog facility is useful when you have a central syslog monitoring system that needs to distinguish among the various network devices that generate syslog data streams. Because your network devices share the eight available facilities, you might need to change this value.

Configuring Logging and Syslog Settings for ASA Devices

(Multiple Device mode only.) You can configure ASA logging settings, and also configure syslog settings if you want to export a copy of system events to an external syslog server. You must configure the PRSM server as a syslog server if you want to see events from the ASA in PRSM.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and open the **Syslog Settings** tab. Open the **ASA Logging Settings** folder.
You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Do any of the following:
- Configure the logging settings as described in [ASA Logging Properties, on page 194](#).
 - Add a syslog server to the logging servers table by clicking the **Add Logging Host (+)** button and filling in the properties described in [ASA Syslog Server Properties, on page 195](#).
 - Select a server in the table and click the **Edit** button to alter its properties.
 - Select a server in the table and click the **Delete** button to remove it.
- Step 3** Click **Save**.
-

ASA Logging Properties

The following logging properties are displayed when you access the Syslog Settings for an ASA device.

Filter on Severity

Choose a message-filtering level from this list to filter syslog messages according to their severity. The level you choose represents the least severe condition to be logged. For example, if you set the severity filter to Error (level 3,) the device will log messages for severity levels 3, 2, 1, and 0. The severity levels are:

- None—No filtering; all messages are sent.
- Emergency (level 0)—System is unusable. Using a severity level of zero is not recommended.
- Alert (level 1)—Immediate action is required.
- Critical (level 2)—Critical conditions exist.
- Error (level 3)—Error conditions exist.
- Warning (level 4)—Warning conditions exist.
- Notification (level 5)—Normal but significant conditions exist.
- Informational (level 6)—Informational messages only.
- Debugging (level 7)—Debugging messages only.

Logging Queue

Specify the number of messages to be queued in the device's syslog buffer before transmission to a syslog server. The default is 512.

Valid values are from 0 to 8192 messages, depending on device. If **Logging Queue** is set to zero, the queue is the maximum configurable size for the device, or 8192 messages.

Logging On/Off

Click to turn logging on the security appliance On or Off.

Send as EMBLEM Format

Turn On or Off EMBLEM formatting of the logged messages. This is the format used by Cisco IOS routers and switches.



Note If you enable EMBLEM formatting, you must use the UDP protocol to publish syslog messages—EMBLEM is not compatible with TCP.

Include debug trace in log

Turn this option On to redirect all debug trace output to the syslog.

Syslog messages do not appear in the console if this option is enabled. Therefore, to see debug messages, you must enable logging at the console and configure it as the destination for the debug syslog message number and logging level. The syslog message number used is 711011. Default logging level for this syslog is **debug**.

Send to standby unit

Use this switch to turn On or Off logging on the failover unit paired with this security appliance.

Allow user traffic when logging host is down

Use this switch to turn On or Off connection blocking to TCP-based syslog servers.

When TCP is the protocol specified for communications with a syslog server, by default the security appliance will drop connections across the firewall if the syslog server is unreachable. Turn this option On to disable connection blocking.

ASA Syslog Server Properties

The following properties are presented when you add or edit a **Logging Host** (syslog server) for an ASA device.

IP Address

Enter the IP address of the syslog server.

EMBLEM On/Off

Turn On if syslog messages will be in Cisco EMBLEM format. If On, the **Protocol** must be **udp**.

Secure On/Off

Turn On if the logging host uses SSL/TLS for TCP connections. (UDP is not supported for secure logging.)

Port

The number of the TCP or UDP port on which the syslog server receives messages. The default port for UDP is 514; the default port for TCP is 1470.

Protocol

The protocol used by this syslog server, either **tcp** or **udp**; **udp** is the default. TCP ports work only with a security appliance syslog server.



Note You must select **udp** if you intend to use the EMBLEM format.

Interface

Specify the device interface used to communicate with this syslog server. Enter or choose the name of an interface or interface role object.

Event Messages

Following are the basic types of messages you might see in Event Viewer:

- Context-Aware Security traffic events—These events relate to traffic flowing through a CX device. The messages are described in [Context-Aware Security Traffic Events](#), on page 196.
- CX device and PRSM system events—These events relate to the operation of the system. You can view these events in the System Event view. The messages are described in [CX Device and PRSM System Events](#), on page 201.
- ASA syslog messages—These events are syslog messages generated by an ASA. For information on the possible messages, see *Cisco ASA Series Syslog Messages* at <http://www.cisco.com/c/en/us/td/docs/security/asa/syslog-guide/syslogs.html>.

For information on the various columns, see [Event Columns](#), on page 214.



Note Unlike the ASA, message numbers for CX/PRSM messages are not inherently meaningful, although you can see the numbers in the Event Type ID column.

Context-Aware Security Traffic Events

The following event messages relate to traffic flowing through a CX device. The list is organized alphabetically based on event name. Unlike ASA syslog messages, the message ID number for Context-Aware Security events is not meaningful, so the number is not listed here.

Authentication Failure

Message: User failed authentication attempt.

Explanation: A user failed to respond with valid credentials when prompted for active authentication. The event details show the username for the failed attempt. Users are prompted to authenticate if a traffic flow matches an identity policy that requires or allows for active authentication and identity information is not already available for the user's IP address.

Recommended Action: This event can occur for completely innocent reasons, such as a user simply mistyping a password.

Authentication failures do not prevent the user from accessing the network by themselves. If the user fails to authenticate correctly, traffic flows from the user will not include identity information, and the flows will never match identity-based criteria in any access policy (that is, identity objects will not be matched). The effect of this failure depends on the access policy set you have configured. If your access policies essentially deny access to unidentified users, authentication failures can have a significant effect on users.

Additionally, the user will be represented by IP address rather than username in dashboards.

If you see a large number of innocent failures, you might consider providing educational information about how to respond to active authentication prompts. If you are using Active Directory, you can also consider implementing transparent authentication or installing the CDA or AD agent to provide less intrusive passive authentication.

Authentication Server Down

Message: Authentication server is down.

Explanation: The system cannot communicate with the indicated server in the indicated directory realm.

Recommended Action: If you do not get an Authentication Server Up message within a reasonable time, evaluate the following potential problems:

- Check whether the server is up and running correctly.
- For Active Directory servers, this message can occur if the system fails to join the AD domain. Try testing AD join by selecting **Components > Directory Realm**. Mouse over the AD realm and click **Edit Realm**, then click the **Test Domain Join** link in the realm properties. If you get a failure message, you need to correct the domain and credentials information and resolve any other issues that prevent domain join.
- Log into the device CLI and use the **ping** and **tracert** commands to verify there is a path to the directory from the device.

Authentication Server Up

Message: Successfully connected to authentication server.

Explanation: The system can communicate with the authentication server. The server and directory realm are indicated in the event message.

Recommended Action: No action required.

Authentication Success

Message: User passed authentication.

Explanation: The user supplied correct credentials during active authentication.

Recommended Action: No action required.

Auth Maximum Retries

Message: This user has reached the maximum number of retries for authentication.

Explanation: The user failed all allowed attempts to provide credentials during active authentication.

Recommended Action: If you see a lot of these events, you might consider increasing the maximum number of authentication retries. Also, review the recommended action for Authentication Failure events for other actions you should consider.

Dropped Event

Message: One or more events were dropped.

Explanation: Events are arriving faster than the system can process. The event indicates the number and type of events that were dropped.

Recommended Action: If the problem is frequent and persistent for a PRSM server, consider increasing the power of the server in terms of memory and processor power. If that is not possible, consider managing fewer devices with the server by installing a second server and moving some devices to the new server's inventory.

Flow Complete

Message: A short-lived flow passed policy constraints and was created and terminated normally.

Explanation: A new connection was created and torn down. Because the connection was short lived, you get this single message rather than a Flow Create event followed by a Flow Tear Down event. For example, DNS look-ups are usually represented with Flow Complete events.

Recommended Action: No action required.

Flow Create

Message: A flow was initiated through the device.

Explanation: A new connection was made, initiating a new traffic flow through the device. You do not get this event for HTTP or TLS/SSL flows, for which you get either HTTP Complete or TLS Complete messages only. There should be a Flow Tear Down or a Flow Deny event that matches the Flow Create event's flow.

Recommended Action: No action required.

Flow Deny

Message: A flow was denied due to policy violation.

Explanation: A traffic flow was dropped because it matched an access policy that applied the Deny action. This message applies to non-HTTP traffic and can also apply to undecrypted HTTPS flows. For HTTP, or decrypted HTTPS, you see an HTTP Deny message instead of Flow Deny.

Recommended Action: No action required unless the flow represents traffic that you want to allow through the device, in which case you need to evaluate your access policies. Open the event details to see the access policy the traffic flow matched. Consider the following possibilities:

- The order of policies in the policy set might need to be changed. The matched policy might need to be moved beneath other Allow policies that the flow should have matched before reaching this Deny policy.
- The traffic matching criteria for the policy might be too broad. Evaluate whether different criteria are needed so that desirable flows do not match the policy.

Flow Tear Down

Message: A flow passed policy constraints and completed normally.

Explanation: A traffic flow has been terminated normally, for example, because the user completed the transaction. Message details include the total bytes for the flow. This message applies to non-HTTP traffic.

Recommended Action: No action required.

HTTP Aborted

Message: An HTTP transaction aborted due to an exception.

Explanation: An unexpected error occurred during HTTP inspection, resulting in a dropped HTTP flow. The drop is not related to your access policies. These messages usually indicate a malformed HTTP packet, or HTTP headers that are excessively long (for example, 16kb). Other possible causes are protocol violations or text that is not a number when a number is expected.

Recommended Action: If you start seeing a lot of HTTP Inspection Aborted events, and they are affecting legitimate traffic, contact the Cisco Technical Assistance Center.

HTTP Complete

Message: An HTTP transaction passed policy constraints and completed normally.

Explanation: The HTTP or decrypted HTTPS traffic flow was allowed by your access policies and it completed successfully.

Recommended Action: No action is required unless the destination web site is one that you intended to block. If the site is one you wanted to block, open the event details to see which policy matched the flow. Consider the following solutions:

- If the traffic matched the wrong policy, look at the order of policies in the policy set. You might need to move this policy below other policies, or move another policy above this one.
- If the traffic matched the correct policy, you can edit the policy to adjust the traffic matching criteria.

HTTP Deny

Message: An HTTP flow was denied due to policy violation.

Explanation: An HTTP traffic flow, or decrypted HTTPS traffic flow, was dropped because it matched an access policy that applied the Deny action.

Recommended Action: No action required unless the flow represents traffic that you want to allow through the device, in which case you need to evaluate your access policies. Open the event details to see the access policy the traffic flow matched. Consider the following possibilities:

- The order of policies in the policy set might need to be changed. The matched policy might need to be moved beneath other Allow policies that the flow should have matched before reaching this Deny policy.
- The traffic matching criteria for the policy might be too broad. Evaluate whether different criteria are needed so that desirable flows do not match the policy.

Packet Deny

Message: A packet has been denied.

Explanation: A packet failed internal security checks. For example, there was an IP checksum failure, an invalid IP or TCP header, or the first TCP packet was not a SYN packet. These security checks are used to prevent spurious traffic. These events are not related to your access policies.

Recommended Action: No action is required unless the events relate to a specific traffic failure you are trying to troubleshoot. If necessary, you can set up global packet capture to capture these dropped packets.

Redirect Authentication

Message: This flow was redirected to be authenticated.

Explanation: The flow matched an identity policy that required or allowed for active authentication, and it was determined that the user needed to be prompted for credentials. You should also see Authentication Failure or Authentication Success events related to this event.

Recommended Action: No action required unless this flow should not have matched an authentication policy that would result in active authentication prompting.

If this flow should not have required authentication, open the event details to see which identity policy the flow matched. Evaluate whether the policy needs to be moved up or down in the policy set or if you need to adjust the traffic matching criteria.

TLS Abort

Message: A TLS or SSL flow was aborted due to a handshake failure or certificate validation error.

Explanation: An attempt was made to decrypt a TLS/SSL traffic flow, but the attempt failed due to validation errors and the connection was dropped.

Recommended Action: Evaluate the deny reason to determine if there was a protocol violation or simply an untrusted certificate. Consider the following actions:

- Handshake failures can result if the site requires strong decryption and you have not uploaded the 3DES/AES K9 license for the device. This is a free license, but its availability is restricted by export regulations. If you can acquire it, do so and upload it. If you cannot, you need to bypass decryption for sites that require it. Look at the K9 License Missing column to determine if this is the problem.
- You can adjust the **Deny Transactions to Servers** decryption settings to relax handshake requirements and connections to servers with untrusted certificates. If you set these options to Off, decryption processing will be bypassed for sites that have these problems and the connection will be allowed but it will not be decrypted. This will lessen the impact on your users but it will reduce your control over traffic to these sites.
- If the problem is simply an untrusted certificate, you can add it to the supplemental certificate store by selecting **Configurations > Certificates**.
- Invalid certificates can occur if the time settings are inconsistent between the server and the device. The invalid certificate might not be valid yet, or it might have expired. If you control the server, check the time settings and fix as necessary; replace expired certificates.

TLS Complete

Message: A TLS/SSL transaction passed policy constraints and completed normally.

Explanation: A TLS/SSL traffic flow was allowed by your access policies and completed normally.

Recommended Action: No action is required unless the destination is one that you intended to block or the flow was not given the desired decryption processing (as indicated in the TLS Flow Decrypted property). If the flow was not handled as desired, open the event details to see which policies matched the flow. Consider the following solutions:

- If the traffic matched the wrong policy (of any type), look at the order of policies in the associated policy set. You might need to move this policy below other policies, or move another policy above this one.
- If the traffic matched the correct policy, you can edit the policy to adjust the traffic matching criteria or action.

CX Device and PRSM System Events

The following event messages relate to activities related to the CX device or PRSM server systems rather than to traffic passing through a CX device. The list is organized alphabetically based on event name. Unlike ASA syslog messages, the message ID number for CX/PRSM events is not meaningful, so the number is not listed here.

Backlog Event Archive Error

Message: An archive of events from %End_Date_And_Time% on device %Device_Name% could not be integrated into the event store. The archive file %Info_String% will be deleted.

Recommended Action: The indicated file of archived events could not be merged into the PRSM event store, probably due to problems with the file, so it is being deleted. No action required.

Backlog Events Dropped

Message: This device has deleted events recorded between %Start_Time_Offset% and %End_Time_Offset%.

Recommended Action: The CX system is running out of disk space to store events that it cannot send to the PRSM server due to a loss of connectivity, and is forced to start deleting backlogged events. You cannot recover this data. You must resolve whatever problem exists with the PRSM server or network connection to avoid further loss of data.

Backlog Events Integrated

Message: An archive of events recorded between %Start_Time_Offset% and %End_Time_Offset% on device %Device_Name% has been integrated into the event store.

Recommended Action: No action required. The PRSM server has finished integrating a set of backlogged events it received from a CX device.

Backlog Events Received

Message: An archive of events recorded between %Start_Time_Offset% and %End_Time_Offset% on device %Device_Name% has been received.

Recommended Action: No action required. The CX system sent backlogged events to the PRSM server and the server has received the events, but has not yet integrated the events into the event store. The CX system will delete the backlog from its disk.

Backlog Sys Event Archive Error

Message: An archive of system events from %End_Date_And_Time% on device %Device_Name% could not be integrated into the event store. The archive file %Info_String% will be deleted.

Recommended Action: The indicated file of archived system events could not be merged into the PRSM event store, probably due to problems with the file, so it is being deleted. No action required.

Connected to Syslog Server

Message: This device has successfully connected to syslog server %Server_Hostname%

Explanation: The CX device was configured to send events to a syslog server, and a connection to the server was successful.

Recommended Action: No action required.

Core Bad File Access

Message: User '%AAA_User%' not allowed to access resource '%Resource_Name%'.

Explanation: The indicated user tried to access the indicated resource, but the user is not authorized for that access.

Recommended Action: Evaluate the event to determine if action is required.

Core Low Memory

Message: System low on memory, %Mem_Size_MB%Mb remaining.

Recommended Action: If possible, add memory to the system.

Core System Shutdown

Message: System shutdown initiated.

Recommended Action: No action required.

Core System Startup

Message: System startup initiated.

Recommended Action: No action required.

Critical Recovery

Message: Critical process %Process_Name% recovery action %Recovery_Action% initiated.

Explanation: The indicated recovery action is being taken for the process.

Recommended Action: No action required.

Database Backup Failure

Message: Failure to backup database: %Info_String%

Explanation: An attempt to back up the database failed for the indicated reason.

Recommended Action: Evaluate the reason for failure and take remedial action if possible. Retry the backup.

Database Backup Success

Message: Database backup completed successfully.

Explanation: Someone intentionally backed up the database and the backup was created successfully.

Recommended Action: No action required.

Database Restore Failure

Message: Failure to restore database: %Info_String%

Explanation: An attempt to restore a database backup failed for the indicated reason.

Recommended Action: Evaluate the reason for failure and take remedial action if possible. Retry the restore.

Database Restore Success

Message: Database restore process completed successfully.

Explanation: A database backup was intentionally restored and the restore was successful.

Recommended Action: No action required.

Decryption Cert Constraint Change

Message: Set basic constraints extension to critical is turned %Info_String% for decryption settings certificate %Certificate_Common_Name%.

Recommended Action: No action required. This message indicates that you turned the basic constraints extension on or off for the certificate generated in the decryption settings, which is used by decryption policies.

Disabled Process

Message: Process %Process_Name% disabled due to %Info_String%.

Explanation: The process is disabled for the indicated reason.

Recommended Action: Evaluate the reason to determine if any action is necessary or possible. You might need to log into the system CLI, stop processes, then restart them.

Disconnected from Syslog Server

Message: This device has disconnected from syslog server %Server_Hostname%

Explanation: The CX device was configured to send events to a syslog server, and a connection to the server was broken.

Recommended Action: Evaluate the communication problem, which might be temporary and not remarkable. If the problem persists, ensure that both the device and the syslog server are configured correctly, and that both are operating normally.

Discover Restart

Message: Device discovered by '%Info_String%', Cisco service restarting ...

Explanation: The device was discovered by the indicated server and processes are restarting to place the device in managed mode.

Recommended Action: No action required.

DP DMA Malloc Failed

Message: Data plane failed to allocate packet block memory

Recommended Action: No action required.

DP HTTP Inspector Unavailable

Message: Data plane cannot communicate with HTTP Inspector service.

Recommended Action: If you turned of the HTTP inspector, this is expected. Otherwise, the system will automatically recover the HTTP Inspector service.

DP Out of Packet Blocks

Message: Data plane is unable to allocate packet block of size: %Block_Size%

Recommended Action: No action required.

DP TLS Proxy Unavailable

Message: Data plane cannot communicate with TLS Proxy service.

Recommended Action: No action required. The system will automatically restore communications with the TLS proxy, which is used by decryption policies.

Event Backlogging Started

Message: This device has started saving events to its local disk.

Recommended Action: No action required. The CX system has lost the connection to the PRSM server and is temporarily saving events on its local disk until the connection is re-established.

Event Backlogging Stopped

Message: This device has stopped saving events to its local disk.

Recommended Action: No action required. After re-establishing the connection to the PRSM server, the CX system has started sending events again and has stopped saving them to the local disk.

Event Receiver Connected

Message: This device has successfully connected to the event receiver on host %PRSM_Hostname%.

Recommended Action: No action required. The CX system has re-established a connection to the PRSM server and can now resume sending events to the server.

Event Receiver Disconnected

Message: This device has disconnected from the event receiver on host %PRSM_Hostname%.

Recommended Action: The CX system no longer has a connection to the PRSM server and cannot send events. Investigate the communication problem. The problem could be with the server itself, which might require a restart or other action. Or, it could involve the network between the device and server, such as routing problems or a temporary loss in a WAN connection.

External Device Configuration Error

Message: %LDAP_Directory_URL% unable to return complete query results: %LDAP_message%.

Recommended Action: You might see this message if your LDAP server does not support paging results, as defined in RFC 2696, <http://www.ietf.org/rfc/rfc2696.txt>. The message will either be "Size limit exceeded" or "Admin limit exceeded." If you get this message, it means that the search results exceeded the maximum allowed by the directory server (this is configured on the server, not on PRSM), and PRSM is working with partial results.

To resolve these errors, ensure that the username configured to access the directory realm is not limited for paging (or the limit is sufficiently large) in the directory's own configuration. If the directory you are using does not support paging, you will need to upgrade the directory to one that does support paging.

Inspector Switch Failed

Message: Failed to switch to new update. Update version %App_Version%.

Explanation: The system inspectors could not switch to a new signature update.

Recommended Action: No action required. The system automatically rolls back to the last good update.

PDTS Cons Stats Ntfy Too Big

Message: The notify message length for ring %Pdts_Ring_Name% exceeded maximum.

Recommended Action: No action required.

PDTS Prod Stats Hiwater Limit

Message: PDTS producer for ring %Pdts_Ring_Name% has reached the hiwater limit.

Recommended Action: No action required.

PDTS Prod Stats Ring Full

Message: PDTS descriptor ring is full for ring %Pdts_Ring_Name%.

Recommended Action: No action required.

PDTS Prod Stats Ring High Thresh Exceeded

Message: PDTS producer for ring %Pdts_Ring_Name% has exceeded high threshold.

Recommended Action: No action required.

PDTS Prod Stats Seg Alloc Fail

Message: Failed to allocate producer segment for ring %Pdts_Ring_Name%.

Recommended Action: No action required.

Policy Complete

Message: Policy version %Policy_Version% has now been successfully installed.

Recommended Action: No action required.

Policy Incomplete

Message: Failed to apply policy version %Policy_Version%. Reason: %Info_String%.

Explanation: The system could not apply the indicated policy version.

Recommended Action: Evaluate the reason to determine if action is required or possible.

Policies Within Limits

Message: Policy configuration is within defined limits. Configuration version is %Smx_Config_Version% and policy version is %Policy_Version%.

Explanation: The system is back within limits. You should look for this message after resolving the issues identified in the “Policy Limit Reached” message. Possible limits differ based on the host device for the CX device. The version numbers indicate the PRSM configuration version compared to the local device version.

Recommended Action: No action required.

Policy Limit Reached

Message: Failed to dispatch policy update as %Limit_Name% limit is reached. %Info_String%. Configuration version is %PRSM_Config_Version% and policy version is %Policy_Version%.

Explanation: The system could not apply the policy change. The informational string explains the reason, for example, "Number of total policies (4) exceeds limit (2)." Possible limits differ based on the host device for the CX device. The version numbers indicate the PRSM configuration version compared to the local device version.

Recommended Action: Evaluate the reason to determine if action is required or possible. Redesign your policies so that you can implement your security policy within the device limits.

Process Exited

Message: Module %Process_Name% exited unexpectedly.

Explanation: The named process failed for some unexpected reason.

Recommended Action: The system will automatically recover the process. You might need to log into the system CLI, stop processes, then restart them if the problem continues. A system reboot might also be necessary eventually.

Process Heartbeat Timeout

Message: Heartbeat timed out for module %Process_Name%, action %Info_String% taken.

Explanation: The heartbeat, which indicates process health, was not returned in the expected time interval for the indicated process. The action taken is indicated.

Recommended Action: No action required.

Process Restart

Message: Restarting module %Process_Name%.

Explanation: The system is restarting the indicated process.

Recommended Action: No action required.

Process Startup

Message: Module %Module_Name% is starting up.

Explanation: The indicated system process is starting.

Recommended Action: No action required.

Protocol Pack Update

Message: Switched to update %Component_Display_Name% (%Application_Name%/ %Component_Name%), version %Component_Version%, Update Version %App_Version%. Protocol Pack info: %Info_String%

Explanation: A component update was download. The message indicates the component name, including the technical application name and component, the update version and other information.

Recommended Action: No action required.

Protocol Pack Update Failed

Message: Update of Protocol Pack Failed for Update %Component_Display_Name% (%Application_Name%/ %Component_Name%), version %Component_Version%, Update Version %App_Version%. Protocol Pack info: %Info_String%

Explanation: A component update failed. The message indicates the component name, including the technical application name and component, the update version and other information.

Recommended Action: No action required. The system automatically rolls back to the last good protocol pack. If you see persistent update failures, contact the Cisco Technical Assistance Center.

Remote Device Restored

Message: %Info_String%

Explanation: Communications have been restored to the Context Directory Agent (CDA) that previously became unavailable. A typical message is "CDA 192.168.8.13 is AVAILABLE."

Recommended Action: No action required.

Remote Device Status Changed

Message: %Info_String%

Explanation: If you configured two Context Directory Agents (CDA) in a device's AD Agent policy, these messages indicate a change in the primary and secondary status of the devices when the primary becomes unavailable. A typical info string is "CDA's 192.168.8.13 state changed to STANDBY." You should see two messages, one indicating the CDA that went to STANDBY, and one indicating the CDA that went to ACTIVE.

Recommended Action: The paired messages should indicate that your high-availability setup was successful in maintaining active contact with a CDA. But you should check to ensure the unavailable CDA is healthy.

Remote Device Unavailable

Message: %Info_String%

Explanation: The device can no longer Communicate with the indicated Context Directory Agent (CDA). A typical info string is "CDA 192.168.8.13 is UNAVAILABLE."

Recommended Action: This might be a temporary problem; look for a Remote Device Restored message. If the problem persists, check the CDA and the network path between the device and CDA. If you configured a secondary CDA, the device will start using the secondary; look for Remote Device Status Changed messages.

Service Restored

Message: Communication with %Service_Name% service restored.

Explanation: The system has restored communication with the indicated service.

Recommended Action: No action required.

Service Unavailable

Message: Cannot communicate with %Service_Name% service.

Explanation: The system cannot communicate with the indicated service.

Recommended Action: No action required. The system automatically restores services.

Syslog Export Statistics

Message: This device has exported %Syslog_Server_Export_Count% events to %Server_Hostname% and dropped %Syslog_Server_Drop_Count% events since %Syslog_Server_Statistics_LastLoggedTime%

Explanation: This message periodically provides statistical information on how many events the CX device sent to the specified syslog server since the indicated time, and how many events were dropped.

Recommended Action: No action required.

Syslog Server Connection Failure

Message: This device was unable to establish a connection with the syslog service on %Server_Hostname% port %Server_IP_Port%. Reason: %Info_String%

Explanation: This message indicates the device should not make a connection to the syslog server.

Recommended Action: Evaluate the reason and fix the problem.

Syslog TLS Session Failure

Message: This device was unable to establish a TLS or SSL session with the syslog service on %Server_Hostname% port %Server_IP_Port%. Reason: %Info_String%

Explanation: This message indicates the device should not make a TLS connection to the syslog server.

Recommended Action: Evaluate the reason and fix the problem.

System Halt

Message: System halt initiated for Product %Product_Name% Release %Release_Name% Version %Release_Version%.

Explanation: The system is being halted down intentionally.

Recommended Action: No action required.

System Shutdown

Message: System shutdown initiated for Product %Product_Name% Release %Release_Name% Version %Release_Version%.

Explanation: The system is being shut down intentionally.

Recommended Action: No action required.

System Startup

Message: System startup initiated for Product %Product_Name% Release %Release_Name% Version %Release_Version%.

Explanation: The system is starting up.

Recommended Action: No action required.

TP Generic Error

Message: The intrusion protection module has encountered an error: %Info_String%.

Explanation: The indicated logical or resource error has occurred in the Next Generation IPS module. The potential errors include corrupted signature or configuration files, or an invalid signature regular expression.

Recommended Action: These errors might indicate a problem with a signature or engine update. These errors are not related to your configuration, nor can you resolve the problem yourself. The problem could impact system efficacy until a new update is available. Please contact the Cisco Technical Assistance Center for more information if you get this error.

Unmanage Restart

Message: Revert to unmanaged mode. Cisco service restarting ...

Explanation: This managed device is reverting to unmanaged mode and services are restarting to complete the change.

Recommended Action: No action required.

Updater Apply Commit Failed

Message: Committing update failed for %Component_Display_Name% (%Application_Name%/ %Component_Name%), version %Component_Version%, Update version %App_Version%.

Explanation: The system tried to commit to a new update, which is the process of switching to start using a new update instead of the previous version of the component.

Recommended Action: No action required. Although a commit failure might result in corrupted data, the system automatically rolls back to the last good version.

Updater Apply Prepare Failed

Message: Preparing update failed for %Component_Display_Name% (%Application_Name%/ %Component_Name%), version %Component_Version%, Update version %App_Version%.

Explanation: The system was not able to prepare the update for use. Preparation includes moving the update to the correct location and performing data verification checks. The failure does not result in the corruption of any active data.

Recommended Action: No action required. The system will try to download a good version of the update after a cool-down period.

Updater Clean Failed

Message: Cleanup after update failed for Update Version %App_Version%

Explanation: The updater could not delete an old update from disk after applying a new one.

Recommended Action: No action required. This should have no effect on the system.

Updater Commit In Progress

Message: Commit update in progress for %Component_Display_Name% (%Application_Name%/Component_Name%), version %Component_Version%. The update to version %App_Version% might take up to 30 minutes.

Explanation: Committing an update for the indicated component version is underway. You are being notified that the update can take up to 30 minutes.

Recommended Action: No action required.

Updater Connection Failed

Message: Failed to connect to the updater server: %Update_Url%

Explanation: The system could not connect to the update server. This normally means that there is a network connectivity problem between the system and the Cisco update server. The message shows the URL for the server.

Recommended Action: Evaluate the network problem. The system must be able to make an HTTP connection to the update server.

- If you configured an HTTP proxy server on the **Configurations > Updates** page, verify that settings are correct and that the required services are running correctly on the proxy.
- If you are not using a proxy, the management interface must have a connection to the Internet that allows HTTP traffic. Log into the system CLI and use **ping** to verify that you can touch the update server, and **traceroute** to determine the path. Verify that HTTP traffic is allowed through the router hops that you control.

Updater Context Write Failed

Message: Failed to write update context to file %File_Path%, Update Version % App_Version%

Explanation: The system was not able to load a new context saved by the updater. The context is what the scanners use. This failure indicates that the context could not be written to disk.

Recommended Action: No action required. The system automatically handles this error case.

Updater Download Failed

Message: Error downloading version %Component_Version% for %Component_Display_Name% (%Application_Name%/Component_Name%).

Explanation: There was an error during the download of the update from the update server.

Recommended Action: No action required. The system will attempt the download again at the next update interval.

Updater Import SAS Failed

Message: Failed to import SAS.

Explanation: A bad Security Application Scanner (SAS) engine was downloaded and applied.

Recommended Action: No action required. The system automatically rolls back to the last good engine.

Updater License Invalid

Message: No valid license for security services. Updates are disabled.

Explanation: All of the subscription licenses have expired. No signature or category updates will be performed.

Recommended Action: Purchase and apply new licenses if you want to use these features.

Updater License Valid

Message: Valid license detected. Updates are enabled.

Explanation: At least one of the subscription licenses has not expired. Therefore, signature and category updates can be retrieved.

Recommended Action: No action required.

Updater Register Failed

Message: Registering update with Management Server failed for %Component_Display_Name% (%Application_Name%/Component_Name%), version %Component_Version%, Update Version %App_Version%.

Explanation: The updater failed to pass the update package to the management plane.

Recommended Action: No action required. The system will try to download a new update later.

Updater Scanner Connected

Message: Scanner has connected to the Update Agent.

Explanation: A scanner connected to the updater, which is required to receive notifications that new updates are available for the scanner to switch to.

Recommended Action: No action required.

Updater Scanner Disconnected

Message: Scanner has been disconnected from the Update Agent. Attempting to reconnect.

Explanation: A scanner has disconnected from the updater.

Recommended Action: No action required.

Updater Switch Failed

Message: Switching to new update failed for %Component_Display_Name% (%Application_Name%/Component_Name%), version %Component_Version%, Update version %App_Version%.

Explanation: The updater was not able to load the new update into memory after committing it.

Recommended Action: No action required. The system will automatically roll back to the last good version.

Updater Switch Response Failed

Message: Some scanners failed to switch to %Component_Display_Name% (%Application_Name%/ %Component_Name%), version %Component_Version%, Update version %App_Version%.

Explanation: One or more scanners failed to load the new update.

Recommended Action: No action required. The system will automatically roll back to the last good version.

Updater Switch Response Success

Message: All scanners switched to new Update Version %App_Version%

Explanation: All scanners have successfully loaded the new update into memory.

Recommended Action: No action required.

Updater Update Applied

Message: Applied update for %Component_Display_Name% (%Application_Name%/ %Component_Name%), version %Component_Version%. Update version is now %App_Version%

Explanation: The previously downloaded update has been successfully applied to the system, but it is not yet active.

Recommended Action: No action required.

Updater Update Change Window

Message: Update Settings changed: Updates Enabled? %Update_Enabled%; Update Window Start time: %Start_Time_Offset%; Update Window End time: %End_Time_Offset%.

Explanation: The settings for the update window have changed as indicated. The change can disable updates, set a specific daily time window for updates, or allow updates all day.

Recommended Action: No action required.

Updater Update Downloaded

Message: Downloaded version %Component_Version% for %Component_Display_Name% (%Application_Name%/ %Component_Name%).

Explanation: The identified component update has been downloaded but not yet applied.

Recommended Action: No action required.

Updater Update Switch

Message: Switched to update %Component_Display_Name% (%Application_Name%/ %Component_Name%), version %Component_Version%, Update Version %App_Version%

Explanation: The system has switched to using this signature update. The update is now active and loaded into memory.

Recommended Action: No action required.

User Action

Message: User %AAA_User% %User_Action%.

Explanation: This user performed the indicated action.

Recommended Action: No action required.

User DB Retrieval Failure

Message: Failed while trying to authenticate user due to: %Info_String%

Explanation: A user attempted to log in, but the system could not verify credentials for the indicated reason.

Recommended Action: No action required.

User Login Failure

Message: %Info_String% user %AAA_User% failed to log in.

Explanation: The indicated user failed to log into the web interface. The message indicates whether the user is locally defined on the system or is a remote user defined on the directory server.

Recommended Action: If the problem is persistent, help the user understand the username/password requirements for logging into the system.

User Login Success

Message: %Info_String% user %AAA_User% successfully logged in.

Explanation: The indicated user logged into the web interface. The message indicates whether the user is locally defined on the system or is a remote user defined on the directory server.

Recommended Action: No action required.

Event Columns

The event table can include the columns described in the following table. Not all columns are available in all event views or for all event types. The device type column indicates the types of devices whose events might include information in the column.

Column	Device Type	Description
AAA Group	ASA	The AAA group policy.
AAA Server	ASA	The AAA server that handled the user request for access and performed the authentication, authorization, or accounting.
AAA Type	ASA	The AAA type, authentication, authorization or accounting.
ACE Hash 1 ACE Hash 2	ASA	The hashcode1 and hashcode2 of the access control list entry (ACE).
ACL Name	ASA	The name or ID of the access control list (ACL).

Column	Device Type	Description
Action	ASA CX	(ASA) The action performed on the flow. For example: Terminated or denied. (CX) The action taken for IPS events. Values are based on the event type: • Info—Flow Tear Down, Flow Create Tear Down, HTTP Complete, TLS Complete. • Deny—Flow Deny, HTTP Deny. • Aborted—HTTP Aborted.
Application	CX	The name of the application used in the traffic flow, if any is available.
Application Tag	CX	If the traffic flow matches an application, the application tag to which the application belongs. If the application maps to more than one tag, a single tag is shown, with preference to showing the “cloud” tag.
Application Type	CX	If the traffic flow matches an application, the application type to which the application belongs.
Attacker	CX	The user who started the attack, as identified by the Next Generation IPS service.
Attacker IP	CX	The address of the user who started the attack, as identified by the Next Generation IPS service.
Auth Policy Name	CX	The name of the identity policy applied to the traffic flow, if any.
Auth Realm Name	CX	The name of the directory realm used in the identity policy applied to the flow.
Auth Retry Count	CX	The number of times the user tried but failed to supply the correct username and password during active authentication.
Auth Server Name	CX	The name of the directory server used during authentication.
Auth Type	CX	The authentication mechanism used, such as basic authentication (clear text), NTLM, or Kerberos.
AVC App Behavior	CX	If an application is matched, the specific behavior of that application being used in the traffic flow, if the application has defined identifiable behaviors.
Backtrace	CX	The back trace generated from parser exception, shown in HTTP Inspection Aborted events.

Column	Device Type	Description
Botnet Category	ASA	The category showing the reason a domain name is blacklisted, for example, botnet, Trojan, spyware, and so on.
Botnet Domain	ASA	The domain name or IP address in the dynamic filter database to which the traffic was initiated. It can be black listed, white listed, or grey listed.
Botnet Domain	ASA	The threat level: none, very-low, low, moderate, high, and very-high.
Byte Count	CX	The number of bytes transmitted in the traffic flow.
Class Map	ASA	The class map name.
Client OS	CX	The name of the operating system running on the client for remote VPN connections.
Component	CX PRSM	In system events, the name of the component to which the event applies.
Config Version	CX	The configuration version for the policies matched by this event. The number relates directly to the version numbers shown in the change history page.
Connection Duration	ASA	The lifetime of the connection.
Connection ID	CX ASA	An identifier for the traffic flow or connection.
Connection Limit	ASA	The maximum number of connections or sessions.
Connection Termination Value	ASA	A factor for which the connection is terminated, for example, incorrect version or invalid payload-type.
Context Name	CX ASA	The name of the security context for an ASA configured in multiple-context mode.
Current Connection Count	ASA	The number of current connections.
Decryption Policy Name	CX	The name of the decryption policy that matched this flow, if any.
Deny Reason	CX	For Flow Deny or HTTP Deny events, the reason the flow was denied, such as "Flow is denied by access policy."

Column	Device Type	Description
Description	CX ASA	The event message.
Destination	CX ASA	The IP address or host name of the destination of the traffic flow.
Destination Host	CX ASA	The fully-qualified domain name (FQDN) of the destination if it is known.
Destination Interface	ASA	The destination interface. For Etherchannel alerts (426001-426003), this is the name of the Etherchannel interface for which this event occurred. The member interface is identified in the Source Interface column.
Destination IP	CX ASA	The IP address of the destination of the traffic flow.
Destination Port	CX ASA	The port number of the destination for TCP/UDP traffic flows.
Destination Service	CX ASA	The destination service for the flow, one of tcp/port, udp/port, icmp/message. For example, tcp/80 or icmp/echo.
Device	CX ASA PRSM	(PRSM Multiple Device mode only.) The device from which the event was received. If the event relates to the PRSM server (such as updater events), PRSM is shown as the device. For devices configured for high availability, the logical name of the pair is shown.
Direction	ASA	The direction of the traffic: inbound or outbound.
Dropped Event Count	CX PRSM	(Dropped Event messages.) The number of event messages dropped, usually due to an event rate higher than the device can handle.
Dropped Event Type	CX	(Dropped Event messages.) The name of the type of events that were dropped.
Egress Interface	CX	The interface through which the traffic left the device.

Column	Device Type	Description
Error Details	CX	If there are OpenSSL errors during decryption processing, the details about those errors. These messages are directly from the OpenSSL library. For example, if ASA CX does not include the certificate for a site, and you have not added it to the Configurations > Certificates page, you will see a decryption error like the following on a TLS Abort event: error: 14090086: SSL routines: SSL3_GET_SERVER_CERTIFICATE: certificate verify failed: Server Certificate Common Name: servername To resolve the error for self-signed certificates, upload the certificate to the Certificates page. For certificates issued by a certificate authority, examine the certificate hierarchy to determine if you should download a root or intermediate certificate to add to the Certificates page so that other sites that use certificates from the CA will be trusted.
Event ID	ASA	A unique sequential number for each event, assigned internally.
Event Name	ASA	A user-friendly name given to the event.
Event Type	CX ASA	The name of the event.
Event Type ID	ASA	For ASA devices, the syslog message number. CX devices will also show an event type ID, but the number is not meaningful.
Hit Count	ASA	The number of times the flow was permitted or denied by the ACL entry in the configured time interval. The value is 1 when the ASA generates the first syslog message for a particular flow.
Hit Count Info	ASA	ACL Hit Count information, for example, First hit.
ICMP Code	ASA	The code of the ICMP type. For example, ICMP Type 3 and Code 0 is Net Unreachable or Code 1 is Host Unreachable.
ICMP Type	ASA	The type of ICMP message. For example, 3 for Destination Unreachable, 8 for Echo.
Identity Source	CX	The source from which the user identity was obtained: proxy (that is, authentication proxy, which is used during active authentication), CDA or AD agent (passive authentication), VPN (from a remote access VPN connection to the ASA), or none.
Identity Type	CX	The type of identity, meaning how the user identity was acquired: active, passive, none, unknown, or guest.

Column	Device Type	Description
Ingress Interface	CX	The interface through which the traffic entered the device.
HTTP Header Injection	CX	If you inject a header in the HTTP Request message, for example, to add your school or district ID to enable YouTube for Schools, the content of the injected header.
K9 License Missing	CX	Whether the 3DES/AES (K9) license is installed, yes or no. This license is required for decrypting traffic with a server that requires strong encryption. Flow Deny or TLS Abort events that indicate a secure session could not be established, with Yes in this column, mean that you need this license to do decryption with the destination. The license is free but subject to export controls; if you cannot install it, bypass decryption for this destination.
License Limit	ASA	The maximum number of licenses.
List Name	ASA	The list that includes the domain name, administrator whitelist, blacklist, or IronPort list.
Malicious Host	ASA	The hostname of the malicious host.
Malicious IP	ASA	The IP address of malicious device.
Max Connection	ASA	The maximum number of NAT connections.
MaxEmbryonic Connection	ASA	The maximum number of embryonic connections.
NAT Destination	ASA	The translated (also called natted) destination IP address.
NAT Destination Service	ASA	The translated (or natted) destination port.
NAT Destination Host	ASA	Host name of the translated destination.
NAT Global IP	ASA	The global address. It can contain IPv4 or IPv6 addresses.
NAT Source	ASA	The translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.
NAT Source Service	ASA	The translated (or natted) source port.
NAT Type	ASA	The type of network address translation, for example Static or Dynamic.
Policy Name	CX	The name of the access policy that matched this traffic flow.

Column	Device Type	Description
Policy Map	ASA	The policy map name.
Protocol	CX ASA	The protocol of the traffic flow, such as tcp, udp, icmp, and so forth.
Protocol Version	ASA	The protocol version.
Protocol (Non L3)	ASA	Some non-Level-3 or -4 protocol seen in the event, for example, TACACS, RADIUS, FTP, or H245.
Rate Limited	CX	Whether a rate limit was applied to the transaction.
Reason	ASA	A rationale associated with certain events. For example, a connection tear down may have an associated reason.
Receive Time	CX ASA	The date and time the event was received.
Reputation Score	CX	The numeric web reputation score of the destination web site.
Reputation Threat Detail	CX	A detailed description of the type of threat.
Reputation Threat Type	CX	A short description of the type of threat that caused the score to be low, or blank if there is no threat in particular.
Request MIME File Type	CX	The media, or MIME, type associated with files contained in the traffic flow request from the source. In the event details, this is called the request content type.
Response MIME File Type	CX	The media, or MIME, type associated with files contained in the traffic flow response from the destination. In the event details, this is called the response content type.
Safe Search	CX	Yes if the device rewrote the search URL to enforce safe search, which eliminates inappropriate content from search results.
Server Certificate Issuer	CX	An identifier of who issued the destination server certificate for TLS/SSL traffic. For example, /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at https://www.verisign.com/rpa (c)09/CN=VeriSign Class 3 Secure Server CA - G2.
Server Certificate Name	CX	The common name on the certificate used in TLS/SSL traffic, such as the host name of the destination server.

Column	Device Type	Description
Severity	CX ASA	The severity of the message, for example, Informational or Error.
Source	CX ASA	The source of the traffic flow, username or IP address. The username is shown only if you configure identity policies and there is a username mapping for the IP address.
Source Host	ASA	The hostname of the source IP address.
Source Interface	ASA	The source interface. For Etherchannel alerts (426001-426003), this is the name of the interface that is part of the Etherchannel bundle for which this event occurred. The Etherchannel interface is identified in the Destination Interface column.
Source IP	CX ASA	The IP address of the source of the traffic flow.
Source Port	CX ASA	The port number of the source of TCP/UDP traffic flows.
SSO Server	ASA	The single sign-on (SSO) server name.
SSO Server Type	ASA	The single sign-on (SSO) server type, for example, SiteMinder.
Target	CX	Who was attacked, as identified by the Next Generation IPS service.
Target IP	CX	The IP address that was attacked, as identified by the Next Generation IPS service.
Threat	CX	The threat identified, if any. For example, German Federal Trojan.
Threat Score	CX	If a threat is identified, the score associated with the threat. Scores are 0 to 100, with 100 being the worst.
TLS Ambiguous Destination	CX	Whether the TLS Proxy is unable to determine which one of the domains present in the server certificate was the client's intended destination, true or false.
TLS Server Cipher Suite	CX	The cipher used in TLS/SSL traffic, for example, RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5.
TLS Flow Decrypted	CX	Whether the traffic flow was decrypted by the TLS proxy, Yes or No.

Column	Device Type	Description
TLS Flow Encrypted	CX	Whether the traffic flow was TLS/SSL encrypted, Yes or No.
TLS Protocol Version	CX	The version of TLS used in the TLS/SSL traffic flow, for example, TLSv1.
TLS Requested Domain	CX	The client's hint to the server indicating which DNS domain is being accessed. This value comes from the Server Name Indication extension to the TLS protocol and this field is empty if the TLS client does not use this extension.
Tunnel Type	ASA	The VPN tunnel type.
URL	CX	For HTTP/HTTPS traffic, the URL of the destination web site.
User Accepted Warning	CX	Whether the user accepted a warning end user notification and continued to the undesirable site. This value relates to access policies that apply the Warn action. For HTTP and decrypted HTTP traffic that matches a Warn policy, the flow is initially denied, with the Deny Reason for an HTTP Deny indicating that the user was warned and a confirmation is pending. A subsequent HTTP Complete or HTTP Abort might indicate that the user accepted this warning.
User Realm	CX	The combination of the authentication realm and username in the format Realm\username.
Username	CX ASA	If known, the username associated with the source of the traffic flow.
VPN Group	ASA	The VPN group policy.
VPN IPSec SPI	ASA	The IPSec Security Parameter Index.
VPN User	ASA	The VPN username.
Web Category	CX	For traffic flows that have a destination URL, the web category to which the URL belongs.



PART

Configuring Context-Aware Security

- [Managing Authentication and Identity Services, page 225](#)
- [Controlling Network Access with Context-Aware Access Policies, page 249](#)
- [Managing SSL/TLS Traffic Flows, page 283](#)



CHAPTER 11

Managing Authentication and Identity Services

You can create access policies based on user identity rather than IP addresses. To enable identity-based services, you configure policies and options to obtain user identity, and then use identity objects in your access policies. The following topics describe authentication and identity services and how to configure them.

- [Overview of Authentication and Identity Services, page 225](#)
- [Configuring Authentication and Identity Services, page 227](#)

Overview of Authentication and Identity Services

Authentication is the act of confirming the identity of a user. You can obtain user identities passively or actively.

With passive authentication, user identity is obtained by checking a mapping of IP addresses to user identity collected by the CDA or AD agent application. Authentication is passive because the user is not prompted to provide credentials.

With active authentication, when an HTTP or decrypted HTTPS traffic flow comes from an IP address for which ASA CX has no user-identity mapping, you can decide whether to authenticate the user who initiated the traffic flow against the directories configured for the network. If the user successfully authenticates, the IP address is considered to have the identity of the authenticated user.

You can apply identity-based access policies to traffic that has either a passive or active user mapping, controlling network access based on who is trying to access the resource rather than controlling it by static IP address-based policies.

There are many separate features involved in providing authentication and identity services:

- **Directory realms**—You must define the directory realms that provide authentication services. A realm contains one or more directory servers, such as Active Directory or OpenLDAP, that define the user names and user group membership for the network. When you configure identity policies, you must select the directory realm that will provide authentication.
- **Identity policies**—Use identity policies to enable policies based on user identity, including username and user group membership. Identity policies never result in dropped or blocked traffic, even if the user fails to authenticate. Instead, they collect user information, so that access policies can match traffic based on user identity, and so that dashboards and events include user identity information.

- **Authentication settings**—Authentication settings control how authentication mappings and prompts are managed. For example, you can define how long a username-to-IP address mapping remains valid before you want to prompt the user to reauthenticate. These settings have system defaults, so you need to adjust them only if you desire different settings.
- **Identity policy objects**—Identity policy objects define the specific user names or user group names for which you want to define access control. You can also selectively exclude names from an object. For example, you could define an object that includes the user group Eng, but exclude users Guest1 and Guest2, who are members of that group.
- **Access policies**—When you specify Identity policy objects as part of the source field in an access policy, you are controlling access to the destination resources based on user identity.
- **CDA or Active Directory agent**—(Optional.) You can install the CDA or AD agent in your network to collect user identity information when users log into the network, before they try to pass traffic through the device. This type of identity is considered a passive identity mapping. By collecting this information, you can enable identity-based access control without forcing users to authenticate directly.
- **Identity-based dashboards**—Many dashboards include identity information if it is available, so you can analyze the traffic on your network based on user identity. The Users dashboard is specifically designed to provide user-based network usage information. You can use these dashboards to identify cases where network acceptable use criteria are not being met.

Supported AAA Servers and Authentication Methods

You can use AAA servers running LDAP (Lightweight Directory Access Protocol) to implement authentication and identity services. Following are the supported servers and the authentication methods you can use with each.

- **Microsoft Active Directory**—You can use the following AD servers. Ensure that you disable LDAP signing on the Active Directory server.

- Windows Server 2008 R2
- Windows Server 2003 R2

You can use the following authentication methods in identity policies when using AD; you can also allow negotiation to select the strongest supported method:

- NTLM (All Windows platforms.)
- Kerberos (Windows XP only.)
- Basic and Form (No restrictions.)

- **OpenLDAP**—Version 2.4.21 or later. The Basic and Form authentication methods are available.

Types of User Identity

To enable identity services, so that traffic flows can be conditionally handled based on the user who initiates the flow, the CX device maps the user name to the IP address of the user's device.

Based on how the user-to-IP address mapping is obtained, users are considered to have one of the following identity types:

- **Active**—The user was directly authenticated by the CX device. Active authentication is applied to HTTP or decrypted HTTPS traffic only. If any other type of traffic matches an identity policy that requires or allows active authentication, then active authentication will not be attempted.
- **Passive**—A user-to-IP address mapping was received from the Context Directory Agent (CDA) or Active Directory (AD) agent. This type of identity can be available regardless of the types of traffic sent by the user.
- **Unknown**—There is no user-to-IP mapping. For example, the user tried to actively authenticate to the CX device, but authentication failed. Users who fail active authentication are represented in user dashboards under the username *Realm\ANONYMOUS*, unless you enabled guest access, in which case the username is Guest. Users who simply do not have a mapping because they were not required to authenticate are shown as their IP address.
- **Guest**—The user failed active authentication and you enabled guest access on the identity policy. The username for these users is Guest in dashboards and events.

What to Tell Users About Authentication

If you configure identity policies to require or allow for active authentication, users might be prompted to authenticate when they make HTTP requests, or HTTPS requests that are decrypted by decryption policies. To help users authenticate correctly, ensure that they know the following:

- Authentication prompts will include the name of the directory realm and the ASA CX management IP address. Ensure that users understand that authentication requests that include this information are valid requests and that they should respond to them.
- When using NTLM or Kerberos authentication with Active Directory, users can enter their name in any of these formats: username, username@domain, DOMAIN\username. For example, user1, user1@example.com, ENG\user1.
- When using basic authentication, users should supply their name in username@domain format, for example, user1@example.com.

Configuring Authentication and Identity Services

The following procedure provides an overview of the process for configuring authentication and identity services. Use this procedure to understand the general configuration process and see the referenced topics for detailed steps.

Procedure

-
- Step 1** Configure directory realms as described in [Configuring Directory Realms](#), on page 230. The directory realms define the directory servers that contain user and user group information. Users authenticate against these servers to provide user identity, which can then be used to provide identity-based access control and reporting.
- Step 2** (Optional) Configure the Active Directory (AD) agent as described in [Identifying the Active Directory Agent](#). If you are using Active Directory in your directory realm, you can install the Context Directory Agent (CDA) or Active Directory agent to provide passive user-to-IP address mappings based on Windows login authentications.

Step 3 (Optional) Change the authentication settings if necessary as described in [Configuring Authentication Settings, on page 246](#).

Authentication settings have default values appropriate for most networks, so you might not need to change them.

Step 4 Create at least one identity policy for each directory realm as described in [Configuring Identity Policies, on page 235](#).

Identity policies determine the type of identity users must supply, either through active authentication, passive mapping, or none at all if you elect to not require authentication. You must have at least one policy per realm, or you will not get user identity mappings for users defined within the realm.

Note If you intend to use active authentication, you must also ensure that the policy redirecting traffic from the ASA to the ASA CX SSP enables the authentication proxy. If you do not enable the authentication proxy, you are limited to passive authentication. For more information, see [Enabling Active Authentication, on page 240](#).

Step 5 If you are using active authentication, and you want to enforce authentication for HTTPS requests, configure decryption policies to decrypt secure traffic from the sources you want to authenticate. The decryption policy should apply the Decrypt Everything action.

Step 6 (Optional) When using Active Directory, you can configure client browsers to provide transparent authentication for NTLM or Kerberos as described in [Enabling Transparent User Authentication, on page 241](#).

When configured to provide transparent authentication, browsers can respond to authentication requests from trusted sources by providing Windows login information without prompting users. Thus, active authentication occurs but users are not aware that authentication happened and they are not inconvenienced or confused by an unexpected authentication prompt.

Step 7 (Optional) Create identity-based access policies as described in [Configuring Context-Aware Access Policies, on page 250](#).

You can control access to a destination by using identity policy objects in the source definition of an access policy. The identity object defines the user or user group names that are allowed, or denied, access to a destination. For information on identity policy objects, see [CX Identity Objects, on page 132](#).

Step 8 Analyze network traffic using identity information in dashboards and events. Many dashboards, such as the Users dashboard, includes identity-based traffic analysis. You can also access dashboards related to identity-based access policies by looking at the policy hits dashboard for the policy. Use this information to determine the efficacy of your policy and to identify users who are violating acceptable use policies. For information on dashboards, see [Viewing Dashboards and Reports, on page 157](#).

In addition to dashboards, the Event Viewer includes user name information on events when available. For information on Event Viewer, see [Viewing Events, on page 183](#).

Overview of Directory Realms

A directory realm is a named list of directory servers. For Active Directory (AD), a realm is equivalent to an AD domain. For LDAP, the realm is any LDAP server and its redundant servers, that is, all servers with the same top level distinguished name (DN).

You use directory realms:

- In identity policies, to identify the directories with which the user must authenticate. There must be an identity policy for each realm in order to use identities defined in the realm in access policies.

- On the Users page, to identify the directory that contains remote users you are granting access to the web interface.

To open the directory realms page, where you can add, edit, or delete realms and the directory servers contained in them, or reorder the directory servers within a realm, select **Components > Directory Realm**.

The Directory Realm page includes the following items:

I want to

Contains the following commands:

- **Add Realm**—To add a new directory realm. You are prompted for a name, description, and directory type. The realm name will appear in dashboards along with the username in the format Realm\username. Thus, you might want to use NetBIOS domain names for your realm names so that username strings include the expected NetBIOS domain name.

List of directory realms and their directory servers

The list shows all directory realms and within each realm is an ordered list of directory servers contained in the realm. The first server in the list is always used unless it becomes unavailable, in which case the next server in the list is tried until a response is received.

If there is more than one AD realm, you can define identity policies that use NTLM, Kerberos, or Advanced active authentication with just one of the realms. The device will bind to that AD realm, which is considered the primary realm. You can use basic and form active authentication, or passive authentication, with all realms.

To see the commands related to a directory realm or server, mouse over the directory realm header or the directory server row. The following are the available commands:

Directory realm commands:

- **Add New Directory**—To add a new directory server to the realm. The server is added to the top of the realm as the first entry. After adding the directory, move it to the desired position before committing your changes.
- **Delete Realm**—To delete the realm. You cannot delete a realm if it is being used in a policy or policy object, or as the global realm for system users.
- **Edit Realm**—To edit the realm properties.

Directory server commands:

- **Delete Directory**—To delete the directory server.
- **Edit Directory**—To edit the directory server properties.
- **Move Up, Move Down**—To move the directory server until it is in the desired position. The up and down commands move the directory a single row. You can also click and drag a directory to the desired location.

Configuring Directory Realms



Tip

Obtain the values for these settings from your AD or OpenLDAP administrator.

A directory realm is a named list of directory servers. For Active Directory (AD), a realm is equivalent to an AD domain. For LDAP, the realm is any LDAP server and its redundant servers, that is, all servers with the same top level distinguished name (DN).

To configure a directory realm, you must create the realm and then add directory servers to the realm. The following procedure explains both aspects.



Tip

(Single Device mode.) When you create your first directory realm, a default identity policy is automatically created for that realm. You can edit the policy to change any characteristic of the policy to suit your needs. In Multiple Device mode, no default policy is created.

Procedure

Step 1 Select **Components > Directory Realm**.

The directory realms are organized in a list, and each directory realm contains a priority list of directory servers. The first directory is always used unless it becomes unavailable, in which case subsequent directories are used. To see the commands related to a realm, you must mouse-over the name of the realm; to see commands related to a directory server, you must mouse-over the row for the directory. You can then select the desired command.

If you need to work with an existing directory realm or server, use the filter controls to help you locate the item.

Step 2 Configure the directory realm.

a) To open the form for creating or editing a directory realm, do one of the following:

- To create a new realm, select **I want to > Add Realm**.
- To edit an existing realm, mouse over the realm name and click **Edit Realm**.

b) Fill in the directory realm properties:

- **Name**—The name of the realm. This name will appear in dashboards along with the username in the format Realm\username. Thus, you might want to use NetBIOS domain names for your realm names so that username strings include the expected NetBIOS domain name.

The name is also visible to end users if you create an identity policy for the realm that results in users occasionally being prompted to authenticate.

- **Description**—A description for the realm.

- **Directory Type**—The type of directory server, either Microsoft **Active Directory** or **Standard LDAP**.

Select SSO if you are creating a single-sign-on (SSO) directory for integration with other management products. For detailed information on creating an SSO realm, see [Configuring SSO Directories and Users](#), on page 371.

- **Primary Domain**—(AD only.) The fully qualified Active Directory domain name that the device should join. For example, example.com. Create separate realms for each domain, even if there are trust relationships among the domains.
- **Join Username, Join Password**—(AD only.) The Active Directory sAMAccountName or User Principal Name to use when joining the device to the AD domain or to leave the domain. These credentials must have the authority within AD to join devices to the domain or to leave the domain.

- c) (AD only.) Click the **Test Domain Join** link to verify that you can join the device to the AD realm. If the test fails, you need to resolve the issues. Log into the CLI and use the **show dns** command to verify that you have configured the right DNS domain for the device, and included the domain in the search domains list. Another potential problem might be that intervening firewalls do not have all required ports open to enable domain join; see the Microsoft support site for details on how to configure a firewall for domains and trusts for specific port requirements for your setup.
- d) Click **Save** to save your changes.

Step 3 Configure the directory servers within a realm:

- a) To open the form for adding or editing a directory server, do one of the following:
- To add a directory server, mouse over the realm name and click **Add New Directory**.
 - To edit an existing directory server, mouse over the server name and click **Edit Directory**.
- b) Fill in the directory server properties. For detailed information, see [Directory Properties, on page 231](#).
- Tip** Be sure to click the **Test Connection** link when filling in the properties. This will test whether the directory can be contacted using those properties. If the connection fails and you are certain the properties are correct, ensure there is a network path between the device and the directory server. If necessary, log into the CLI to use commands such as **ping** and **traceroute**.
- c) Click **Save** to save your changes.
- You can repeat the process of adding directories to identify all servers used in the realm.

- Step 4** If necessary, move the server entries so that they are in priority order within the directory realm, with the primary server at the top of the list.
- You can drag and drop server entries, or use the **Move Up** or **Move Down** links that appear when you mouse over a server entry.

Directory Properties



Tip Obtain the values for these settings from your AD or OpenLDAP administrator.

The following table describes properties for directories that you include in directory realms. Where indicated, some properties apply to certain directory types only. For more information about LDAP properties and their syntax, refer to RFC 2253.

Table 6: Directory Properties

Property	Description
Directory Hostname	The DNS name or IP address of the directory server.
Port	The port number used for communications with the server. The default is 389. Note Port 389 is the only supported port, which supplies standard LDAP (plain text) connections. You cannot use secure LDAP (LDAP over SSL) on port 636, nor can you specify the Active Directory Global Catalog Server on port 3268.
LDAP Login Name (LDAP only.)	The distinguished name of the directory object in the LDAP hierarchy used for authenticated binding. The LDAP login name represents a user record in the LDAP server that the administrator uses for binding (administrator privileges are not required for the user). For example, cn=Administrator,dc=example,dc=com. This string is case-sensitive and alphanumeric. Special characters are allowed.
AD Login Name (AD only.)	The user name used for authenticated binding with the AD server, for example, username@example.com. For Active Directory, the user privilege requirements differ based on the type of authentication you will allow in your identity policies. Ensure you specify a user with the required privileges: • NTLM, Basic—Any valid user account should work. • Kerberos—The user account must have the “Validated Write to Service Principle Name” permission. See the Active Directory documentation for details on delegating authority to modify SPNs.
AD/LDAP Password	The password for the user specified in AD/LDAP Login Name.
User Search Base	The LDAP search base distinguished name used to fully-qualify usernames being authenticated against LDAP directories. The field also defines the location in the LDAP hierarchy for searching or querying user information in both LDAP and AD. For example, cn=users,dc=example,dc=com. The maximum length is 128 characters. The string is case-sensitive. Spaces are not permitted, but other special characters are allowed. If you do not specify a user search base, the system will create a generic one consisting of the entire domain components of the directory name. For example, if the directory name is ad.example.com, the constructed qualifier would be dc=example,dc=com. The generic name might or might not work in your network, so it is best to explicitly enter a qualifier. For standard LDAP, you probably will always need to explicitly enter a qualifier. If you use an IP address instead of a DNS name, you will always need to enter a qualifier. For more information, see Determining the Directory Search Base, on page 233.

Property	Description
Group Search Base	The LDAP search base distinguished name used to search individual groups for user membership for authorization against LDAP directories. The field also defines the location in the LDAP hierarchy for searching or querying user group information in both LDAP and AD. For example, ou=groups,dc=example,dc=com. The maximum length is 128 characters. The string is case-sensitive. Spaces are not permitted, but other special characters are allowed. If you do not specify a group search base, the system will create a generic one consisting of the entire domain components of the directory name. For example, if the directory name is ad.example.com, the constructed qualifier would be dc=example,dc=com. The generic name might or might not work in your network, so it is best to explicitly enter a qualifier. If you use an IP address instead of a DNS name, you will always need to enter a qualifier. For more information, see Determining the Directory Search Base, on page 233. Note It is possible, but not necessary, that the user and group search base is the same string.
Group Attribute	The LDAP attribute that lists all users that belong to a group. Select one of the following: • member—The normal group attribute for Active Directory. • uniqueMember—The normal group attribute for OpenLDAP. • Custom—Select this option if you created a custom group attribute in your directory, such as UserInGroup, and enter the attribute value in the field provided.
Test Connection link	Tests whether the properties you entered will successfully connect to the directory server. If the connection fails, check your settings. If you are certain they are correct, check whether there is a network path between the device and the directory.

Determining the Directory Search Base

When you configure directory properties, you need to specify the user and group search bases. These bases are defined in your directory server, and differ from network to network. You must enter the correct bases for identity policies to work. If the bases are wrong, the system cannot determine user or group names, and thus identity-based policies will be inoperable.



Tip

To get the correct bases, consult the administrator who is responsible for the directory servers.

For active directory, you can determine the correct bases by logging into the Active Directory server as domain administrator, and using the **dsquery** command at a command prompt as follows to determine the bases:

User search base

Enter the **dsquery user** command with a known username (partial or complete) to determine the base distinguished name. For example, the following command uses the partial name "John*" to return information for all users that start with "John."

```
C:\Users\Administrator>dsquery user -name "Jphn*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

The user search base would be "DC=csc-lab,DC=example,DC=com."

Group search base

Enter the **dsquery group** command with a known group name to determine the base distinguished name. For example, the following command uses the group name Employees to return the distinguished name:

```
C:\>dsquery group -name "Employees"
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"
```

The group search base would be "DC=csc-lab,DC=example,DC=com."

You can also use the ADSI Edit program to browse the Active Directory structure (**Start > Run > adsiedit.msc**). In ADSI Edit, right click any object, such as an organizational unit (OU), group, or user, and choose **Properties** to view the distinguished name. You can then copy the string of DC values as the base.

To verify that you have the correct base:

- 1 Click the Test Connection button in the directory properties to verify connectivity. Resolve any problems, and save the directory properties.
- 2 Commit changes to the device.
- 3 Select **Components > Objects** and then **I want to > Add CX Identity Object**. Try to add known user and group names from the directory. You should see auto-complete suggestions as you type for matching users and groups in the realm that contains the directory. If these suggestions appear in a drop-down list, then the system was able to query the directory successfully. If you see no suggestions, and you are certain the string you typed should appear in a user or group name, you need to correct the corresponding search base.

Deleting Directory Realms or Directories

You can delete directories within a realm, or you can delete the entire directory realm. However, you cannot delete a directory realm if it is currently being used in a policy or policy object, or as the global realm for system users..

Procedure

Step 1 Select **Components > Directory Realm**.

Step 2 Do any of the following:

- To delete a directory server from a directory realm, mouse over the server name within the realm and click **Delete Directory**.

- To delete a directory realm, mouse over the name of the realm and click **Delete Realm**.

Configuring Identity Policies

Use identity policies to enable policies based on user identity, including username and user group membership. Identity policies never result in dropped or blocked traffic, even if the user fails to authenticate.

Instead, identity policies can prompt users to provide username/password when attempting to connect to a destination according to your matching criteria and authentication action. If the user fails authentication, the user's traffic is evaluated against your access rules and is permitted or denied based on those rules. If no passive authentication mapping is available for the IP address of the workstation the user is using, only the user's IP address is used for matching purposes, so any identity-based rules you create will not apply.

Thus, you might have an identity-based access rule that would allow traffic for UserA to ServerA, and disallows all other access to ServerA. If UserA successfully authenticates, the access rule will apply and UserA will be allowed to access ServerA. If UserA fails authentication, and there is no passive mapping, the access rule will not apply and UserA will not be allowed access to ServerA.

Tips

- By active or passive authentication, you can ensure that the user associated with a traffic flow is known, allowing identity-based access rules to function correctly, and providing user information in dashboards and events.
- Active authentication is applied to HTTP or decrypted HTTPS traffic only. If any other type of traffic matches an identity policy that requires or allows active authentication, then active authentication will not be attempted. Thus, it is not necessary to create Do Not Require Authentication policies for non-HTTP/HTTPS traffic. Likewise, it is not meaningful to create a policy that applies the Get Identity via Active Authentication action for traffic matching criteria that excludes HTTP traffic, for example, by selecting a service group that specifies ICMP as the only service type.
- Identity policies are applied based on first match for traffic matching criteria. Ensure that you define the matching criteria precisely so that the desired action, including the directory realm to use, is applied to each traffic class.

Before You Begin

You must create the directory realm before you can configure identity policies for the realm.

(Single Device mode only.) When you create the first directory realm, a default identity policy is automatically created for the realm. You can edit or delete the default policy to suit your needs.

Procedure

- Step 1** Select **Configurations > Policies/Settings** and open the **Identity Policies** tab.
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Do any of the following:
 - To add a new policy, use one of the **Add Policy** buttons. If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.

- To edit an existing policy, select the policy and click the **Edit Policy** button.
- To base a new policy on a similar existing policy, select the policy and click the **Duplicate Policy** button.

A form opens with the policy properties.

Step 3 Define the traffic matching criteria using the **Source**, **Destination**, and **Service** fields.

You can leave any field blank to not restrict traffic based on that criteria.

Step 4 Select the directory realm in the **Realm** field.

Step 5 Define the action to apply to matching traffic, including authentication type and user agents if necessary. For detailed information about the action-related settings, read [Identity Policy Properties](#), on page 236. Consider the following tips:

- The available options differ based on directory type and whether you configured a CDA or AD agent.
- If you select an option that allows for active authentication, either **Get Identity via Active Authentication** or **Get Identity Using AD Agent** with **Yes** selected for the active authentication question, you can exclude user agents from active authentication. Exclude agents that cannot respond to active authentication prompts, for example, software update applications.
- With active authentication, you also select the authentication method: basic or form (for all realm types), plus NTLM, Kerberos, or Advanced (AD only). Select the method supported by your server and clients; select Advanced if you support Kerberos, NTLM, and basic. If you have more than one AD realm, you can use NTLM, Kerberos, or Advanced with a single AD realm only; all other AD realms must use basic or form.

Note If you select **form**, you can customize the active authentication login form presented to the user on the End User Notification page (select **Administration** > **End User Notification**).

Step 6 If you want to limit the policy to traffic on specific interfaces on the parent device, select the **Source Interface Role** or the **Destination Interface Role**, or both, that identify the interfaces.

The default is to apply the policy to traffic between any interfaces on the device. If you select interfaces that do not exist on the device, the policy is never applied to traffic.

Step 7 Click **Save Policy**.

Step 8 If necessary, move the policy so that it is in priority order.

Policies are applied on a first-match basis, so you must ensure that policies with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

To move a policy set or rule, you click and hold the Move icon (the vertical double-headed arrow on the left margin) and drag it to the policy after which you want to insert it. You can also simply edit the sequence number and change it to the desired value.

Identity Policy Properties

Use identity policies on CX devices to define the user authentication requirements for matching traffic. Identity policies never result in blocked traffic. Instead, they determine whether user identity is obtained for the source IP address of a traffic flow.

Requiring authentication makes it possible to configure access policies based on user identity, and provides user-based usage information in dashboards.

Identity policies have the following properties:

Policy Name

The name of the policy. This name appears in Event Viewer for authentication events generated by traffic that matches this policy, so choose a name that will help you analyze event data.

Enable Policy: On/Off

Whether the policy is enabled. You can turn a policy off to temporarily disable it without deleting the policy. Disabled policies are never applied to traffic.

Traffic Matching Criteria

The traffic matching criteria that identifies the traffic to which the policy applies. To match the policy, the flow must match every specified property, that is, there is an AND relationship between the properties. Use the default Any selection if you do not want to restrict the policy based on that condition. Leave all fields with the default Any to match every possible traffic flow.

All of the following criteria are used to determine the traffic to which a policy applies.

- **Source**—A list of network groups. If a packet matches any selected object, it is considered to satisfy the source condition.
- **Destination**—A list of network groups. If a packet matches any selected object, it is considered to satisfy the source condition.
- **Service**—A list of service groups that define protocol and port combinations. If a packet matches any selected object, it is considered to satisfy the service condition.



Note

(Multiple Device mode.) When using PRSM in Multiple Device mode, you can also use network objects or groups defined on the device that contains the CX device for source or destination criteria, or ASA service objects for the service criteria. The network group objects come in two types: one that can be used on both ASA and CX devices, and one that can be used on CX devices only, which is explicitly called CX network group.

For information on how to select items, including how to add, edit, or remove them, filter the selection list, create or edit objects, or view object contents, see [Selecting Items](#), on page 27.

Realm

The directory realm used to authenticate traffic. If the user is prompted for authentication, servers in this realm are used to verify the credentials supplied by the user.

Action

The type of authentication required for matching traffic flows. The options differ based on the directory type and whether you configured a CDA or AD agent. Select one of these options based on availability:

Get Identity Using AD Agent

(AD with configured CDA or AD agent only.) If a passive user-to-IP address mapping was obtained from the CDA or AD agent, use it.

Select **Yes** or **No** for **Do you want to use active authentication if AD agent cannot identify the user?** If you select **Yes** (the default), and a passive mapping for the user's IP address was not obtained from the CDA or AD agent, the system tries to get identity through the client, either transparently (NTLM, Kerberos only) or by prompting the user to authenticate.

If you select **No**, and a passive mapping is not available, the user's IP address will not be associated with a user name, and identity-based access rules will not be applied to the user's traffic.

Get Identity via Active Authentication

(All directory types.) Obtain identity information even if a passive mapping exists for the user. Identity is obtained transparently if you use NTLM or Kerberos and the clients have the correct configuration; otherwise, users are prompted to authenticate.

Once authenticated, the user's IP address is considered a surrogate for the user, and the user is not required to reauthenticate for every subsequent connection. Reauthentication is required after the authenticated session duration setting is exceeded.

Do Not Require Authentication

(All directory types except AD with a CDA or AD agent configured.) Do not obtain user identity. Identity-based access rules will not be applied to the user's traffic.

**Note**

Active authentication is applied to HTTP or decrypted HTTPS traffic only. If any other type of traffic matches an identity policy that requires or allows active authentication, then active authentication will not be attempted.

Do you want to use guest access if active authentication cannot identify user?: Yes/No

If you select an option that requires or allows for active authentication, select whether users who fail active authentication are labeled as Guest users. These users will match the Guest Users identity object. You can write access policies to provide special handling for this category of user. These users appear in dashboards and events under the Guest user name.

If you select **No**, users who fail active authentication map to the Unknown Users identity object. You can also write access policies for unknown users.

Authentication Type

If you select an option that requires or allows for active authentication, select the authentication method to use during active authentication. You can use the following authentication methods; select one for which your directory servers are configured:

- **NTLM** (NT LAN Manager, AD realms only.). Supported by all Windows platforms.
- **Kerberos** (AD realms only). Supported for Windows XP only.
- **Basic**. This is the default. Supported on all platforms.
- **Advanced** (AD realms only). Select this option to allow the device to negotiate the method between the user agent (the application the user is using to initiate the traffic flow) and the Active Directory server. Negotiation results in the strongest commonly supported method being used, in order, Kerberos, NTLM, then basic.
- **Form**. This is a type of basic authentication, where the user is presented with a login browser page. You can customize the active authentication form on the End User Notification page (select **Administration > End User Notification**). Supported on all platforms.

If you allow for NTLM or Kerberos, clients can configure their browsers to allow for transparent authentication as described in [Enabling Transparent User Authentication, on page 241](#). Otherwise, users are prompted for their directory username and password.



Note

If you have more than one AD realm, you can use NTLM, Kerberos, or Advanced with a single AD realm only; all other AD realms must use basic or form.

Exclude User Agent

If you select an option that requires or allows for active authentication, you can exclude user agents (applications) that cannot respond to authentication requests, such as software update applications or remote access VPN clients that send authentication traffic through the VPN tunnel (such as Android 2.3 with AnyConnect 2.5). Select the user agent policy objects that identify the user agents (in the Include list in the object) that you do not want to prompt for authentication.

Interface Roles

The criteria that identifies the parent device's interfaces to which the policy applies. To match the policy, the traffic must enter the device on one of the source interfaces and leave the device on one of the destination interfaces. The default is any interface for both source and destination, meaning the policy is not restricted to specific interfaces.

To limit the policy to specific interfaces, select the appropriate interface role objects in either the **Source Interface Role** or **Destination Interface Role** fields, or both. The interface role objects define the interface names or naming patterns for the interfaces.



Tip

If you specify interface roles, and no interfaces on the device match the interface names defined in the role, the policy will never apply to any traffic on the device.

Tags

Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.

Ticket ID

A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)

Enabling Active Authentication

If you want to use active authentication, you need to address the following requirements:

- The class map for the traffic redirection policy on the ASA must include the `auth-proxy` keyword, for example **`cxsc fail-open auth-proxy`**.

If you configure redirection using PRSM, the keyword is automatically included.

- The default port used by the ASA for active authentication is `tcp/885`. You can configure a different port using the **`cxsc auth-proxy port number`** command using the ASA CLI. A non-default port must be higher than 1024. You can see the currently configured port using the **`show run all cxsc`** command.
- If there are firewalls between the ASA and the user, you must open the authentication port on those firewalls.
- Ensure that time settings are consistent among the directory servers, ASA CX, and clients. A time shift among these devices can prevent successful user authentication. “Consistent” means that you can use different time zones, but the time should be the same relative to those zones; for example, 10 AM PST = 1 PM EST.
- When using Active Directory with Kerberos authentication, the domain controller, ASA CX, and client must all be in the same domain, or authentication will fail. For NTLM and basic authentication, the devices should be in the domain, but authentication might work even if they are not in the same domain. Although NTLM is supported with all Windows clients, Kerberos is supported with Windows XP clients only.

To increase the likelihood of successful authentication, consider selecting **Advanced** as the authentication method. This will allow the system to negotiate the strongest method supported by both the client and server, and to try different methods if one fails.

- If you use Kerberos or NTLM with Active Directory, you can configure browsers to transparently respond to active authentication requests. For detailed information, see [Enabling Transparent User Authentication, on page 241](#).
- Not all user agents can successfully respond to active authentication requests. For example, if a user agent in a remote access VPN connection sends the authentication traffic through the VPN tunnel, active authentication will not succeed. Android 2.3 using AnyConnect 2.5 is an example of this type of agent. Software updaters might also not successfully respond to active authentication.

To account for these types of user agent, you can use an existing user agent object, or you can create a user agent policy object that lists these agents in the Include list. Then, in the active authentication identity policy, select the objects in the **Exclude User Agent** field.

- Users are prompted only if the traffic is HTTP or decrypted HTTPS. To prompt for HTTPS flows, you must create decryption policies that apply the Decrypt Everything action to the appropriate traffic sources.

Special Configuration Requirements for Remote Access VPN

If the ASA hosts remote access AnyConnect VPN connections, the active authentication prompt might not be displayed for certain clients. For example, Windows 7 Enterprise and Professional Editions, and Mac OS X 10.6.8, clients have this problem.

To enable active authentication prompting in these cases, you need to configure a split tunnel policy on the VPN access group to exclude the ASA's Internet IP address from the VPN. The following example shows what such a configuration would look like.

```
ASA-5525-3# show running-config interface
!
interface GigabitEthernet0/4
 nameif internet
 security-level 100
 ip address 10.194.204.37 255.255.255.0
!

ASA-5525-3# show running-config access-list
access-list Split_Tunnel_List standard permit host 10.194.204.37

ASA-5525-3# show running-config group-policy
group-policy test internal
group-policy test attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
 split-tunnel-policy excludespecified
 split-tunnel-network-list value Split_Tunnel_List
ASA-5525-3#
```

Enabling Transparent User Authentication

If you configure the identity policy for a realm to allow for active authentication, either **Get Identity via Active Authentication** or **Get Identity Using AD Agent** with **Yes** selected for the active authentication question, you can use the following authentication methods to acquire user identity:

Basic Authentication (Active Directory and LDAP)

With basic authentication, users are always prompted to authenticate with their directory username and password. The password is transmitted in clear text. For that reason, basic authentication is not considered a secure form of authentication.

Basic is the default authentication mechanism.

Form (Active Directory and LDAP)

This is a type of basic authentication, where the user is presented with a login browser page. You can customize the active authentication form on the End User Notification page (select **Administration > End User Notification**). Users are always presented with the login form.

Integrated Windows Authentication (Active Directory only)

With integrated Windows authentication, you take advantage of the fact that users log into a domain to use their workstation. The browser tries to use this domain login when accessing a server, or in the case of ASA CX, the network protected by the ASA CX. The password is not transmitted. If authentication is successful, the user is transparently authenticated; the user is unaware that any authentication challenge was made or satisfied.

If the browser cannot satisfy an authentication request using the domain login credentials, the user is prompted for username and password, which is the same user experience as basic authentication. Thus, if you configure integrated Windows authentication, it can reduce the need for users to supply credentials when accessing the network or servers in the same domain.

You must configure client browsers to support integrated Windows authentication to enable transparent authentication. The configuration is explained below.

When you configure an authentication policy, you select the specific type of authentication method used in your network. The options are:

- **NTLM.** Supported by all Windows platforms.
- **Kerberos.** Supported by Windows XP only.
- **Advanced,** where the strongest method allowed by both the Active Directory server and the user agent is used. (The user agent is typically a web browser through which the user is initiating a traffic flow.) The order of strength is Kerberos, NTLM, then basic.

The following sections explain the general requirements and basic configuration of integrated Windows authentication for some commonly used browsers that support it; users should consult the help for their browser (or other user agent) for more detailed information, because the techniques can change between software releases.



Tip

Not all browsers support integrated Windows authentication, such as Chrome and Safari (based on the versions available when this was written). Users will be prompted for username and password. Consult the browser's documentation to determine if support is available in the version you use.

Requirements for Transparent Authentication

Users must configure their browser or user agent to implement transparent authentication. They can do this individually, or you can configure it for them and push the configuration to client workstations using your software distribution tools. If you decide to have users do it themselves, ensure that you provide the specific configuration parameters that work for your network.

Regardless of browser or user agent, you must implement the following general configuration:

- Add the ASA interface through which users connect to the network to the Trusted Sites list. You can use the IP address or if available, the fully-qualified domain name (for example, asa_inside.example.com). You can also use wildcards or partial addresses to create a generalized trusted site. For example, you can typically cover all internal sites using *.example.com or simply example.com, trusting all servers in your network. If you add the specific address of the ASA interface, you might need to add several addresses to the trusted sites to account for all user access points to the network.
- Integrated Windows authentication does not work through a proxy server. Therefore, you must either not use a proxy, or you must add the ASA interface to the addresses excluded from going through the

proxy. If you decide that you must use a proxy, users will be prompted for authentication even if you use the NTLM or Kerberos methods.

**Tip**

Configuring transparent authentication is not a requirement, but a convenience to end users. If you do not configure transparent authentication, users are presented with a login challenge for all authentication methods.

Configuring Internet Explorer for Transparent Authentication

To configure Internet Explorer for both NTLM and Kerberos transparent authentication:

Procedure

Step 1 Select **Tools > Internet Options**.

Step 2 Select the **Security** tab, select the **Local Intranet** zone, then do the following:

- a) Click the **Sites** button to open the list of trusted sites.
- b) Ensure that at least one of the following options is selected:
 - **Automatically detect intranet network**. If you select this option, all other options are disabled.
 - **Include all sites that bypass the proxy**.

c) Click **Advanced** to open the Local Intranet Sites dialog box, then paste the URL you want to trust into the **Add Site** box and click **Add**.

Repeat the process if you have more than one URL. Use wildcards to specify a partial URL, such as `http://*.example.com` or simply `*.example.com`.

Close the dialog boxes to return to the Internet Options dialog box.

d) With **Local Intranet** still selected, click **Custom Level** to open the Security Settings dialog box. Find the **User Authentication > Logon** setting and select **Automatic logon only in Intranet zone**. Click **OK**.

Step 3 In the Internet Options dialog box, click the **Connections** tab, then click **LAN Settings**.

If **Use a proxy server for your LAN** is selected, you need to ensure that the ASA interface bypasses the proxy. Do any of the following as appropriate:

- Select **Bypass proxy server for local addresses**.
- Click **Advanced** and enter the address into the **Do not use proxy server for addresses beginning with** box. You can use wildcards, for example, `*.example.com`.

Configuring Firefox for Transparent Authentication

Firefox has different properties for NTLM and Kerberos authentication. The following steps explain the configuration for both methods. If you do not support both methods, skip the steps for the unsupported method.

Procedure

Step 1 Open **about:config**. Use the filter bar to help you locate the preferences that you need to modify.

Step 2 To support NTLM, modify the following preferences (filter on `network.automatic`):

- **network.automatic-ntlm-auth.trusted-uris**—Double-click the preference, enter the URL, and click **OK**. You can enter multiple URLs by separating them with commas; including the protocol is optional. For example:

```
http://host.example.com, http://hostname, myhost.example.com
```

You can also use partial URLs. Firefox matches the end of the string, not a random substring. Thus, you could include your entire internal network by specifying just your domain name. For example:

```
example.com
```

- **network.automatic-ntlm-auth.allow-proxies**—Ensure that the value is **true**, which is the default. Double-click to change the value if it is currently false.

Step 3 To support Kerberos, modify the following preferences (filter on `network.negotiate`):

- **network.negotiate-auth.allow-proxies**—Ensure that the value is **true**, which is the default. Double-click to change the value if it is currently false.
- **network.negotiate-auth.delegation-uris**—Double-click and enter `http://,https://`.
- **network.negotiate-auth.gsslib**—Ensure that the value is blank, which is the default. If this preference has a value, right-click it and select **Reset**, or double-click it and erase the value.
- **network.negotiate-auth.trusted-uris**—Double-click and enter `http://,https://`.
- **network.negotiate-auth.using-native-gsslib**—Ensure that the value is **true**, which is the default. Double-click to change the value if it is currently false.

Step 4 Check the HTTP proxy settings. You can find these by selecting **Tools > Options**, then click the **Network** tab in the Options dialog box. Click the **Settings** button in the Connection group.

- If **No Proxy** is selected, there is nothing to configure.
- If **Use System Proxy Settings** is selected, you need to modify the **network.proxy.no_proxies_on** property in `about:config` to add the trusted URIs you included in **network.automatic-ntlm-auth.trusted-uris** (or would have included, if you configured Kerberos only).
- If **Manual Proxy Configuration** is selected, update the **No Proxy For** list to include these trusted URIs.
- If one of the other options is selected, ensure that the properties used for those configurations exclude the same trusted URIs.

Identifying the Active Directory Agent

The Cisco Context Directory Agent (CDA) or Cisco Active Directory (AD) Agent provides user-to-IP address mappings to all devices that are configured to use it. For users who log into the network domain on your standard (non-VPN) network, the agent, in communication with the AD server, obtains the login information and creates a user-to-IP address mapping table. This information can be augmented by other devices in the network, such as the ASA, which can provide mappings obtained from VPN and direct sources. Identity mappings obtained from the AD agent are considered passive mappings.

Both the ASA and CX devices use the same CDA or AD agent setup to enable identity-aware firewall services. CDA replaces the older AD agent software, but the web interface uses “AD agent” to refer to either application.



Tip

Configuring a CDA or AD agent is optional. Configure it only if you want to support passive mappings. Note that if you do not support passive mappings, you must use active authentication in your identity policies or you will not have user names available for access control, and events and dashboards will not include user information.

Before You Begin

CDA and AD agent are separate software that you must install in your network. You must configure one of them to work with the Active Directory servers and with the network devices that are its consumer devices or clients. Before completing this task, install and configure the agent software.

Obtain the CDA or AD agent software from <http://www.cisco.com/go/asa>.

For information on setting up and configuring the software, see the following documents:

- CDA—*Installing and Configuring Context Directory Agent*, http://www.cisco.com/c/en/us/td/docs/security/ibf/cda_10/Install_Config_guide/cda10.html.
- AD Agent—*Installation and Setup Guide for the Active Directory Agent*, http://www.cisco.com/c/en/us/td/docs/security/ibf/setup_guide/ad_agent_setup_guide/ibf10_install.html

You must add the CX device as a consumer device (CDA) or client (AD agent), which you can do before or after you complete this procedure. Keep in mind that the RADIUS shared secret configured for the CX device on the CDA or AD agent and the one configured here must be the same.

Procedure

- Step 1** Select **Configurations > Policies/Settings** and open the **AD Agent** tab.
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Enter the following information:
 - **Hostname or IP**—The DNS name or IP address of the CDA or AD agent server.
 - **Password**—The RADIUS shared secret that is configured on the CDA or AD agent for use with this client device.
- Step 3** Click **Test** to check whether the agent can be contacted using the supplied information.

If the connection fails, check your settings. If you are certain they are correct, check whether there is a network path between the device and the agent.

- Step 4** If available, configure the secondary agent.
If you have a secondary agent configured for the device, click **Add Secondary CDA Agent**, fill in the address and password, and test the connection. If the primary becomes unavailable, the secondary will be used to obtain mappings. This provides a high-availability setup for the agent.
- Step 5** Click **Save** to save your changes.
-

What to Do Next

CDA or AD agent mappings are used only if you allow for passive mappings in the identity policies for the realm that contains the AD servers that are also clients of the agent. Thus, you should check your identity policies to ensure they specify **Get Identity Using AD Agent**. If your policies use **Get Identity via Active Authentication**, then the passive mappings are not used.

Ensure that you define directory realms for each AD domain for which the agent collects identity information.

Configuring Authentication Settings

You can configure authentication settings related to how your identity policies function.

Procedure

- Step 1** Select **Configurations > Policies/Settings** and open the **Auth Settings** tab.
(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Change the following options as needed:
- **Authenticated session duration**—The number of hours for which a user-to-IP address mapping will be maintained. When a mapping reaches this age, it is deleted and a new mapping is obtained based on your identity policy settings. For example, if you use active authentication for the realm that matches the user's IP address, the user will be authenticated during the user's next connection attempt. However, if your policy uses passive mappings and does not allow for active authentication, the user will not be authenticated.
 - **Failed authentication timeout**—If a user fails to correctly authenticate during active authentication, and exceeds the maximum authentication attempts, the IP address for the user is considered to have failed authentication. This timeout value determines the length of time, in minutes, before the user at that IP address is again prompted to authenticate. During this time, all traffic from the IP address is evaluated based on the IP address alone, and no user or user group based rules are applied to the traffic. Thus, during this failed timeout period, a user might be prevented from accessing resources for which the user would be allowed if the user had successfully authenticated.
 - **Maximum authentication attempts**—The number of times a user can retry authentication when prompted to authenticate by ASA CX. The number of attempts is reset when the user successfully authenticates. If the user fails to authenticate, the user is not again prompted for authentication until the failed authentication timeout is exceeded.

- **Group refresh interval**—How often user group membership is updated from the directory servers, in hours. The default is every 24 hours (once a day). If you add a user to a group, the user is not recognized as being a member of the group until the next update. Membership for a group is obtained only if you use the group in a policy.
- **Guest user access timeout**—If a user fails active authentication and becomes a guest user, the length in time, in hours, that the user will remain a guest. After the timeout is passed, the user will again be prompted to authenticate. There is no limit to how often the user can be a guest.

Step 3 Click **Save** to save your changes.



Controlling Network Access with Context-Aware Access Policies

The following topics explain how to use context-aware access policies on CX devices to control access to the network.

- [Overview of Context-Aware Access Policies, page 249](#)
- [Configuring Context-Aware Access Policies, page 250](#)
- [Notifying Users of Blocking Policies, page 259](#)
- [URL and Application Filtering, page 266](#)
- [Web Reputation Filtering \(Malware Protection\), page 273](#)
- [Next Generation IPS Filtering, page 276](#)
- [Configuring Signature and Engine Updates, page 279](#)

Overview of Context-Aware Access Policies

The context-aware access policy is the primary policy for implementing acceptable use policies through a CX device. Use context-aware access policies to supply the following services:

- Traditional access control based on the source and destination IP addresses, protocols, and ports for a traffic flow.
- Identity-based access control to allow or deny access based on the user requesting the access, regardless of which IP address the user is currently using. You can enforce identity-based access control by specifying user groups rather than individual users, so that a user is provided access based on group membership.
- Application-based access control to allow or deny specific applications or general types of application. Because some undesirable applications can change port usage, using traditional service definitions of protocol and port is not always effective. Through inspection, the application used in a traffic flow can frequently be determined. Thus, you can write policies based on application names such as Facebook or LinkedIn, making your policies easier to understand and evaluate.

Some applications have multiple behaviors that you can selectively allow or deny. For example, you could allow Facebook but deny posting to Facebook.

- Client-based access control to allow selective access based on the HTTP user agent being used to initiate a traffic flow (for example, web browsers) or for remote access VPN users, the operating system of their client.
- URL filtering to prevent access to undesirable web sites. You can control access to specific URLs or to entire web site categories, such as Gambling web sites.
- Warning policies to notify users that access to certain sites is against policy, without overtly denying access to those sites. Users can click a link to continue to the site. (Works with HTTP and decrypted HTTPS only; all other traffic is simply allowed.)
- Web reputation filtering to prevent access to web sites that have low public reputation scores. By filtering on reputation, you can allow access to an otherwise high-reputation web site while preventing advertisements or other material on the site hosted from external low-reputation sites. Thus, users might see pages with empty boxes where the low-reputation information would have appeared.
- File transport control to selectively deny the uploading or downloading of files based on MIME type. For example, if you have a high-security zone in your network, you might want to prohibit all file uploads from that zone.
- Next Generation IPS filtering to compare the traffic contents against attack threats. If a connection matches a threat, you can drop the connection to block the threat. You can also choose to monitor but allow, or completely ignore, threats that you decide are benign.
- Rate limiting (also called policing) to ensure that no traffic exceeds the maximum rate that you configure, thus ensuring that bandwidth-intensive traffic flows cannot take over all resources.
- Safe Search enforcement to prevent users from relaxing search engine controls to include inappropriate or explicit results for searches.
- Header injection to add headers to HTTP Request messages to web sites that support the header. Injecting a header can provide you with specialized handling of requests to those sites.

Default Context-Aware Access Policy Behavior

If a traffic flow does not match any of your access policies, an implicit action is applied to the flow. All non-matching traffic flows are **allowed without condition** by default. This default policy is named Implicit Allow when it appears in dashboards or events.



Note

The default context-aware access policy behavior is the exact opposite of traditional firewall access policies. For example, the ASA denies any traffic flows that do not match an allow rule in the global or interface-specific access policies.

It is best practice to create an explicit rule that defines the action to apply to non-matching traffic flows. Place the policy last in the access policy set. If desired, you can apply the Deny action instead of the Allow action. For traffic matching conditions, use the default Any for source, destination, and application.

Configuring Context-Aware Access Policies

Use context-aware access policies to control access to network resources. You can control access based on:

- Traditional 5-tuple characteristics such as source and destination IP addresses, protocol, and ports.
- The user who is making the request, or the user groups in which the user is a member.
- The application that is being used. You can also control access for generalized application types.
- The HTTP client type being used to make a request (such as the browser type), or the operating system of a VPN client.
- The destination URL of a web request, including the generalized category of the URL.

When you create an access policy that allows network access, you can limit the allowed activity by applying Next Generation IPS filtering, by selectively prohibiting the uploading or downloading of certain types of files, or by disallowing access to web sites that have poor public reputations.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and open the **Access Policies** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Tip** In Multiple Device mode mode, this tab includes access policies for both the CX device and the parent ASA. Click **Context-Aware Policies** to ensure that you are working in the CX access policy section.
- Step 2** Do any of the following:
- To add a new policy, use one of the **Add Policy** buttons. If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.
 - To edit an existing policy, select the policy and click the **Edit Policy** button.
 - To base a new policy on a similar existing policy, select the policy and click the **Duplicate Policy** button.
- A form opens with the policy properties.
- Step 3** Select the policy action to apply to matching traffic.
- **Allow**—Allow the traffic subject to the profile and application behavior settings in the policy.
 - **Warn**—For HTTP and decrypted HTTPS connections, display a warning notification to advise the user that access to the site is not recommended. The user can click a link to continue with the connection. Thus, the connection is initially denied, but potentially allowed. Any non-HTTP/decrypted HTTPS traffic is simply allowed.
 - **Deny**—Drop the traffic unconditionally.
- Step 4** Define the traffic matching criteria using the **Source**, **Destination**, and **Application** fields. You can leave any field blank to not restrict traffic based on that criteria. See the reference topic for detailed information about each field, but consider the following tips:
- If you need to create very complex source or destination criteria, use the source and destination object groups. These objects allow complex combinations of other objects to precisely define traffic flows.
 - To implement URL filtering, use URL objects in the destination criteria. You can use URL categories to control access to all web sites that provide a particular type of service. For example, you could disallow all gambling web sites by using the Gambling category without needing to know the URLs for every

gambling site. You could also set up a URL object to disallow a category, but exclude specific web sites within the category that you do want to allow.

- To implement application control, specify criteria in the Application field. You can control applications based on types or tags, which apply to all applications thus classified, or you can control specific applications, including application services that you define yourself. When use application specifications, you can control access without limiting the control to specific ports.

Note Some applications, such as Facebook and LinkedIn, allow granular control of specific application behaviors. These behaviors appear when you select an item that includes applications with controllable behaviors.

Step 5 If desired, configure the time range for the policy.

If you specify a time range object, traffic can match the policy during the specified times only. Outside the time range, the policy is not in effect and traffic that would match the policy is compared to subsequent policies. The local time on the device is used.

Step 6 (Optional) Unless the policy action is **Deny**, you can also configure the following profiles to selectively disallow actions:

- **Bandwidth Limit**—The maximum bandwidth to allow each traffic flow that matches this policy, from 1 Kbps to 4000 Mbps. You can specify the limit in **Mbps** or **Kbps**, select the appropriate measure.
- **Safe Search: On/Off**—Whether to enforce Safe Search for search engine or other supported content search requests. By enforcing Safe Search, you prevent users from relaxing search engine settings, ensuring that you filter out inappropriate or explicit content from search results. The default is **Off**, which allows users to configure the search engine as desired.
- **File filtering**—You can select a profile object that defines file MIME types that should not be downloaded or uploaded.
- **Web reputation**—You can select a profile object that defines the public reputation score range that should be blocked. Use this to protect against malware. To use the device level profile, select **Device Level Profile (name)**; the name of the profile configured is shown in the option. The pre-defined system object **Default web reputation profile** implements the recommended blocking of sites with reputation scores from -10 to -6.
- **NG IPS**—You can select a profile object that defines the Next Generation IPS filtering policy to apply. If you do not select a profile, no filtering is applied. To use the device level profile, select **Device Level Profile (name)**; the name of the profile configured is shown in the option. The pre-defined system object **Default NG IPS profile** implements the recommended policy.
- **Header Injection**—You can select a profile object that defines a header to inject into HTTP Request messages sent to web sites that support the header, for example, YouTube for Schools. Injecting a header can provide you with specialized handling of requests to those sites. You must ensure that the destination for the policy includes at least the web sites that support the header. Headers are not injected into requests to non-supporting sites.

Tip You can see whether intrusion prevention (Next Generation IPS filtering) and malware protection (web reputation) are on or off for the device by looking at the status information above the access policy list. Mouse over the On/Off indication to see details about the device-level profile for each feature. There is an **Edit Settings** link in the popup to open the settings tab for the feature, where you can change the status and profile.

Step 7 If you want to limit the policy to traffic on specific interfaces on the parent device, select the **Source Interface Role** or the **Destination Interface Role**, or both, that identify the interfaces. The default is to apply the policy to traffic between any interfaces on the device. If you select interfaces that do not exist on the device, the policy is never applied to traffic.

Step 8 Click **Save Policy**.

Step 9 If necessary, move the policy so that it is in priority order. Policies are applied on a first-match basis, so you must ensure that policies with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

To move a policy set or rule, you click and hold the Move icon (the vertical double-headed arrow on the left margin) and drag it to the policy after which you want to insert it. You can also simply edit the sequence number and change it to the desired value.

What to Do Next

Analyze the activity of the policy. When viewing the policies list, each policy includes hit count information, which is linked to the detailed Policy Hits dashboard for the policy. You can also access the Policy Hits dashboards directly by selecting **Dashboard > Policies**.

Context-Aware Access Policy Properties

Use context-aware access policies on CX devices to control access to the network.

Access policies have the following properties:

Policy Name

The name of the policy. This name appears in dashboards and Event Viewer for data and events generated by traffic that matches this policy, so choose a name that will help you analyze dashboard and event data.

Enable Policy: On/Off

Whether the policy is enabled. You can turn a policy off to temporarily disable it without deleting the policy. Disabled policies are never applied to traffic.

Policy Action

One of the following:

- **Allow**—Allow the traffic subject to the profile and application behavior settings in the policy.
- **Warn**—For HTTP and decrypted HTTPS connections, display a warning notification to advise the user that access to the site is not recommended. The user can click a link to continue with the connection. Thus, the connection is initially denied, but potentially allowed. Any non-HTTP/decrypted HTTPS traffic is simply allowed.
- **Deny**—Drop the traffic unconditionally.

Eventing: On/Off

Whether traffic flows that match the policy will generate events and dashboard data. The default is **On**. If you turn off eventing, traffic that matches this policy will not be reflected in dashboards, and you will not see events for the flows in Event Viewer.

Capture Packets: On/Off

Whether to capture packets for flows that match this policy, if, and only if, the match criteria for the policy are limited to Layer 3/Layer 4 (L3/L4) criteria (network objects, service objects) or they use the default Any. The packet capture default is **Off**. All packets are captured, so carefully consider traffic volumes for matching flows before enabling packet capture.

Packets are not captured for policies that use any criteria other than L3/L4 criteria, even if you enable packet capture.

The packet capture file is not written to disk until you turn off packet capture. To upload packet captures to a server, log into the system CLI and use the **support diagnostic** command.

For more detailed information on how to capture packets, see [Capturing Packets](#), on page 378.

Traffic Matching Criteria

You can create complex traffic matching criteria to define precise policies. To match the access policy, the flow must match every specified property, that is, there is an AND relationship between the properties. Use the default Any selection if you do not want to restrict the policy based on that condition. Leave all fields with the default Any to match every possible traffic flow.

The **Source**, **Destination**, and **Application/Service** criteria are used to determine the traffic to which a policy applies. For information on how to select items, including how to add, edit, or remove them, filter the selection list, create or edit objects, or view object contents, see [Selecting Items](#), on page 27.

Source

A list of policy objects of the following types: network group (IP addresses), identity (user or user group names), user agent (the type of client application that is making a web request), Secure Mobility (type of remote access VPN client), or source object group (a collection of objects in complex AND/OR relationships that you cannot define directly in a policy). If a packet matches any selected object, it is considered to satisfy the source condition.

**Note**

(Multiple Device mode.) When using PRSM in Multiple Device mode, you can also use network objects or groups defined on the device that contains the CX device for source or destination criteria, or ASA service objects for the service criteria. The network group objects come in two types: one that can be used on both ASA and CX devices, and one that can be used on CX devices only, which is explicitly called CX network group.

Destination

A list of policy objects of the following types: network group, URL (URLs or web categories), or destination object group (a collection of objects in complex AND/OR relationships that you cannot define directly in a policy). If a packet matches any selected object, it is considered to satisfy the destination condition.

If you disable the URL filtering feature, or you do not have a valid Web Security Essentials license, you cannot use URL objects in this field or in a destination object group.



Tip When configuring URL objects for access policies, be aware that paths cannot be matched for encrypted traffic (where a decryption policy did not decrypt the flow) or for any decrypted flow that is not HTTPS; in these cases, the access policy matches URLs that specify a domain name only.

Application/Service

A list of applications, application types, application tags, application objects, service groups (protocol and port combinations), or application service objects (which define an application based on a combination of service and application specifications). Because traffic is inspected, the application for a traffic flow can often be determined regardless of the port used by the flow; you can create rules directed to a specific application or application type by name rather than trying to predict the ports used. If a packet matches any selected application specification, it is considered to satisfy the application condition.



Tip If you disable the Application Services feature, or you do not have a valid Application Visibility and Control license, this field is named Services and you are limited to using service objects and groups.

Some applications have multiple application behaviors. For example, Facebook includes behaviors such as Post and Tag, categorized by Facebook areas or features, such as Events, General, Messages, Notes, Photos, and Places. If you specify an application type that has multiple behaviors in an access policy whose action is not Deny, you have granular control over these behaviors, so that you can in general allow the application type, but deny specific behaviors. For example, you could allow Facebook posting, but not allow the upload of photos or message attachments.

If you select applications that include multiple behaviors, the **Set Application Behaviors** control appears beneath the Application box. Each behavior is listed separately. You can do the following to control the specific behaviors:

- To change the settings for all behaviors at once, select **Allow All** or **Deny All** for **Set Global Behavior To**. These options provide a shortcut for changing the Allow/Deny setting throughout the behaviors list. For example, if your intention is to deny most behaviors, but allow a few, you can select **Deny All** initially, then change the desired behaviors to Allow. The default is to allow all application behaviors.
- To change the setting for an individual behavior, click the **Allow/Deny** field to show the desired option. The Allow/Deny field appears only if you change the overall policy action to Allow.

Shared/Local

(Multiple Device mode only.) The devices on which to configure this policy. If you leave this field blank, the policy is configured on all devices that share the policy set that contains the policy. If you want to limit this policy to a subset of the devices that share the policy set, select those devices here; the policy will not be configured on any unlisted devices that otherwise share the policy set. The devices available for selection are constrained to those that currently share the policy set.

For example, you can use this setting to create a handful of policies specific to a device that otherwise should use the same policies as a group of devices.

Time Range

A time range object that defines the times when this policy will be active, as evaluated by the device's local time. If you do not select an object, the policy is always active. If you select an object, the policy is active during the specified times,

Profile

Unless you select Deny for Policy Action, you can optionally select profile options to implement acceptable use policies. Using profiles, you can drop certain types of traffic that is otherwise allowed:

- **Bandwidth Limit**—The maximum bandwidth to allow traffic that matches this policy, from 1 Kbps to 4000 Mbps. You can specify the limit in **Mbps** or **Kbps**, select the appropriate measure.
- **Safe Search: On/Off**—Whether to enforce Safe Search for search engine or other supported content search requests. By enforcing Safe Search, you prevent users from relaxing search engine settings, ensuring that you filter out inappropriate or explicit content from search results. The default is **Off**, which allows users to configure the search engine as desired.
- **File Filtering**—A profile object that determines which types of files users can upload or download.
- **Web Reputation**—A profile object that determines which traffic is dropped based on the web reputation of the traffic. If you do not select a profile, no filtering is applied. To use the device level profile, select **Device Level Profile (name)**; the name of the profile configured is shown in the option. The pre-defined system object **Default web reputation profile** implements the recommended blocking of sites with reputation scores from -10 to -6.
- **NG IPS**—A profile object that defines the Next Generation IPS filtering policy to apply. If you do not select a profile, no filtering is applied. To use the device level profile, select **Device Level Profile (name)**; the name of the profile configured is shown in the option. The pre-defined system object **Default NG IPS profile** implements the recommended policy.
- **Header Injection**—A profile object that defines a header to inject into HTTP Request messages sent to web sites that support the header, for example, YouTube for Schools. Injecting a header can provide you with specialized handling of requests to those sites. You must ensure that the destination for the policy includes at least the web sites that support the header. Headers are not injected into requests to non-supporting sites.

Interface Roles

The criteria that identifies the parent device's interfaces to which the policy applies. To match the policy, the traffic must enter the device on one of the source interfaces and leave the device on one of the destination interfaces. The default is any interface for both source and destination, meaning the policy is not restricted to specific interfaces.

To limit the policy to specific interfaces, select the appropriate interface role objects in either the **Source Interface Role** or **Destination Interface Role** fields, or both. The interface role objects define the interface names or naming patterns for the interfaces.



Tip If you specify interface roles, and no interfaces on the device match the interface names defined in the role, the policy will never apply to any traffic on the device.

Tags

Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.

Ticket ID

A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)

Warning Users of Undesirable Sites

You can use Warning access policies to notify users when they try to access sites that you deem undesirable. For HTTP, or decrypted HTTPS, connections that match a warning policy, the connection is initially denied, and the Warning end-user notification page is shown. After reading your message, the user can elect to click a link that will continue to the site. Thus, Warning policies initially result in a deny action, but can be coupled with an allow action. In Event Viewer, the deny reason indicates that a user acceptance to a warning is pending in these cases. An HTTP Complete message with Yes in the User Accepted Warning field indicates that the user continued to the site.

Because the user must be shown an HTML warning page, warning policies make sense for browser-hosted HTTP/HTTPS traffic only. Thus, a warning policy should use a URL object in the destination. It would make no sense, for example, to apply the Warn action to a rule for GRE traffic. Specifically:

- HTTP/HTTPS traffic that cannot be shown a warning is dropped. That is, traffic for web-based applications that are not hosted in a browser will typically be dropped. Thus, Warning policies are not good choices for application filtering.
- All non-HTTP or non-decrypted HTTPS traffic that matches a Warning policy is simply allowed.

You can modify the Warning end-user notification page to explain your organization's acceptable use policies.

Limitations for Warning Policies

If a user clicks the link to continue to a site, the system tracks the acceptance based on the user's IP address and the warning policy, but not the destination. Subsequent traffic from that IP address that matches the policy will be allowed without warning until the acceptance times out after 8 hours. This method of tracking has the following implications when the user accepts the warning:

- If you use NAT to map multiple addresses to a single IP address, the first user who accepts a warning will accept it for all users. Subsequent users who try to access a site you are warning against will not see the warning.
- If you use web categories in the warning policy, the user accepts the warning for all sites in that category. Thus, if the user goes to Gambling Site A and accepts the warning, the user will not see a warning for Gambling Site B.
- If you specify more than one web category in the warning policy, the user accepts the warning for all categories at once. Thus, if you create a warning policy for Gambling and Games, if the user goes to Gambling Site A and accepts the warning, the user will not see a warning for Gaming Site B.

Recommendations for Warning Policies

There is a single Warning end-user notification page that you can customize. You can use this page to list all web categories and applications that you are warning against.

When configuring the warning policies, you have two main strategies that you can employ:

- 1 Create a single policy that includes all border-line sites. This is the simplest method, but if you specify more than a single site or category, if the user accepts the warning for one, the user accepts it for all. The user might not be warned for every border-line access attempt.
- 2 Create a separate warning policy for each site or category. Depending on how many sites and categories fall in your border-line area, this can bloat your policy list. However, it will increase the chances that the user will be warned for every questionable access attempt. You will also be able to track the volume of access attempts for each category based on policy hit counts.

Applying Rate Limits (Policing)

Rate limiting, also called policing, is a way of ensuring that no traffic exceeds the maximum rate (in bits/second) that you configure, thus ensuring that bandwidth-intensive applications cannot take over all resources. When traffic exceeds the maximum rate, CX drops the excess traffic.

To apply a rate limit, you enter a value in the **Bandwidth Limit** field, under **Profile**, in a CX Context-Aware access policy. You can specify the limit in **Mbps** or **Kbps**; ensure that you select the right measure.

For example, you could create access policies to apply a 50 Kbps rate limit for any of the following:

- In **Application/Service**, select the File Sharing, iTunes, and Social Networking application types.
- In **Destination**, select a URL object that specifies high bandwidth categories, such as Entertainment, Games, Streaming Audio, and Streaming Video.
- In **Source**, select an identity object that specifies user groups whose access should be constrained.

All concurrent traffic flows that match the policy will have the limit applied collectively. The limit does not affect flows that match other access policies. Events for matching flows will indicate that a limit was applied.

Be aware that you can also configure policing rate limits and other Quality of Service (QoS) settings on the ASA. If you apply rate limits in both devices, the actual maximum limit might be lower than the limit you configure in the access policy. Additionally, the ASA rate limit might apply to traffic that you are not trying to limit in CX.

Enforcing Safe Search

Many search engines and other content-heavy web sites, such as Google and Yahoo, provide a feature called *Safe Search*. With Safe Search, you can configure the site to filter out inappropriate or explicit results from a search request. Each site uses different terminology for this search option, such as Google's "Filter Explicit Results" or Yahoo's "Filter out adult Web, video, and image search results."

Because Safe Search is optional, a user can turn it off and get unfiltered results. This might be undesirable in your organization, especially when the search results contain images that could easily be seen by other people. Thus, you might want to use your CX Context-Aware access policies to enforce Safe Search.

To enforce Safe Search, you simply select **Safe Search: On** in the Profile section of a CX Context-Aware access policy. Use the Source and Destination fields to tailor the policy to the users and networks that need Safe Search enforcement.

When enforcing Safe Search, CX implements strict blocking, not moderate blocking. The HTTP inspector will modify search URLs to include the required string, or modify the HTTP header, based on the implementation used by the targeted search engine. If CX does not support a particular search engine, all user access to that engine will be denied for traffic flows that match a Safe Search-enabled policy.

Keep the following tips in mind when enforcing Safe Search:

- If CX must rewrite the user's search URL, the Safe Search column in traffic events will say Yes.
- If CX does not support a search engine, users will see a notification that the site is blocked, and you will see an HTTP Deny event.
- Safe search enforcement will apply to an HTTPS site only if you have a decryption policy that decrypts the traffic. If the traffic is not decrypted, the search URL cannot be rewritten.
- For a list of supported sites, see the release notes, <http://www.cisco.com/c/en/us/support/security/asa-next-generation-firewall-services/products-release-notes-list.html>.

Notifying Users of Blocking Policies

When you create access policies that deny traffic flows, end users are blocked from the destination. You might want to make public your general policies, especially if you implement URL filtering or selective blocking of applications or application behaviors. For example, if users know beforehand that you are blocking access to all gambling web sites, or to Facebook, they will not try to access those sites and will not be surprised if they are blocked if they do try.

The following topics explain end user notification and how to configure your own notification pages.

When Are Notifications Sent?

In many situations, the CX device will show an end user notification page when blocking web destinations in the user's browser. This notification indicates that your organization's policies block access to the resource.

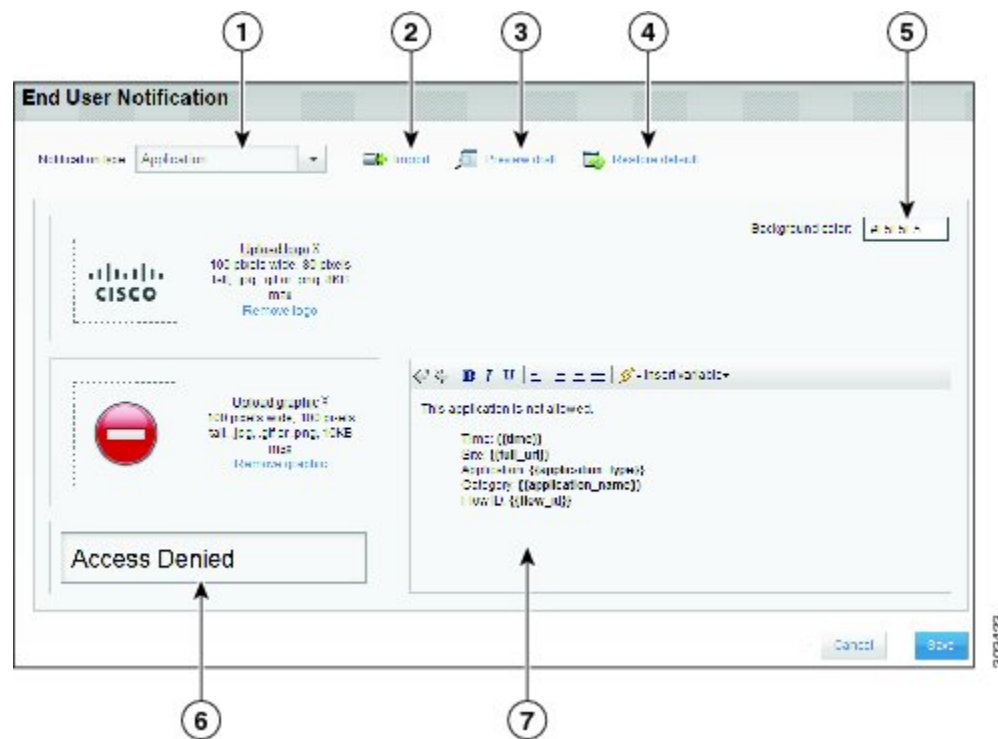
Showing an end user notification page is not always possible. Users should typically see the notification if they are trying to open a standard URL to a web destination, and you are broadly applying blocking to the web site. However, notification is not always possible. The following list explains some of the situations in which users will be blocked from a resource without getting a notification:

- Notifications are never sent for non-web traffic, that is, users might see notifications only if they are accessing an HTTP or HTTPS resource.
- Notifications are never sent if the destination is denied because the transaction matches a Next Generation IPS threat that you are blocking.
- If you deny access based on IP address, user name, or user group membership, no notifications are sent.
- For warning policies, notifications are shown regardless of what elements the traffic matches, including IP address, username, user group membership, URLs, applications, and so forth. HTTP/HTTPS traffic for which notifications cannot be displayed is blocked, but non-HTTP/HTTPS traffic is simply allowed.
- If you deny access to a site that is a Web 2.0-style application, where the site gives the appearance of a self-contained application rather than a standard web page, it is very likely that users will not see notifications. This occurs because the web site is using Javascript to control the user experience, and instead of loading new pages, often uses AJAX calls to update content without changing the URL. The device can recognize requests for application behaviors that you have denied, but cannot insert a user notification into the site's Javascript.
- Some policies result in "late" verdicts on whether the flow will be allowed or denied. To ensure good network performance, the device might send some of a traffic flow to the destination before determining that the flow should be denied. This can happen when you have policies that block file uploads or downloads, or that block flows based on application specifications. If the flow is eventually denied after an initial response from the destination has been received, the flow is dropped mid-stream and no notification is possible.
- The order of your access policies matter. If a traffic flow matches a deny policy that is low in the access policy set, and policies higher in the policy set require additional analysis to determine if a flow matches (for example, policies that specify application criteria), the deny verdict might come late, after part of the flow has already been sent and an initial response received. Because policy sets are analyzed on a first match basis, you should always put more specific policies above more general policies. You should also put simpler policies, such as URL filtering, above more complex application filtering policies.

End User Notifications Page

Use the end user notification feature to customize the pages shown to users when you deny, or warn against, access to a site. You can create different notifications for the different types of reasons you might be blocking access. The following image and text explains the basics of using this page.

Figure 16: End User Notification Page



The following points explain the image call-outs.

(1) Notification Type

You can configure different notifications based on the reason for denying access to a resource. If more than one deny reason applies to a traffic flow, the notification used is based on the following priority. (The Warning notification is always shown for warning policies.)

- Web reputation—The traffic violated the allowed reputation range defined in the web reputation profile attached to policy.
- File type—A file in the traffic flow was not allowed based on the file filtering profile attached to the access policy.
- URL filtering—The destination web site was not allowed. This might happen based on URL or based on the web category of the site.
- Application—The traffic flow was for an application or application behavior that is not allowed.
- Destination—The traffic flow was for a site that is not allowed for some other reason. This might include denying site access based on source criteria, such as user identity, user group membership, and so forth. This message is shown if no other message fits the deny reason.
- Warning—The traffic matched a policy with the Warn action. The notification page will include a link that allows the user to continue to the undesirable site.
- Authentication—The traffic matched an identity policy that uses the “form” authentication method. This page prompts the user for username and password.

(2) Import

Click this button to import your own HTML file for the selected notification type.

(3) Preview Draft

Click this button to see how the message you are editing will appear to users. Sample values are used for variables.

(4) Restore Default

Click this button to return the message you are editing to the system default. You are shown the default message and asked to confirm your decision; click **Restore** to complete the action.

(5) Background Color

The hexadecimal number that represents the background color for the notification panel. Click in the box to open a color palette and click the color you want, or edit the number directly if you know the desired value. If you edit the number, click outside the box to complete your change.

(6) Left Pane of Message

From top to bottom, the left pane of the end user notification message contains the following items:

- Logo image—Click **Upload Logo** to add your own organization's logo. The page explains the image limits. You can click **Remove Logo** if you do not want a graphic.
- Action image—An image that indicates action you are taking. Click **Upload Graphic** to add your own image, or click **Remove Graphic** if you do not want one.
- Message headline—A text message that indicates the action you are taking.

(7) Right Pane of Message

The detailed part of the message. Editing controls across the top let you manipulate the message. The controls and elements of the pane are:

- Undo, Redo buttons—You can cycle through your changes to undo and redo them when necessary.
- B, I, U—Bold, italicize, or underline text.
- Right, left, center, or justify text alignment.
- Chain link—Enter a hyperlinked URL. You are prompted for the URL and the text for the link. Click **Set** to add the link at the cursor position.
- Insert variable—Insert a system variable at the cursor position. The value assigned to the variable for the denied traffic flow will be presented to the end user. Variables are enclosed in double braces, `{{variable_name}}`.
- View HTML Source <> button—Toggle the message body view between formatted and source code. Viewing the source code can help you design custom pages, and in some cases, makes it easier to update a page.
- Message body—Type in the message body box. Use the Tab/Reverse Tab key to add or remove indents.

Customizing End User Notifications

You can change the notifications shown to end users when they are denied access to a web page, or warned against accessing the site. You can customize the pages by editing the pre-defined notifications, or you can import your own HTML to use as the notification page.

The following topics explain how to change the notification pages.

Editing End User Notifications

You can edit the pages shown to users when you deny, or warn against, access to a site. There are different pages for each denial reason.

Procedure

Step 1 Select **Administration > End User Notification**.

For detailed information about this page, including the available notification types, see [End User Notifications Page](#), on page 261.

Step 2 Select the type of notification you want to edit from the **Notification Type** list.

Step 3 Make your edits.

Following are some tips for editing the notification messages:

- The toolbar above the right pane lets you manipulate some characteristics of the text. You can also use the Tab/Reverse Tab key to manage text indentation.
- Click the View HTML Source <> button to toggle between formatted and source code views. In some cases, making your edits to the source code is easier.

- You can upload your own images for the logo and action image shown on the notification. The web interface explains the size and file type limitations for the images.
- Use the hypertext link button to build links to your internal help or acceptable use policy pages.
- Insert variables to show the user detailed information about the traffic flow you are denying. Because the denial might be to part of a page and not the entire page, the user might not be aware that the site being visited pulls information from unacceptable sites.
- Click **Preview Draft** to see what your edits will look like.
- If you want to start over, click **Restore Default**.

Step 4 Click **Save**. You need to save your edits for each notification type. Repeat the process to edit additional messages.

Importing End User Notifications

Instead of editing the pre-defined notification pages, you can create your own page and import it into the application. By importing pages, you can create more complex pages than possible using the editor.

You cannot edit the imported file. If you need to make changes, edit your original file and import it again.

Before You Begin

Create a separate HTML page for each notification type you intend to replace. Although you can import plain text, the application expects HTML, and you probably will not get good results unless you insert the desired markup tags.

Following are some tips about how to configure the HTML file for a notification page:

- The file should include complete, valid HTML markup, including the `<html>` container tag. We suggest that you use an HTML editor to generate the appropriate markup. Test the file in a browser before importing it to ensure that you get the desired presentation.
- For the authentication page, you must have input boxes for the username and password. The following code is the minimum requirement:

```
<form enctype="text/plain" method="POST" name="loginform" id="loginform">
<input type="text" name="name" id="name"/>
<input type="password" name="pass" id="pass"/>
</form>
```

- Insert whatever CSS styles you require directly into the HTML file.
- Although you can use an `<img>` tag to refer to an image that resides on a web server, it is possible your policies will prevent access to the server for some users. If you want to include images, and ensure that the image is always available for all users, you can generate the base64 encoding for the image and insert it in the following markup. This example assumes a PNG graphic, but you can use JPEG or other graphic types supported by browsers if you adjust the image media type declaration.

```
<div
  class="class_name"
  style="background-image: url
```

```
(data:image/png;base64,insert-string-here)">
</div>
```

Procedure

- Step 1** Select **Administration > End User Notification**.
For detailed information about this page, including the available notification types, see [End User Notifications Page, on page 261](#).
- Step 2** Select the type of notification you want to import from the **Notification Type** list.
- Step 3** Click **Import**.
- Step 4** In the Import EUN File popup, click **Browse** and select your HTML file.
- Step 5** Click **Upload**.
If the file includes acceptable content, it is uploaded and shown, and the message “Upload Successful” appears at the bottom of the page. You can click **Preview Draft** to verify it will appear to end users as expected.
If the results are not acceptable, click **Do Not Use Imported Version** to return to the pre-defined page.
If the file cannot be uploaded, you should see an error message at the bottom of the page. Following are some common problems:
 - **File not composed of valid text**—The file contents are not recognized as HTML. For example, you might have selected an RTF file. Ensure that you save the file as HTML before trying to import it.
 - **Error: Invalid variable name {{var_name}}**—The *var_name* is not a recognized variable name. Any text that appears between two sets of braces must be a recognized variable. The message mentions the first wrong variable name encountered, but there might be more than one incorrect variable in the file. Correct all variable names and try again.

End User Notification Variables

Any text within double braces, such as `{{variable_name}}`, is considered a system variable. Variables are replaced with values from the flow when the end user notification message is presented to the user. Use variables to help users understand the reasons for the action you are taking and to aid your help desk staff if users ask for an explanation.

The available variables differ based on the notification type. Many variables are available for all types of messages whereas others are limited to one type, as explained in the following table.

If the variable name does not match a name listed in the following table, users will see an empty space in place of your variable name.

Variable Name	Example	Description	Notification Types
application_behavior	Tweet	The application behavior, which is not available for all applications.	Application
application_name	Twitter	The name of the application.	Application
application_tag	Cloud	The tag assigned to the application.	Application

Variable Name	Example	Description	Notification Types
application_type	Social Networking	The general type of application.	Application
blocking_reason	Application	The reason access was blocked.	All
continue_url	http://server.com?redirect= http://www.example.com/index/	The URL that will be used if the user clicks the link to continue.	Warning Authentication
destination_ip	10.100.10.10	The IP address of the destination site.	All
destination_port	80	The TCP/UDP port on the destination site.	All
file_type	audio	The media, or MIME, type for the file.	File type
flow_id	384	The identifier given to the traffic flow by the firewall.	All
full_url	http://www.example.com/index/	The URL of the destination, including the full path.	All
source_ip	10.100.10.10	The IP address of the traffic source.	All
source_port	80	The TCP/UDP port of the traffic source.	All
time	02:50:55pm UTC	When the traffic flow occurred.	All
threat_type	Phishing	The threat type associated with the low reputation site. The reputation must be -6 or below to have a threat type.	Web reputation
uploads_or_downloads	upload	Whether the file transfer was an upload (source to destination) or download (destination to source).	File type
web_category	Social Networking	The general web category to which the destination URL belongs.	URL filtering
web_reputation	-6.7	The web reputation of the destination site, from -10 (worst) to 10 (best).	Web reputation

URL and Application Filtering

Context-Aware Security access rules allow you to control network access based on individual URLs or URL categories (called URL filtering) and application criteria, a combination of applications and traditional port-based service specifications, and even different behaviors for individual applications (called application filtering). These features can make it easier for you to define and deploy a policy without having to determine

the exact characteristics of the traffic you are trying to prevent or allow, especially for traffic that intentionally changes ports to avoid firewall blocking.

Although you can define similar policies using URL filtering and application filtering, these types of filtering are not equivalent. For example, you do not get the same results if you create an access rule denying the Games URL category as you do creating an access rule denying the Games application type.

The following topics explain URL and application filtering in more detail.

Comparing URL and Application Filtering

URL and application filtering serve two different purposes:

URL Filtering

URL filtering denies or allows traffic based on the URL of the destination site and works for HTTP or HTTPS traffic only.

The purpose of URL filtering is primarily to completely block or allow access to a web site. Although you can target individual pages, you typically specify a host name (such as www.example.com) or a URL category, which defines a list of host names that provide a particular type of service (such as Gambling).

Thus, URL filtering rules are broad in their application and can be easily applied, so there is no delay in the device allowing or denying traffic.

You can also use URL filtering in decryption policies to help identify traffic flows that should receive specific types of decryption handling. For example, you could target the Finance category and apply the Do Not Decrypt action, so that you do not spend device resources decrypting traffic to sites that are generally trustworthy. Application filtering is not available in decryption policies.

To configure URL filtering, you specify URL objects in the Destination field of access or decryption policies. You can also include URL objects in destination object groups, which you can then use to specify the destination in these policies.

Application Filtering

Application filtering denies or allows traffic based on more subtle characteristics of the traffic flow. For some applications, you can specify different actions based on the behaviors available with the application; for example, you could allow Facebook access but prevent users from posting photographs. You can write policies based on specific applications, or on groupings of applications using application types and tags.

Additionally, there are applications and application types for many non-HTTP/HTTPS traffic flows. There are even applications and application types for non-TCP/UDP flows, such as ICMP and various routing protocols. Thus, you can define policies at an application level for traffic flows unrelated to web browsing.



Note Applications that use protocols other than HTTP or HTTPS typically must use their default ports to be recognized.

Also note that the applications included in an application type do not necessarily include all and only the same web sites included in the equivalent URL category.

Because it might not be obvious at the start of a traffic flow which application or behavior is included in the flow, part of a flow might be allowed before a decision is reached on the content of the flow. A deny access policy might be applied in the middle of a flow rather than at the start of the flow.

When trying to decide whether to use URL filtering or application filtering for HTTP/HTTPS traffic flows, consider whether your intention is to create a policy that applies to all traffic directed at a web site. If your intention is to treat all such traffic the same way (denying it or allowing it), use URL filtering. If your intention is to selectively block or allow traffic to the site, use application filtering.

Also keep in mind that URL and application filtering require special licenses.

Controlling Applications

The Application Visibility and Control (AVC) engine inspects traffic to determine the application associated with a traffic flow. Inspection can determine, for example, the specific application being carried over an HTTP traffic flow, differentiating between Facebook and LinkedIn, for example.

Because there are a wide variety of web-based applications, AVC makes it possible to control specific web-based applications rather than forcing you to apply a blanket policy to all web traffic, or use URL filtering to attempt to control an application associated with a specific web site. Application control gives you more granular control over web traffic than just URL filtering.

AVC also can identify non-web traffic, so that you can create application-based policies rather than protocol/port based policies. For example, you could create an application-based policy for Border Gateway Protocol traffic rather than the TCP/179 service. 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.

To control traffic flows based on applications, you create context-aware access policies that specify any combination of the following in the Application field:

- Application type, to control the use of a group of related applications. For example, you can write a policy for Instant Messaging applications to cover AOL Instant Messenger, Google Talk, ICQ, and many other IM applications, if your intention is to treat them all the same. An application will map to a single type.

- Application tag, to control the use of a group of related applications. Tags are an additional level of grouping compared to types, and can group applications from different types. For example, you can write a policy for cloud applications. Unlike types, an application can map to multiple tags. Also, tags can be similar to types. Thus, use care when filtering based on tags.
- Application, to control the use of a specific application.
- Application object, to control a group of applications based solely on application criteria that you define in an application policy object.
- Application-Service object, to control applications that you define based on application criteria and traditional service group objects that specify protocol and port.

Decryption Requirements for Application Filtering

Some application information might be available for encrypted traffic flows. However, in many cases, the application or behavior used in a traffic flow can be determined only if the traffic flow is not encrypted. In addition, the identified application might not be as specific as it could be, for example, Facebook, but not Facebook Games.

Thus, if an application typically uses the HTTPS (encrypted) protocol, you must ensure that any access policy you write for the application is paired with a decryption policy that applies an action that decrypts the traffic for the application.

For example, if you write an access policy for any source to any destination and specify an application that uses encryption, your decryption policy must also apply to any source and any destination, or the application might not be decrypted in all cases, meaning that the application will not always be identified.

Tips for Application Filtering

If you want to create traffic matching criteria in access policies using the application criterion, you typically just select the desired application specifications. You can do this directly or by creating reusable application or application service objects.

However, there are occasionally tricks to getting the results that you expect. The following table provides some tips on using application filtering for certain applications.

Application	Filtering Criteria
AOL Instant Messenger (AIM)	To target all AIM traffic, you must select two applications: AOL Instant Messenger and AOL protocol. Note AOL protocol is also used with ICQ, so if you want to allow one of ICQ or AIM, and disallow the other, you must allow AOL protocol.
BitTorrent	There is more than one application that relates to BitTorrent. You can get unexpected results if you allow one but deny another, particularly when dealing with the BitTorrent and BitTorrent Networking applications. There is also an Encrypted BitTorrent application. Best practice is to select all of these applications if you intend to write a policy on any one of them. Either allow or deny them as a group.

Application	Filtering Criteria
ICMP	There are many ways to target Internet Control Message Protocol (ICMP) traffic: • Service objects—You can use service objects instead of application filtering. You can use the pre-defined protocol-icmp or protocol-icmp6 to target all ICMP traffic (IPv4 or IPv6), or there are pre-defined objects that target each ICMP message type (named icmp-* and icmp6-*). You can also create objects to define any combination of message types. • Applications—There are several applications such as internet control message protocol, internet control message protocol version 4, and ipv6-icmp. However, these applications do not match ping, which has its own application. There are also applications for some other message types named ipv6-*, but not all message types have their own application.
ICQ	To target all ICQ (“I seek you”) traffic, you must select two applications: icq and AOL protocol. Note AOL protocol is also used with AIM, so if you want to allow one of ICQ or AIM, and disallow the other, you must allow AOL protocol.
eMule	To target eMule traffic, select the eDonkey and encrypted emule applications.

Using the Application Viewer

Use the Application Viewer to:

- Explore the applications and application types currently available for access control and reporting.
- Determine the applications that are contained within an application type, or to which type an application belongs.
- Determine the controllable behaviors available for an application, if any.
- View the current usage of an application or application type within policies or policy objects.
- View a hit count for each application, which indicates the number of times users tried to use the application. The hit count is linked to the application detail dashboard for the application.
- View a hit count for each application type, which indicates the number of times users tried to use applications of that type. The count is a summary of all application hits within the type. The hit count is linked to the application type detail dashboard.



Tip

The hit count is based on the time range currently selected in the dashboards. Mouse over the hit count to see the time range.

To open the Applications viewer, select **Components > Applications**.

The Application Viewer includes the following items:

- **I want to**—Includes the following commands:
 - **View by Application Types**—To display application types in the list, not individual applications.
 - **View by Application Names**—To display individual applications in the list, not application types.
 - **View New Applications**—To display applications that have been added in the past 30 days through new application signature downloads.
- **List of applications or application types**—Each application shows the name, description, application type, behaviors, ports, and when the application was added. If you view the list by application type, the applications are organized in application type folders. Open a folder to see which applications are contained within the type.

The following information is also available:

- If any traffic for the application or application type has been seen, a hit count is also shown; click the hit count link to view the detailed dashboard for the application or application type.
- If the application or application type has been used in a policy or policy object, a summary of the usage is shown in the list. Mouse over the item and click the **View Usage Details** command to see details about the policies and objects. Also click this link to view the full description of an object it is has been truncated with an ellipsis.

URL Filtering

URL Filtering allows you 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 web sites.

You can also allow or block access based on individual URLs. For example, you could allow access to all web servers on your internal network, or block access to a new web site that has not yet been categorized.

To implement URL filtering, you do the following:

- Create URL objects that define the categories or individual URLs, or both, that you want to treat the same way. You can put categories or URLs in the exclude list of the object to exclude sites that would otherwise match the categories or URLs in the include list. For example, you could create a URL object for the Games category with the intention of blocking most games, but put a few specific URLs for gaming sites in the exclude list to allow access to those sites.
- (Optional.) Create destination objects to define a complex combination of URL objects associated with network group objects to define access based on a combination of destination IP addresses for hosts or networks and the URLs or categories of servers with matching addresses.
- Use URL objects or destination objects in the following policies:
 - Access, to either allow or block access to the included URLs or categories.
 - Decryption, to determine whether HTTPS access to the included URLs or categories is decrypted so that the traffic can be examined for deeper characteristics, such as application content or behavior.

URL Categories

To view descriptions of the available URL categories, select **Components > Web Filtering Categories**.

You can also view the description of a category by clicking the **View Details** link in the selection list in the URL object.

From the **I want to** menu on the Web Filtering Categories page, you can also perform these actions:

- **Look up or submit URLs for re-categorization**—To check to which category a particular URL belongs. This can help you design URL filtering policies to implement your desired filtering. If you disagree with a categorization, you can submit a recommendation for re-categorization. This command opens a separate web page on Cisco.com, and you must have a Cisco.com login to use it. For more information, see [Determining the Category for a URL](#), on page 272.
- **Look up web reputation score**—To determine the reputation of a web site. This can help you design web reputation filtering policies. Enter the web site (for example, www.example.com) and click **Get Score**.

Determining the Category for a URL

URL categories are powerful tools for creating rules. For example, you might want to block gambling on the corporate network if gambling is not consistent with your corporate acceptable use policies. By creating an access rule denying the Gambling category, you implement your policy without having to type in the address of every individual gambling web site, and you do not need to invest your time in scouring the Internet to determine the address of every possible gambling site.

On the other hand, you do not want to block traffic to an acceptable site by inadvertently blocking the URL category to which the site belongs.

Thus, you might want to determine the web category of a site before defining rules that might affect traffic to the site. If you determine the site belongs to a category that you otherwise want to block, you can add the acceptable site to the Exclude list in the URL object that includes the otherwise objectionable category.

You can use any of the following methods to determine the URL category of a web site:

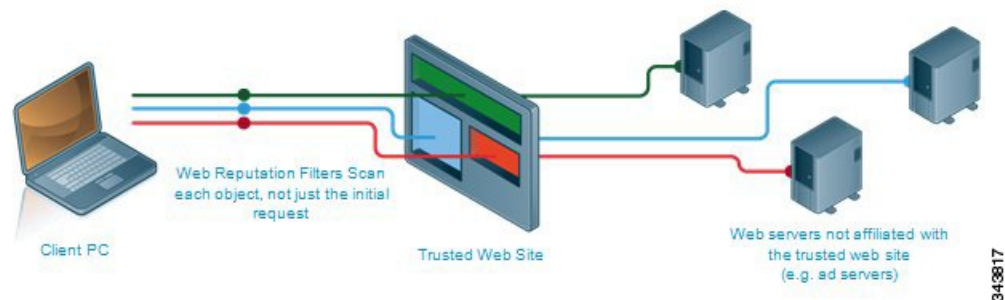
- If traffic to the site has already gone through the device, you can look at dashboards or Event Viewer to find the site.
 - **Dashboards**—Look at the Web Destinations dashboard and find the web site. Click the site to see the detailed dashboard for the destination. The Top Destinations group shows the URL category as well as the application and application type.
 - **Event Viewer**—Find an event with the web site as the destination. For example, open the web site from a workstation whose traffic goes through the device while you are looking at events in real time. The event details include the URL category.
- You can use the following procedure to look up the category for a site, especially if you have strong reasons to believe the site hosts malware or is otherwise objectionable, meaning that you do not want to open the site directly. You must have an account on Cisco.com.
 - 1 Open the following URL in your web browser: https://securityhub.cisco.com/web/submit_urls. You can go there directly, or you can select **Components > Web Filtering Categories**, then select **I want to > Look Up or Submit URLs for Recategorization**, which opens the site. You will be prompted to log into Cisco.com if you are not already logged in.

- 2 On the Lookup or Submit URLs tab, enter the URL in the URLs for Lookup box. You can enter more than one URL at a time.
- 3 Select **ASA CX**.
- 4 Click **Lookup**.

Upon successful lookup, a table lists the URLs you entered and their associated URL categories. If there is no category, the URL has not yet been categorized. If you disagree with the category, or you have a suggestion for an uncategorized URL, you can select the URL, then select the category you believe is more appropriate, and click **Submit** to make a request that the category be changed. You can track your requests on the Status on Submitted URLs tab.

Web Reputation Filtering (Malware Protection)

Users are continually at risk of obtaining malware from Internet sites. Even trusted sites can be hijacked to serve malware to unsuspecting users. As illustrated below, web pages can contain objects coming from different sources. These objects can include images, executables, Javascript, advertisements, and so forth. Compromised web sites often incorporate objects hosted on external sources. Real security means looking at each object individually, not just the initial request.



The Cisco Threat Operations Center uses dynamic updates and actionable intelligence obtained from ASAs, IPSs, Email security appliances, web security appliances, and system administrators to calculate a web reputation score for web sites. Web reputation is a statistical assessment based on context and past behavior and combines many factors of varying significance into one correlated metric. Similar to a person's credit score, web reputation is a continuous value along a graduated scale from -10 to 10. By defining a low reputation zone, you can implement predictive, zero-day protection against low reputation sites, the ones that are most likely to serve malware to your users.

The following topics explain how to implement web reputation filtering.

Guide to Web Reputation Scores

Following is a general guideline to the web reputation scores:

-10 to -6

Sites in the lowest reputation zone are dedicated or hijacked sites that persistently distribute key loggers, root-kits, and other malware. Also included are phishing sites, bots, and drive-by installers. Sites in this reputation range are almost guaranteed to be malicious.

The pre-defined default web reputation profile defines this zone as the low reputation zone.

-6 to -3

Sites in this zone tend to be aggressive ad syndication and user tracking networks. These sites are suspected of being malicious, but maliciousness has not been confirmed.

-3 to 3

Sites in this zone tend to be well managed, responsible content syndication networks and user generated content sites.

0 to 5

Sites in this zone have some history of responsible behavior or third party validation.

5 to 10

Sites in this zone have a long history of responsible behavior, have significant traffic volume, and are widely accessed.

**Tip**

To look up the reputation of a site, select **Components > Web Filtering Categories**, then select **I want to > Look up web reputation score**.

Configuring Web Reputation Filtering

To implement reputation-based processing, you apply a web reputation profile to the following types of policy:

- Access policies that allow traffic. By adding a web reputation profile, the policy will in general allow matching traffic, but drop any traffic from a low reputation site. You can apply the profile to any or all access policies that have the Allow action.
- Decryption policies whose action is Decrypt Potentially Malicious Traffic. By adding a web reputation profile, any low reputation sites that match the policy will be decrypted, so that access policies have knowledge of the content of the traffic. The access policies can then drop the traffic if configured to do so. Even if you do not have a matching access policy that drops the traffic, decrypting the low reputation traffic provides data for reports that is otherwise unavailable for encrypted TLS/SSL traffic flows.

For access policies, you can configure a device-level profile and have the policy use that profile. You can then easily change your default filtering policy by editing the **Malware Protection** settings.

You must have a Web Security Essentials license to implement web reputation filtering.

Procedure

-
- Step 1** Select **Components > Objects** and create the web reputation profiles needed to implement your filtering policies.
- There is a Default Web Reputation Profile object. If this object satisfies your requirements, you do not need to create your own objects. Otherwise, select **I want to > Add Web Reputation Profile** and create the object. Adjust the slider to determine the low reputation zone, which is blocked (denied), and the high reputation zone, which is allowed.
- Keep in mind that the reputation score for a site can change over time, so a site can move between zones as its relative danger assessment changes.
- To look up the reputation of a site, select **Components > Web Filtering Categories**, then select **I want to > Look up web reputation score**.
- Step 2** Select **Configurations > Policies/Settings**, open the **Malware Protection** tab, and enable web reputation filtering and select a device-level profile.
- The device-level profile is applied to all traffic matching access policies configured to use the device-level profile. Use the option to define your default web reputation filtering policy.
- (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 3** Edit access policies to apply the desired profile.
- For each access policy that should apply a web reputation filtering profile, edit the policy and select the appropriate profile. To use the device-level profile, select **Device Level Profile (name)**; the name of the profile configured is shown in the option. If you select no profile (or if the device-level profile is “none”), web reputation filtering is not applied to matching traffic. You can create web reputation profiles on the Policy Objects page, or you can create them while editing the access policies.
- Step 4** Configure decryption policies if you want to use reputation as a basis for decrypting encrypted traffic.
- If you select **Decrypt Potentially Malicious Traffic** as the action of a decryption policy, you select a web reputation profile to design the low reputation zone. Sites in that zone are decrypted, whereas sites in the high zone are not decrypted.
- Step 5** Monitor the results:
- Select **Dashboard > Malware Traffic**.
 - Select **Events > Events**, then select the Context Aware Security or Encrypted Traffic views.
-

Configuring Malware Protection (Web Reputation) Settings

You can configure a device-level web reputation profile and apply it to CX Context-Aware access policies. By configuring a device-level profile, you can easily apply uniform reputation filtering across your policies and quickly change settings by simply changing the device-level profile or by editing it.

Although web reputation filtering is enabled by default, you can turn it off in these settings.

**Note**

You cannot configure decryption policies to use the device level profile configured here, because the web reputation setting is not optional for reputation-based decryption. You must explicitly select a profile in each decryption policy that requires one.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and open the **Malware Protection** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Select **Malware Protection: On** to enable web reputation filtering. If you change this setting, filtering is enabled or disabled when you commit your changes. However, the change applies to new traffic flows; any existing traffic flows continue to be filtered or not filtered based on the previous setting. You must have the Web Security Essentials license to enable the service.
- Step 3** Select the device-level web reputation profile object in **Web Reputation Profile**. The system-defined **Default web reputation profile** implements the recommended filtering, but you can select **Create New Profile** to create your own, or select any other already-defined profile. If an access policy specifies **Device Level Profile (name)**, the profile defined here is used for matching traffic. If you leave the device-level profile empty, web reputation filtering will be disabled for any access policy configured to use it.
- Step 4** Click **Save**.
-

Next Generation IPS Filtering

Next Generation IPS (Intrusion Prevention System) filtering analyzes network traffic in real time, comparing the traffic contents against known threats. If a connection matches a threat, you can drop the connection to block the threat. You can also choose to monitor but allow, or completely ignore, threats that you decide are benign.

The Cisco Security Intelligence Operations Center develops signatures that identify threats. Multiple signatures can map to a single threat. New signature sets are downloaded on a regular basis unless you disable updates. You can also implement automatic blocking of blacklisted sites, which are sites considered to be always dangerous.

The following topics explain how to implement Next Generation IPS filtering.

Configuring Next Generation IPS Filtering

You can configure device-level and per-access policy settings for Next Generation IPS filtering.

You must have the Next Generation IPS license to enable filtering.

Procedure

-
- Step 1** Select **Components > Objects** and create the NG IPS profiles needed to implement your filtering policies. There is a Default NG IPS profile object. If this object satisfies your requirements, you do not need to create your own objects. Otherwise, select **I want to > Add NG IPS Profile** and create the object. Adjust the sliders to determine the zones you will block (deny), allow and monitor (alert, that is, generate events), and allow and do not monitor (ignore, that is, do not generate events). You can also configure exceptions for these zones if you know of specific threats that fall into a zone but which you want to treat differently.
- Keep in mind that the score for a threat can change over time, so a threat can move between zones as its relative danger assessment changes.
- You can see descriptions of the various threats by selecting **Components > Threats**.
- Step 2** Select **Configurations > Policies/Settings**, open the **Intrusion Prevention** tab, and enable Next Generation IPS filtering, select a device-level profile, and configure other settings.
- The device-level profile is applied to all traffic matching access policies configured to use the device-level profile. Use the option to define your default Next Generation IPS filtering policy.
- (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 3** Edit access policies to apply the desired profile.
- For each access policy that should apply a Next Generation IPS filtering profile, edit the policy and select the appropriate NG IPS profile. To use the device-level profile, select **Device Level Profile (name)**; the name of the profile configured is shown in the option. If you select no profile (or if the device-level profile is “none”), Next Generation IPS filtering is not applied to matching traffic. You can create NG IPS profiles on the Policy Objects page, or you can create them while editing the access policies.
- Step 4** Configure decryption policies if you want the most effective Next Generation IPS filtering for encrypted traffic.
- In some cases, Next Generation IPS filtering can recognize threats in encrypted traffic. However, in other cases, the traffic must be decrypted for the threat to be identified. Thus, decryption is not an absolute requirement for Next Generation IPS filtering.
- Step 5** Monitor the results:
- Select **Dashboard > NG Intrusion Prevention**.
 - Select **Events > Events**, then select the NG IPS view.
-

Configuring Intrusion Prevention Settings

Use the Next Generation IPS settings to enable the service, define the device-level filtering profile, and set other advanced options.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and open the **Intrusion Prevention** tab.

(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

- Step 2** Select **Intrusion Prevention: On** to enable Next Generation IPS filtering.
If you change this setting, filtering is enabled or disabled when you commit your changes. However, the change applies to new traffic flows; any existing traffic flows continue to be filtered or not filtered based on the previous setting.
You must have the Next Generation IPS license to enable the service.
- Step 3** Select the device-level NG IPS profile object in **NG IPS Profile**.
The system-defined **Default NG IPS profile** implements the recommended filtering, but you can select **Create New Profile** to create your own, or select any other already-defined profile.
If an access policy specifies **Device Level Profile (name)**, the profile defined here is used for matching traffic.
If you leave the device-level profile empty, Next Generation IPS filtering will be disabled for any access policy configured to use it.
- Step 4** Configure the following advanced settings as desired:
- **Scan High Reputation Traffic : On/Off**—Whether to perform Next Generation IPS filtering for traffic flows to high reputation sites, which are defined as low risk, that is, worthy of being bypassed. Next Generation IPS can identify certain types of traffic as being highly unlikely to contain threats, and web reputation can be part of this identification. Be aware that reputation scores are updated regularly with WBSR downloads, and you need to have an active Web Security Essentials license for these downloads to occur; otherwise, the reputation scores used in this evaluation will become dated.
 - **Block Blacklisted Traffic: On/Off**—Whether to block the sites on the blacklist downloaded periodically through the engine and signature updates. These sites are considered so threatening that all traffic from them or to them is dangerous. The actual sites on the list change as updates occur. If you enable this option, blacklisted traffic flows are blocked before any other access policies are considered.
 - **Blacklisted Traffic Eventing: On/Off**—Whether to generate traffic events when a traffic flow is dropped because it involves a blacklisted site. If you turn this off, blacklisted flows are dropped silently. If you enable eventing, dropped traffic generates Flow Deny events where the policy name is Blacklist (Source) or Blacklist (Destination), depending on whether the blacklist site originated the traffic or was the destination.
- Step 5** Click **Save**.
-

Viewing Next Generation IPS Threats

You can view descriptions of the threats available in the system.

Select **Components > Threats** to see the list.

For threats with long descriptions, which are truncated, mouse over the threat and click **Read More**. You can find additional detail from external sources by clicking the **Go to Information Site** link; the link will open in a new window.

Configuring Signature and Engine Updates

Applications and their attributes, URL categories, and web reputation are defined by signatures and applied by Security Application Scanner (SAS) engines. Next Generation IPS also includes a signature and engine package. Updates to these and other components are made available frequently on an update server. You can configure a time window and an HTTP proxy for obtaining these updates.

If you do not change the update settings, the device checks the update server every 5 minutes throughout the day and downloads updates if any are found. Updates can result in the following changes:

- New URL categories, applications, application behaviors, application types or tags, or Next Generation IPS threats.
- Changes to existing URL categories, applications and their attributes, or Next Generation IPS threats. Existing items might be renamed or deleted. Two or more items can be merged, or a single item can be split into one or more item.
 - If an item is simply renamed, the new name appears in any policy that used the item and your policy continues to behave as expected.
 - If an item is deleted, split, or merged, the item is replaced with an error message indicating that it is unsupported. No traffic will match the item. You must edit each affected policy to select an appropriate replacement.
- Changes in the URLs contained within a URL category.
- Changes in the web reputation of web sites.

Changes in how an application or web site is categorized can alter how traffic for the application, or traffic to the web site, is handled based on your existing policies. For example, if a new site is added to a category that you are blocking, traffic to that site might have been allowed prior to the update, but users will suddenly find traffic blocked after the update.

If new behaviors are added to an application for which you have written a policy, the new behaviors are initially allowed. You need to edit the appropriate policy if you want to deny the behavior. Use the Application Viewer to see which applications are new in the past 30 days to help you identify whether new access policies are desirable. To open the Applications viewer, select **Components > Applications**.



Tip

If you define a proxy in PRSM Multiple Device mode, the same proxy is used by all managed CX devices. Ensure that the geographical location of the proxy in relation to the managed devices makes sense. If you cannot use the same proxy for all managed devices, use multiple PRSM servers to manage groups of devices that can use the same proxy. Alternatively, alter the firewall rules for the management networks for each device to allow access to the Internet, so that a proxy is not needed.

Procedure

Step 1 Select **Configurations > Updates**.

The Updates page shows the various components that can be updated, including the date and time of the last update and the component version. In PRSM Multiple Device mode, there are separate lists for PRSM and for each managed CX device; you can compare the component versions among the systems. Messages indicate whether there has been an update failure.

Components include the following:

- **Application Visibility and Control Signatures**—These signatures define the applications and their attributes for which you can configure policies.
- **Network Participation Engine**—This client collects attack and usage data and sends it to Cisco for analysis if you opt into network participation.
- **Next Generation IPS components**—These components are used in Next Generation IPS threat filtering, and include separate components for threat signatures, the engine that evaluates traffic, and the base reputation drop list, which is a blacklist of high-threat sites.
- **Root Certificate Authority Certificates**—A list of well-known trusted root CA certificates, which are used in decryption processing.
- **Security Application Scanner Engine**—This engine evaluates traffic to determine the application, web category, or web reputation associated with the destination.
- **WSE (Web Security Essentials) components**—These components are used in URL and web reputation filtering, and include separate components for IPv4 data to support reputation verdicts, URL categories, web reputation rules, and data that supports URL category and web reputation verdicts.

Step 2 If you want to change the **Update Frequency**, click **Edit** and select how frequently to download updates:

- **Check every 5 minutes**—The update server is checked every 5 minutes throughout the day seven days a week. This is the default.
- **Check every 5 minutes within window**—The update server is checked daily but only within the time window that you select. Click in the boxes to select the start and end times, which can be in 15 minute increments. For example, you could select “From 12:00 AM to 04:00 AM” to limit updates to a lower-traffic early morning period. The time window is limited to a single day. You cannot specify a time window that straddles midnight.
- **Never update**—The update server is checked, but updates are not downloaded. Use this setting temporarily or if you decide to not purchase feature licenses.

Step 3 If you need to use an **HTTP proxy**, and it is not enabled and configured already, click **Edit** and fill in the proxy information.
Click **Help** in the proxy window for more information.

What to Do Next

- Use Event Viewer to see system events related to updates. Look at the System Events view and look for updater connection events.
- Use the Application Viewer to see the new applications that have been installed in the past 30 days.
- Configure policies to use new items.
- View the dashboards to see statistics for new items. New items are immediately available in dashboards, assuming any traffic that goes through the system matches them.

Troubleshooting Signature and Engine Updates

Use Event Viewer to see system events related to updates. Look at the System Events view and look for updater connection events.

Following are some typical issues you might encounter:

- Updates occur only if the system has active licenses for the services associated with a signature or engine update. Ensure that you have the appropriate licenses for features that you are using.
- Updates occur only if the system has a route to the Internet and can reach the Cisco update server. You have two choices: either ensure that the network to which the management interface is connected has a route to the Internet, or configure an HTTP proxy server for the Updater.
- When using PRSM Multiple Device mode, be aware that both the CX device and the PRSM server download updates.
 - If you import a device that has a more recent version than the PRSM server, you might see "(Unrecognized application)" in imported access policies that include specifications for applications not available in PRSM. These policies will deploy correctly, and PRSM will show the correct application name as soon as it has the updated signatures.
 - If the PRSM server has the more recent update, applications that are no longer defined in the signatures have "(deprecated)" appended to the name in the policy. However, these application names appear in dashboards and reports without this indication. You should pro-actively redefine policies that specify deprecated applications.
- If you define a proxy in PRSM Multiple Device mode, the same proxy is used by all managed CX devices. Ensure that the geographical location of the proxy in relation to the managed devices makes sense. If you cannot use the same proxy for all managed devices, use multiple PRSM servers to manage groups of devices that can use the same proxy. Alternatively, alter the firewall rules for the management networks for each CX device to allow access to the Internet, so that a proxy is not needed.
- Signatures are not updated unless the related engine is at the required version. Once the new engine is installed, new signature files that require it will be installed.
- The system can gracefully recognize bad updates, remove the update, and return to the previous good version without user intervention. The last known good version is always kept for recovery purposes.



Managing SSL/TLS Traffic Flows

Some protocols, such as HTTPS, use Secure Sockets Layer (SSL) or its follow-on version, Transport Layer Security (TLS), to encrypt traffic for secure transmissions. Because encrypted traffic cannot be inspected, you must decrypt it if you want to apply access rules that consider higher-layer traffic characteristics to make access decisions.

The following topics explain SSL/TLS traffic flow management and decryption in more detail.

- [Overview of SSL/TLS Traffic Management, page 283](#)
- [Configuring SSL/TLS Decryption, page 288](#)
- [Troubleshooting TLS/SSL Decryption, page 302](#)

Overview of SSL/TLS Traffic Management

The SSL/TLS protocols are widely used to protect traffic by encrypting it. Because the traffic is encrypted, traffic inspectors cannot determine the content of the traffic. In ASA CX, you use decryption policies to determine whether you decrypt a traffic flow.

You have the following options for handling SSL/TLS encrypted traffic:

Decrypt the traffic, inspect it, then re-encrypt it

If you elect to decrypt traffic, the ASA CX acts as a man-in-the-middle:

- Incoming traffic is decrypted.
- The traffic is inspected. Access rules are applied.
- If the traffic is allowed, any profiles defined in the access policy for the flow are applied, and the flow is re-encrypted and sent to its destination.
- Return trip traffic is also decrypted, inspected, then re-encrypted and sent to the client.

If you decide to decrypt traffic flows, users must accept the ASA CX certificate as a Trusted Root Certification Authority. For more information, see [Downloading and Installing the SSL/TLS Certificate, on page 293](#).



Note

To emphasize, even if you elect to decrypt a traffic flow, decryption is done simply to allow inspection. The end-to-end traffic flow is encrypted, because ASA CX re-encrypts the flow before sending it to the destination. The decrypted content is never sent to another host; it never leaves the device.

Conditionally decrypt potentially malicious traffic

You can conditionally decrypt traffic based on the web reputation assigned to the destination. If the web reputation falls into the low reputation zone that you define, the traffic is decrypted and handled like other decrypted flows. If the web reputation falls into the high reputation zone, it is not decrypted and is handled like other undecrypted flows.

Do not decrypt the traffic

If you do not decrypt TLS traffic, ASA CX is unable to inspect the encrypted protocol and is limited to what can be gleaned from analysis of the TLS handshake and the server's certificate. Because access rules based on network group, service group, or user identity have already been applied, encrypted traffic flows might already be denied before they are evaluated by decryption policies.

For encrypted traffic that is not decrypted, access rules can be applied based on network (IP address), service (ports, protocol), and user identity objects. For URL objects, the domain name only is matched, as is the web category, but you cannot specify differentiated behavior for different resources on the same web server or domain. For application objects, matches might occur for some applications and application types, but not for behaviors or very specific applications (for example, Facebook but not Facebook Games). The encrypted traffic flow will never match specifications that include user agent policy objects.

In addition, the profiles that you apply to allowed traffic flows might not be implemented. For example, file filtering properties to control uploads and downloads will not be effective, and Next Generation IPS filtering profiles might not be fully effective. However, web reputation filtering should work. Because the content of the encrypted flow is not known, some flows that would otherwise be dropped might be allowed.

The following topics explain decryption in more detail.

Why Decrypt Traffic?



Tip

The purpose of access policies in ASA CX is to detect, monitor, measure, and control what people are doing on your network. For protocols hidden within an SSL/TLS session, you cannot do these things well unless you also decrypt the traffic flow.

You have the choice whether to decrypt encrypted traffic, and you can decide to decrypt some traffic flows but not others. When you consider whether to decrypt traffic, the type of encrypted traffic that is of most interest is HTTPS.

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.

By decrypting HTTPS traffic, you can accomplish the following:

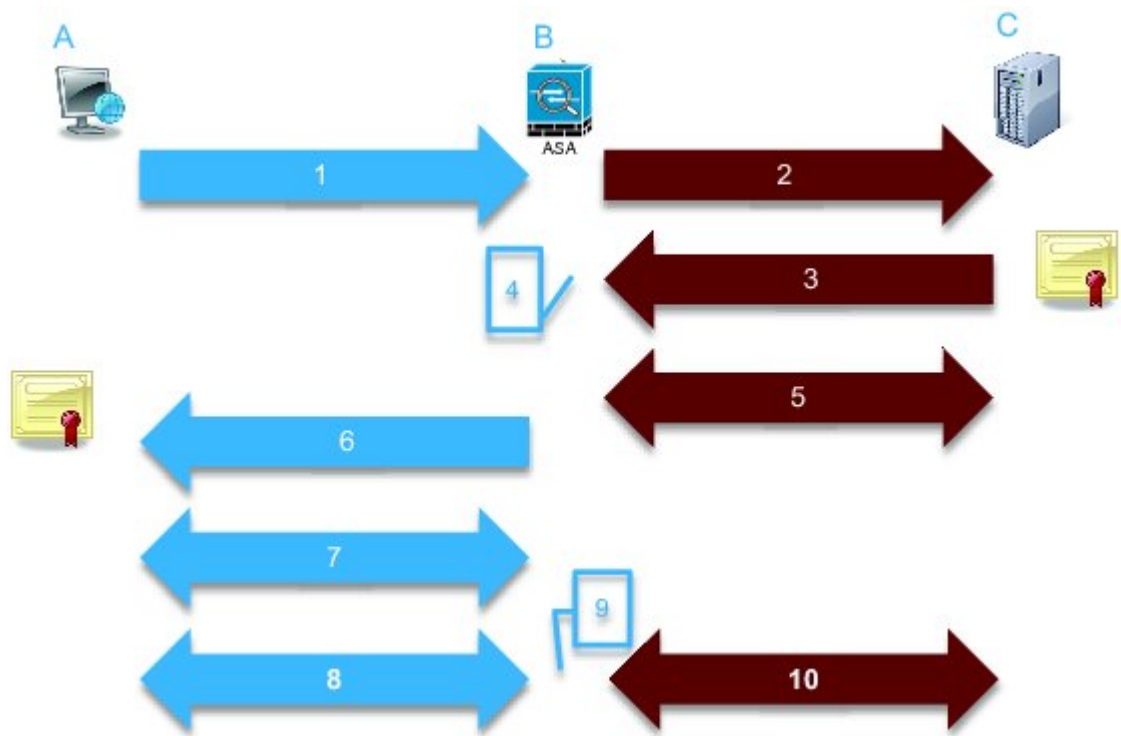
- **Gain insight into network traffic**—You can gain greater insight into your network traffic, for example, the application behaviors being used. By decrypting traffic, dashboards can include more information about web sites accessed using HTTPS.
- **Improve the effectiveness of Next Generation IPS filtering**—Some threats might not be recognized in encrypted flows.
- **Block undesired file exchanges**—You can selectively block file uploads or downloads to implement your security policies.
- **Control access based on inspected characteristics**—Because some traffic characteristics are known through inspection only, such as application behaviors and user agent, you can apply access policies using these characteristics only if you first decrypt the traffic.

General characteristics, such as IP address, protocol and port, URL category, web reputation, and general application and application type information, are available without decryption.

Decrypted Traffic Flow

Encrypted traffic flows that are decrypted are handled using the following process.

Figure 17: Decrypted Traffic Flow



- **1, 2**—Client Hello.

The client (A) starts the encrypted session by sending a hello to the intended destination (C). When the traffic flow enters the CX device (B), the device sends its own hello to the destination server.



Note If the initial flow matches a deny access policy (for example, based on the IP address of the client), the flow is dropped upon entry to the CX device.

- **3**—Server Hello and Certificate

The server responds to the hello and sends its certificate.

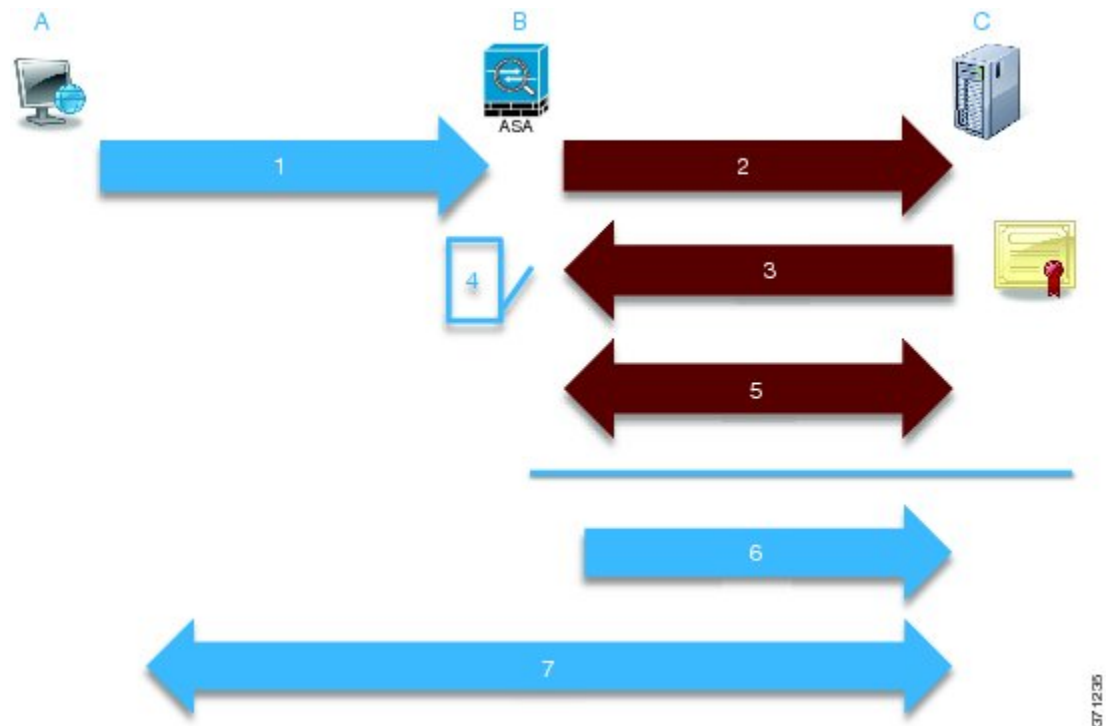
- **4**—CX device verifies the server certificate and enforces decryption policies. In this case, decrypt is the decision.
- **5**—Handshake between the CX device and server.
- **6**—Server hello and certificate.
The CX device sends its own server hello and certificate to the client.
- **7**—Handshake between the client and CX device.

- 8—Encrypted data flows between the client and the CX device.
- 9—The CX device decrypts the flow, inspects it, and applies access policies again. If the traffic matches a deny policy, the flow is dropped at this point.
- 10—Encrypted data flows between the CX device and server if the flow is allowed by access policies.

Do Not Decrypt Traffic Flow

Encrypted traffic flows that are not decrypted are handled using the following process.

Figure 18: Do Not Decrypt Traffic Flow



- 1, 2—Client Hello.
The client (A) starts the encrypted session by sending a hello to the intended destination (C). When the traffic flow enters the CX device (B), the device sends its own hello to the destination server.
- 3—Server Hello and Certificate
The server responds to the hello and sends its certificate.
- 4—The CX device verifies the server certificate and enforces decryption policies. In this case, do not decrypt is the decision. Therefore, the connection is added to the pass-through cache so that it bypasses decryption.
- 5—The CX device terminates the traffic flow with server.

- **6, 7**—The CX device initiates a new flow between the client and server, replaying the initial client hello. Because the connection is in the pass-through cache, the connection is established directly between the client and server.

Tips and Limitations for Decryption

Keep the following in mind when configuring decryption:

- A 3DES/AES (K9) license is required for strong encryption. If you do not have a 3DES/AES (K9) license, decryption processing with a server that requires strong encryption will fail. Any flow that requires decryption that the device cannot perform will be denied regardless of access policies. Although the 3DES/AES (K9) license is free, its availability is limited by export restrictions. Consult Cisco.com for details. If you are not authorized to use the 3DES/AES (K9) license, you need to bypass decryption for these sites. You can also allow these transactions by selecting **Deny Transactions to Servers; If the Secure Sessions Handshake Fails: Off** in the decryption settings.
- Decryption policies are applied to a traffic flow only if the flow begins with the SSL/TLS handshake. Traffic flows that negotiate encryption, such as SMTP over TLS, are never decrypted. Traffic flows that negotiate encryption are treated as if they were unencrypted traffic flows.
- If you enable decryption, but do not create any decryption policies, no traffic is decrypted, and encrypted traffic flows are allowed or denied based on your access policies. You must create decryption policies that apply the Decrypt Everything or Decrypt Potentially Malicious Traffic actions to decrypt any flows.
- When configuring URL objects for use in decryption policies, do not include path information. When evaluating whether traffic matches a URL object, the decryption policy completely ignores any URLs that include path information. If the object contains a mix of URLs with domain name only and URLs that include paths, the decryption policy treats the object as containing only those URLs that specify just a domain name.
- Enabling decryption might decrease the throughput of the system and affect the performance of applications that use SSL/TLS encrypted protocols.
- Some applications do not support decrypting traffic between the client and server. This might be because they cannot add certificates to their trusted certificate store, because they have a hard-coded list of certificates that they will trust, or because they prompt for a client certificate during the connection. Examples include Internet Messaging applications, Dropbox, iTunes, and many banking sites. For these applications, you must bypass decryption as described in [Bypassing Decryption for Unsupported Applications](#), on page 300. You can also try relaxing decryption processing by selecting **Deny Transactions to Servers; If the Secure Sessions Handshake Fails: Off** in the decryption settings.
- The system includes a list of root Certificate Authority certificates that are commonly included with web browsers. These certificates are regularly updated unless you disable updates. Examine your Updater settings at **Configurations > Updates**.

Configuring SSL/TLS Decryption

The following procedure provides an overview of the process for configuring SSL/TLS traffic flow decryption. Use this procedure to understand the general configuration process and see the referenced topics for detailed steps.

Procedure

-
- Step 1** Obtain and install the CX 3DES/AES (K9) license, which supports strong encryption. A 3DES/AES (K9) license is required for strong encryption. If you do not have a 3DES/AES (K9) license, decryption processing with a server that requires strong encryption will fail. Any flow that requires decryption that the device cannot perform will be denied regardless of access policies. Although the 3DES/AES (K9) license is free, its availability is limited by export restrictions.
- If you cannot use a 3DES/AES (K9) license, you should test decryption processing in a controlled environment to ensure that it satisfies your requirements before enabling decryption in your production network. Without a 3DES/AES (K9) license, your decryption policies will require careful testing and fine-tuning to ensure that desirable traffic is not blocked.
- Step 2** Enable decryption and select the CA certificate to use as described in [Configuring Decryption Settings, on page 289](#).
You must enable decryption. If you do not enable it, no traffic flows are decrypted and decryption policies are not used.
- The CA certificate is used to decrypt traffic flows from the user. Certificates from the intended destination are used to re-encrypt a traffic flow before sending it to the destination.
- Step 3** Configure decryption policies as described in [Configuring Decryption Policies, on page 295](#).
Decryption policies define how you want to handle different traffic flows. You can decrypt and inspect them, conditionally decrypt them based on web reputation, or simply not decrypt them. The default is that no traffic is decrypted, so you must create a policy that implements some type of decryption to decrypt any traffic flows.
- Step 4** Bypass decryption for trusted sites and sites that do not support decryption as described in [Bypassing Decryption for Unsupported Applications, on page 300](#).
Consider not decrypting traffic to well known URL categories, such as Finance, to avoid unnecessary decryption processing of flows that are probably safe. Additionally, bypass decryption for applications used in your network that do not work if traffic is decrypted between the client and server, for example, Instant Messaging applications.
- Step 5** Configure client applications to recognize the CA certificate that is used in decryption as a trusted root CA certificate.
Users must have the CA certificate that is used in the encryption process defined as a Trusted Root Certificate Authority in their applications that use TLS/SSL. Download the CA certificate and make it available to users to install in their browsers as described in [Downloading and Installing the SSL/TLS Certificate, on page 293](#). You can avoid user interaction by pre-installing the certificate in user browsers using your software management methods. Some non-browser applications might not allow you to add certificates; you might need to bypass decryption for these applications.
- Step 6** Use Event Viewer to view and analyze decryption events.
Select **Events > Events** to open Event Viewer.
-

Configuring Decryption Settings

Before you can implement decryption policies on ASA CX, you must enable them and identify the Certificate Authority (CA) certificate that the ASA CX will use to managed decrypted traffic flows.

The CA certificate is used to issue temporary replacement certificates for each site that is visited by a client application. The temporary certificate is used in place of the real server certificates in the secure (SSL or TLS) session between the client and ASA CX. Meanwhile, the real server certificate is used in the secure session between ASA CX and the server. This approach enables ASA CX to decrypt the content coming in to the device from either side, and then re-encrypt it before relaying it.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and open the **Decryption Settings** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Select **Enable Decryption Policies: On** to enable TLS/SSL decryption and decryption policies. If you enable decryption policies, additional settings appear to allow you to select the CA certificate to use for managing decrypted flows.
- Step 3** If desired, change the **Deny Transactions to Servers** options to relax certificate handling requirements to reduce the number of failed TLS/SSL transactions:
- **Using an Untrusted Certificate: On/Off**—Whether a session with a server whose certificate is not trusted should be allowed anyway. This can include expired certificates, unknown issuers, mismatched hostnames, etc.
 - **If the Secure Sessions Handshake Fails: On/Off**—Whether a session should be dropped if the TLS/SSL handshake fails. If you have any decryption policies, even sessions that would match a Do Not Decrypt policy can be dropped if there are handshake problems. This option applies to an error in the TLS handshake, not due to untrusted certificate, that would result in an SSLv3 Alert Handshake error.
- If you select **Off** for either option, sessions that have the associated problem are allowed without decryption. Thus, no access policies that require decryption will be applied to these transactions.
- Step 4** Select the **Certificate Initialization Method** to use, either **Generate** or **Import**, and fill in the fields. If you already enabled decryption, summary information about the currently configured certificate appears on the page instead of the **Certificate Initialization Method** field. There are links to **Export** or **Replace** the certificate.
- If you click **Replace**, the **Certificate Initialization Method** field appears and you can select how to replace the certificate.
- For detailed information about configuring the certificate, see [Configuring the Decryption Certificate, on page 291](#).
- Tip** You can click **Export** to export the certificate in a file that you can upload to browsers so that users do not need to save the certificate when prompted during a decrypted traffic flow.
- Step 5** Click **Save** to save your changes.
-

What to Do Next

If you enable decryption, you can now configure decryption policies.

Configuring the Decryption Certificate

ASA CX mimics the TLS 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 certificate authority configured in the appliance.

When you enable the decryption policies, you must configure the CA certificate that the appliance uses to sign its server certificates. It uses this CA certificate to issue new, temporary certificates that substitute for the certificate presented by the destination server.

You can enter certificate information using the following certificate initialization methods:

Generate

You can enter some basic organization information and have the system generate a new Certificate Authority (CA) certificate for you. This certificate will be a self-signed root CA certificate. You might want to generate a certificate if your organization does not have its own certificate authority available to issue an intermediate CA certificate.

Import

You can import (upload) a CA certificate file and its matching private key file created outside of the system. You might want to upload a certificate and key file if the clients on the network are already configured to trust that certificate or the CA that issued it.

You can upload either a root or an intermediate certificate that has been signed by a certificate authority. When the ASA CX 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 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 certificate authority, but does not want to upload the root certificate to the ASA CX for security reasons.

If you request a new certificate from a CA, ensure that you request a certificate that is itself a Certificate Authority. In other words, you need to have a certificate that is enabled for issuing additional “child” certificates.

The certificate and key files you upload must be in PEM format. DER format is not supported. For information about how to convert a DER formatted certificate or key to PEM format, see [Converting Certificate and Key Formats](#), on page 293.



Note

The certificate you upload must have the basic constraints extension present to work with Mozilla Firefox browsers. This constraint allows Firefox to recognize the certificate as a trusted CA. In general, the certificate should include the basic constraints extension, that is, it should be a CA certificate.

The certificate that you generate or upload must be recognized by client applications (typically, browsers) or users might see warnings about untrusted certificates. You must also configure the user’s applications to recognize the certificate as explained in [Downloading and Installing the SSL/TLS Certificate](#), on page 293.

The following procedure explains how to generate or upload the certificate required by decryption policies.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and open the **Decryption Settings** tab.
Ensure that **Enable Decryption Policies: On** is selected.
- (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Do one of the following:
- Select **Certificate Initialization Method: Generate** to create a new certificate.
 - Select **Certificate Initialization Method: Import** to upload an already existing certificate and private key file.
 - If you already have a configured decryption certificate and want to replace it, click **Current Certificate Information: Replace**, then select one of the initialization methods.
- Step 3** If you selected **Generate**, fill in the following information:
- **Common Name**—(CN.) The common name to include in the certificate. This could be the name of the device, web site, or another text string.
 - **Organization**—(O.) The organization or company name to include in the certificate.
 - **Organizational Unit**—(OU.) The name of the organization unit (for example, a department name) to include in the certificate.
 - **Country**—(C.) The two-character ISO 3166 country code to include in the certificate. For example, the country code for the United States is US.
 - **Months to Expiration**—The number of months the certificate should remain valid. The default is 12 months.
 - **Set Basic Constraints Extension to Critical: On/Off**—Whether to set the Basic Constraints extension to critical. The Basic Constraints extension indicates that the certificate is a CA certificate and that it can be used to sign other certificates. If you set the extension as critical, you are saying that this extension is very important to the meaning of the certificate and that client applications should not accept the certificate if they do not understand what the extension means. Most TLS clients should recognize the extension. However, you can select **Off** to work around client applications that do not understand what the extension means.
- The information you include in these certificate fields will be visible to end-users if they examine the certificate details in their web browsers. Use the Common Name and Organization fields to give end users a good idea about the certificate's ownership.
- Step 4** If you selected **Import**, fill in the following information:
- **Certificate**—Click **Browse** to select the CA certificate file you want use and upload it to the device.
 - **Key**—Click **Browse** to select the private key file you want to use and upload it to the device.
 - **Private Key Phrase**—Enter the pass phrase for the private key file if it is protected by a pass phrase.
- Step 5** Click **Save**.

The certificate is generated or imported. Summary information about the certificate is displayed on the page. You can click **Export** to export the certificate.

Converting Certificate and Key Formats

The root certificate and private key files you upload 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:

```
openssl rsa -inform DER -in key_in_DER -outform PEM -out out_file_name
```

For DSA keys, use the following command:

```
openssl dsa -inform DER -in key_in_DER -outform PEM -out out_file_name
```

For more information about using OpenSSL, see the OpenSSL documentation, or visit <http://openssl.org>.

Downloading and Installing the SSL/TLS Certificate

If you decide to decrypt traffic, users must have the ASA CX CA certificate that is used in the encryption process defined as a Trusted Root Certificate Authority in their applications that use TLS/SSL. Typically if you generate a certificate, or sometimes even if you import one, the certificate is not already defined as trusted in these 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 web site's security certificate. Usually, the error message says that the web site's security certificate was not issued by a trusted certificate authority or the web site was certified by an unknown authority, but the warning might also suggest there is a possible man-in-the-middle attack in progress. Some other client applications do not show this warning message to users nor allow users to accept the unrecognized certificate.

You have the following options for providing users with the required certificate:

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. Users should accept the certificate and save it in the Trusted Root Certificate Authority storage area so that they are not prompted again the next time they access the site.



Note

The user needs to accept and trust the CA certificate that created the replacement certificate. If they instead simply trust the replacement server certificate, they will continue to see warnings for each different HTTPS site that they visit.

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 using, you can download the root certificate from the decryption settings. Click the **Export** link and save the file.

You can either make the certificate available to users by E-mailing it or placing it on a shared site, or you could incorporate the certificate into your corporate workstation image and use your application update facilities to distribute it automatically to users.



Tip

To reduce the possibility of client machines getting a certificate error, do not commit changes to the certificate until after you export it and add it to client applications.

The following procedure explains how to download the CA certificate and install it into the browser.

Procedure

-
- Step 1** If necessary, download the certificate from ASA CX.
- Select **Configurations > Policies/Settings** and open the **Decryption Settings** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
 - Click the **Export** link next to the Current Certificate Information heading. Depending on your browser configuration, you might be prompted to open or save the file. Save it to your desired destination.
- Step 2** Install the certificate in the Trusted Root Certificate Authority storage area in web browsers on client systems, or make it available for clients to install themselves. The process differs depending on the type of browser, and can differ depending on the browser version. For example, you can use the following process on Firefox 11.
- In Firefox, select **Tools > Options**.
 - Select **Advanced**, then select the **Encryption** tab.
 - Click **View Certificates** to open the Certificate Manager.
 - Select the **Authorities** tab.
 - Click **Import**, locate and select the downloaded file (ca.crt.pem), and click **OK**. The Downloading Certificate dialog box opens.
 - Select **Trust this CA to identify web sites** and click **OK**. You should now see the CA name in the list of Certificate Names on the Authorities tab. You can now close all of the certificate dialog boxes and return to the browser window.
-

Managing Supplemental Trusted Certificates

When ASA CX receives a connection request for an TLS server, it validates the trustworthiness of the destination server by verifying the root certificate authority that signed the server certificate. If ASA CX does not recognize the root certificate that signed the server certificate, then it does not trust the server certificate.

This happens when the TLS server uses a certificate authority that is not listed in the set of trusted certificate authorities that ship with the ASA CX. This might happen if your organization uses an internal certificate authority to sign certificates for servers on the internal network.

**Tip**

The primary symptom of this problem is that you will see TLS Abort events in Event Viewer indicating that the server presented an untrusted or invalid certificate. You can relax this restriction and allow these transactions by selecting **Deny Transactions to Servers; Using an Untrusted Certificate: Off** in the decryption settings.

To prevent ASA CX 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. These supplemental certificates are used in conjunction with the built-in trusted certificates.

You can upload multiple certificate files, and each file you upload can contain multiple certificates. You can upload root CA certificates, intermediate CA certificates, or even individual server certificates. However, each certificate you upload must be in PEM format.

**Note**

The system includes a build-in list of well-known trusted root CA certificates, which are not shown on the supplemental certificates page. These certificates are regularly updated unless you disable updates. Examine your Updater settings at **Configurations > Updates**.

Procedure

-
- Step 1** Select **Configurations > Certificates**.
The certificates list shows all certificates that you have imported, including the common name, organization, organizational unit, and country for each, if these are defined in the certificate.
- Note** When you no longer need a certificate, mouse over it in the certificates list and click **Delete Certificate**.
- Step 2** Select **I Want To > Import New Certificate**.
- Step 3** Click **Browse** and select the certificate file.
- Step 4** Click **Save**.
The certificate is added to the list of root certificates.
-

Configuring Decryption Policies

Use context-aware decryption policies on ASA CX to determine how to handle SSL/TLS encrypted traffic flows. Decrypting traffic flows makes it possible to apply access policies on characteristics that cannot be gleaned from Layer 3/4 characteristics and information available from the server certificate and TLS handshake. For example, application behaviors, and some threat characteristics. Without decryption, you can still control access based on IP address, protocol/port, URL, URL category, web reputation, and general application and application type information.

**Tip**

The default is to not decrypt encrypted traffic. Thus, focus on creating policies that apply the Decrypt Everything or Decrypt Potentially Malicious Traffic actions. Policies that use Do Not Decrypt are necessary only if they specify a subset of traffic that would otherwise match a policy that applies some level of decryption.

Procedure

- Step 1** Select **Configurations > Policies/Settings** and open the **Decryption Policies** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Do any of the following:
- To add a new policy, use one of the **Add Policy** buttons. If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.
 - To edit an existing policy, select the policy and click the **Edit Policy** button.
 - To base a new policy on a similar existing policy, select the policy and click the **Duplicate Policy** button.
- A form opens with the policy properties.
- Step 3** Define the traffic matching criteria using the **Source**, **Destination**, and **Service** fields. You can leave any field blank to not restrict the policy based on that criteria. If you need to create very complex source or destination criteria, use the source and destination group policy objects. These objects allow complex combinations of other objects to precisely define traffic flows. See the reference topic for detailed information about each field.
- Step 4** Define the action to apply to matching traffic:
- **Decrypt Everything**—Select **Decrypt Everything** to have the matching traffic decrypted and subjected to additional access control policies. This option is best used for traffic classes whose security and threat characteristics you are unsure of.
 - **Decrypt Potentially Malicious Traffic**—Select **Decrypt Potentially Malicious Traffic** to conditionally decrypt traffic based on web reputation. Matching traffic that falls into the low reputation zone is decrypted, while high reputation traffic is not decrypted. If you select this option, you must also select the web reputation profile object that defines the low reputation zone in the **Web Reputation** field.
 - **Do Not Decrypt**—For traffic that you are certain is acceptable, such as traffic to well-known banks or other financial institutions, you can select **Do Not Decrypt** so that the traffic is passed freely and no processing power is used to decrypt the traffic.
- Step 5** If you want to limit the policy to traffic on specific interfaces on the parent device, select the **Source Interface Role** or the **Destination Interface Role**, or both, that identify the interfaces. The default is to apply the policy to traffic between any interfaces on the device. If you select interfaces that do not exist on the device, the policy is never applied to traffic.
- Step 6** Click **Save Policy**.
- Step 7** If necessary, move the policy so that it is in priority order.

Policies are applied on a first-match basis, so you must ensure that policies with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

To move a policy set or rule, you click and hold the Move icon (the vertical double-headed arrow on the left margin) and drag it to the policy after which you want to insert it. You can also simply edit the sequence number and change it to the desired value.

Decryption Policy Properties

Use context-aware decryption policies on ASA CX to determine how to handle SSL/TLS encrypted traffic flows. Decrypting traffic flows makes it possible to apply access policies on characteristics that cannot be gleaned from Layer 3/4 characteristics and information available from the server certificate and TLS handshake. For example, application behaviors, and some threat characteristics. Without decryption, you can still control access based on IP address, protocol/port, URL, URL category, web reputation, and general application and application type information.

Decryption policies have the following properties:

Policy Name

The name of the policy. This name appears in Event Viewer for decryption events generated by traffic that matches this policy, so choose a name that will help you analyze event data.

Enable Policy: On/Off

Whether the policy is enabled. You can turn a policy off to temporarily disable it without deleting the policy. Disabled policies are never applied to traffic.

Traffic Matching Criteria

The traffic matching criteria that identifies the traffic to which the policy applies. To match the policy, the flow must match every specified property, that is, there is an AND relationship between the properties. Use the default Any selection if you do not want to restrict the policy based on that condition. Leave all fields with the default Any to match every possible traffic flow.

All of the following criteria are used to determine the traffic to which a policy applies.

- **Source**—A list of policy objects of the following types: network group (IP addresses), identity (user or user group names), or Secure Mobility (type of remote access VPN client). If a packet matches any selected object, it is considered to satisfy the source condition.
- **Destination**—A list of policy objects of the following types: network group, URL (URLs or web categories), or destination object group (a collection of network group or URL objects in complex AND/OR relationships that you cannot define directly in a policy). If a packet matches any selected object, it is considered to satisfy the destination condition.

If you disable the URL filtering feature, or you do not have a valid Web Security Essentials license, you cannot use URL objects in this field or in a destination object group.



Tip

When configuring URL objects for use in decryption policies, do not include path information. When evaluating whether traffic matches a URL object, the decryption policy completely ignores any URLs that include path information. If the object contains a mix of URLs with domain name only and URLs that include paths, the decryption policy treats the object as containing only those URLs that specify just a domain name.

- **Service**—A list of service groups that define protocol and port combinations. If a packet matches any selected object, it is considered to satisfy the service condition.



Note

(Multiple Device mode.) When using PRSM in Multiple Device mode, you can also use network objects or groups defined on the device that contains the CX device for source or destination criteria, or ASA service objects for the service criteria. The network group objects come in two types: one that can be used on both ASA and CX devices, and one that can be used on CX devices only, which is explicitly called CX network group.

For information on how to select items, including how to add, edit, or remove them, filter the selection list, create or edit objects, or view object contents, see [Selecting Items](#), on page 27.

Action

The Action section determines whether matching traffic flows are decrypted. Your options are:

- **Decrypt Everything**— Decrypt and inspect the traffic. If access policies allow the traffic flow, it is reencrypted and sent to its destination.



Note

A traffic flow can be denied if a secure session to the remote server cannot be established, for example, because the device could not trust the remote server's certificate. Also, if the server requires strong encryption, you must have a 3DES/AES (K9) license for the ASA CX or the flow will be denied.

- **Decrypt Potentially Malicious Traffic**—Conditionally decrypt traffic based on web reputation. Matching traffic that falls into the low reputation zone is decrypted, while high reputation traffic is not decrypted. If you select this option, you must also select the web reputation profile object that defines the low reputation zone in the **Web Reputation** field.

If you want to deny traffic to low reputation web sites, you should use the same web reputation profile in your access policies.

- **Do Not Decrypt**—(Default.) Do not decrypt the traffic. These traffic flows are not inspected. However, enough information is gathered from HTTP headers and the destination server certificate to enable URL object matching for your destination criteria. URL matching is based on the destination domain name, which can also be matched against a URL category.



Note

Do Not Decrypt is the default action for encrypted flows that do not match any decryption policy.

Interface Roles

The criteria that identifies the parent device's interfaces to which the policy applies. To match the policy, the traffic must enter the device on one of the source interfaces and leave the device on one of the destination interfaces. The default is any interface for both source and destination, meaning the policy is not restricted to specific interfaces.

To limit the policy to specific interfaces, select the appropriate interface role objects in either the **Source Interface Role** or **Destination Interface Role** fields, or both. The interface role objects define the interface names or naming patterns for the interfaces.



Tip

If you specify interface roles, and no interfaces on the device match the interface names defined in the role, the policy will never apply to any traffic on the device.

Tags

Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.

Ticket ID

A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)

Bypassing Decryption for Unsupported Applications

Some applications, such as Dropbox and most Instant Messaging applications such as AOL Instant Messenger (AIM), are not able to add certificates to their trusted root certificate store. These applications require that the certificate used in decryption already be the one that is trusted. These applications will not work if ASA CX decrypts the traffic with a certificate that is not trusted. If you do not, or cannot, upload an appropriate certificate in the decryption settings, your decryption policies must identify the traffic and apply the Do Not Decrypt action if you want to allow these applications.

In addition, some HTTPS servers do not work as expected when traffic to them is decrypted by a proxy server, such as the ASA CX. For example, some web sites and their associated web applications and applets, such as high security banking sites, maintain a hard-coded list of trusted certificates instead of relying on the operating system certificate store.

Finally, some applications, such as iTunes, prompt for a client certificate during the connection. If you apply decryption to these sites, the connection will fail. You must bypass decryption on these sites.

Consider the following as symptoms that an application cannot support ASA CX decryption:

- In Event Viewer, look for TLS Abort events that include an “unknown ca” or “bad certificate” alert in the Error Details column, indicating that the Certificate Authority specified in the certificate is not known or there is some other unacceptable problem with it. This is a likely error if you generate a self-signed certificate. In these cases, you might be able to resolve the problem by uploading a supplemental certificate from the untrusted CA or server (select **Configurations > Certificates**). You can also relax this restriction and allow these transactions by selecting **Deny Transactions to Servers; Using an Untrusted Certificate: Off** in the decryption settings.
- In Event Viewer, look for TLS Abort events where there is a failure to establish a secure session with the server with decryption error details indicating a handshake failure. This might indicate that the server uses strong encryption, which requires a 3DES/AES (K9) license. (If the K9 License Missing column for the event says Yes, you do not have the license installed.) If you can acquire the 3DES/AES (K9) license for your device, upload it and the problem should resolve itself. If you are not authorized to use the 3DES/AES (K9) license, you need to bypass decryption for the site.
- For AIM, users will not be able to log in. Other applications might have the same problem.
- For Dropbox, users might see an “Unable to make a secure connection” message. Other applications might have the same problem.

You can bypass decryption for traffic to the servers used in these applications to ensure all users can access these types of sites. To bypass decryption, you:

- 1 Create objects that identify the destination of the traffic. For HTTPS, you can use URL objects; for other types of TLS traffic, use network objects.
- 2 Create a decryption policy that uses the object as the destination and apply the Do Not Decrypt action. Ensure that the policy is higher in the policy set than any policies that would apply decryption processing on the same traffic.

**Tip**

Another option is to select **Deny Transactions to Servers; If the Secure Sessions Handshake Fails: Off** in the decryption settings. This will bypass decryption for all sites for which the handshake fails, which includes sites that require strong decryption when you do not support it, and sites that prompt for a client certificate during the connection, such as iTunes. Whereas creating bypass rules exempts specific identified sites from decryption, this option creates a blanket do not decrypt exemption for all sites that cannot support decryption due to session establishment problems.

The following example shows how to create a bypass decryption rule for AIM.

Procedure

- Step 1** Select **Configurations > Policies/Settings** and open the **Decryption Policies** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
- Step 2** Use one of the **Add Policy** buttons to add a new policy. If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.
- Step 3** Enter a name for the policy, for example, Bypass AIM.
- Step 4** Create and select the object:
 - a) Click in the **Destination** field and select **Create New Object** at the bottom of the drop-down list.
 - b) Enter an object name, for example, AIM.
 - c) Select **URL Object** as the object type.
 - d) Select the **Instant Messaging** URL category in the Include list, or optionally, in the URL field, enter the following items:
 - 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

Tip You can do both, so that the object specifies a category and the list of servers. If you list the servers, be aware that the actual list of servers used by AIM might change over time, so you might need to adjust the list.

- e) Click **Save Object**.

The object is created and added to the Destination field.

Step 5 Select **Do Not Decrypt** in the **Action** field.

Step 6 Click **Save Policy**.

Troubleshooting TLS/SSL Decryption

In general, if users have trouble connecting to a TLS/SSL server after you turn on decryption for the site, you have the following options:

- If the certificate is untrusted, add it to the supplemental certificate store. You can also relax this restriction and allow these transactions by selecting **Deny Transactions to Servers; Using an Untrusted Certificate: Off** in the decryption settings.
- If the certificate is invalid, and you control the target server, check the server's time settings and ensure they are consistent with the CX time settings. Using NTP is advised. The invalid certificate might not be valid yet, or it might have expired. (Replace expired certificates.)
- Many sites simply do not support man-in-the-middle decryption. For these sites, create decryption policies that apply the Do Not Decrypt action to bypass them. For sites that prompt for certificates at the start of a connection, you can also allow the connection by selecting **Deny Transactions to Servers; If the secure session handshake fails: Off** in the decryption settings.

The following are common problem areas and resolution suggestions.

Hints from the user's client or browser

Look for warnings or errors from the user application or browser during the failed access attempt.

Client does not trust the local Certificate Authority (CA) certificate

Web browsers usually display a warning when they do not trust the certificate. However, other clients, such as Instant Messaging clients, might fail without displaying any warnings.

Ensure that the certificate ASA CX uses for decryption is installed on the clients. Installation procedures vary by browser.

ASA CX does not trust the server certificate

Look for TLS Abort events in Event Viewer for the user's access attempt. The error description should explain why the flow was denied.

If the error indicates that the server presented an untrusted or invalid certificate, explore the following possibilities.

- Invalid certificates can occur if the time settings are inconsistent between the server and the CX device. The invalid certificate might not be valid yet, or it might have expired. If you control the server, check the time settings and fix as necessary; replace expired certificates.
- For untrusted certificates, you can resolve the problem by uploading the certificate to the Certificates page (select **Configurations > Certificates**). For certificates issued by a certificate authority, examine the certificate hierarchy to determine if you should download a root or intermediate certificate to add to the Certificates page so that other sites that use certificates from the CA will be trusted. You can also relax this restriction and allow these transactions by selecting **Deny Transactions to Servers; Using an Untrusted Certificate: Off** in the decryption settings.



Tip All self-signed certificates will be untrusted until you add them on the Certificates page.

ASA CX fails to establish a TLS session with the server

Look for TLS Abort events in Event Viewer for the user's access attempt where the error indicates a handshake failure.

Handshake failures might indicate that the server uses strong encryption, which requires a 3DES/AES (K9) license. (If the K9 License Missing column for the event says Yes, you do not have the license installed.) If you can acquire the 3DES/AES (K9) license for your device, upload it and the problem should resolve itself. If you are not authorized to use the 3DES/AES (K9) license, you need to bypass decryption for the site.

Applications that prompt for a client certificate during the connection, such as iTunes, can also experience handshake failures.



Tip Keep in mind that many TLS/SSL applications will not work with man-in-the-middle decryption, including most financial web sites. You should configure your decryption policies to bypass decryption for any TLS/SSL sites you want to allow that will not work with this type of decryption. Selecting **Deny Transactions to Servers; If the Secure Sessions Handshake Fails: Off** in the decryption settings might also resolve some of these problems, if you are willing to relax this restriction.

Client fails to establish a TLS session with ASA CX

This problem should be rare. Ensure that the decryption certificate you uploaded or generated in the decryption settings will be recognized by the user clients you are decrypting.



PART **IV**

Configuring the ASA

- [Managing High Availability, page 307](#)
- [Interface Management, page 313](#)
- [Configuring Network Address Translation, page 343](#)
- [Configuring Access Policies, page 357](#)



Managing High Availability

The topics in this section describe configuring and managing failover, or High Availability, settings for designated pairs of devices.

- [About High Availability, page 307](#)
- [Configuring Devices for Failover, page 308](#)
- [Managing High Availability, page 308](#)

About High Availability

Cisco High Availability (HA) enables network-wide protection by providing fast recovery from faults that may occur in any part of the network. With Cisco High Availability, network hardware and software work together and enable rapid recovery from disruptions to ensure fault transparency to users and network applications.

In the context of this document, “high availability” is used more narrowly, usually referring to a pair of ASAs or CX modules operating in failover mode. In fact, “failover” and “high availability” are used somewhat interchangeably.

Configuring failover requires two identical ASAs connected to each other through a dedicated failover link and, optionally, a state link. The health of the active unit and its interfaces is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs.

Currently, PRSM supports only Active/Standby failover, where one unit is the active unit which passes traffic, and the standby unit does not actively pass traffic. When failover occurs, the active unit fails over to become the standby unit, which then becomes active and begins passing traffic. You can use Active/Standby failover for ASAs in single- or multiple-context mode.

Stateless and Stateful Failover

The ASA supports two types of failover, Stateless and Stateful.

With Stateless failover, when failover occurs, all active connections are dropped. Clients need to re-establish connections when the new active unit takes over.

With Stateful Failover, the active unit continually passes per-connection state information to the standby unit. When failover occurs, the same connection information is available on the new active unit. Supported end-user applications are not required to reconnect to keep the same communication session.

Configuring Devices for Failover

Configuring high availability on ASA CX devices requires two identical units connected to each other through a dedicated failover link, with one active unit passing traffic while the other unit waits in a standby state. The health of the active unit and its interfaces is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs and the standby unit begins processing traffic.

The following conditions must be met in order to configure two ASA CX devices for high availability:

- Both units must be the same model, have the same number and types of interfaces, and the same amount of RAM installed.
- Both units must be operating in the same mode (routed or transparent, single or multiple context). They must have the same major (first number) and minor (second number) software version.
- Each ASA CX must have the proper licenses.

You can use Cisco Prime Security Manager (PRSM) to manage and monitor pairs of ASA devices operating in Active/Standby failover mode. These devices can optionally include CX devices, which will also fail over. You also can manage CX modules as an HA pair if they reside in ASAs that are otherwise not supported, such as those configured in multiple-context mode. Each HA pair is managed as a unit.

Pairing Devices for Failover

Before [Adding an ASA High Availability Pair, on page 94](#)) to the inventory in PRSM, you must configure the pair of ASAs to operate together in failover mode. This is performed outside of PRSM; you can configure Active/Standby failover on two devices using the Adaptive Security Device Manager (ASDM) or the command-line interface (CLI):

- Using ASDM to configure the two devices is described in http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/asdm71/general/asdm_71_general_config/ha_failover.html.
- Using the CLI to configure the two devices is described in http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/ha_failover.html.

Managing High Availability

The High Availability page displays the failover properties configured on the selected device (preferably the active member of a failover pair), and lets you edit them.

Procedure

-
- Step 1** To manage failover configuration for a specific device, select **Configurations > Policies/Settings**.
- Step 2** Select the desired device: be sure **Devices** is chosen in the **Policies/Settings** view selector, and then select the device you want to manage from the Devices list.
This must be a device configured as the active member of an Active/Standby failover pair.
- Step 3** Click the **High Availability** tab to display the device's High Availability page.
The device's failover properties are presented in four sections: **Basic Configuration**, **Criteria**, **MAC Addresses**, and **Interfaces**.

- Step 4** Update the failover properties as necessary.
These properties are described in [High Availability Configuration Properties](#), on page 309.
- Step 5** Click **Save** to save the updated properties to this device; the other, secondary device is updated automatically.
-

High Availability Configuration Properties

The failover, or High Availability (HA), properties assigned to a device that is a member of a designated Active/Standby failover pair are displayed in four sections on the **High Availability** page.

The settings are the same for both devices, and can be viewed on the **High Availability** page for either. However, we recommend updating HA properties on the **High Availability** page for the currently active device.

Basic Configuration Properties

Expand this section to access the following basic failover configuration properties:

LAN Failover

The LAN failover settings are grouped at the top of the **Basic Configuration** section: **Interface**, **Logical Name**, **Active IP**, **Standby IP**, and **Subnet Mask**.

Interface

This read-only field presents the name of the physical interface assigned for failover communications during failover pair configuration. See [How to Configure High Availability](#), on page 44 for more information.

Logical Name

The name assigned to the failover-link interface for identification.

Active IP

The active IP address assigned to the interface. The IP address can be either an IPv4 or an IPv6 address; you cannot configure both types of addresses on the failover link interface.

Standby IP

The IP address used by the secondary unit to communicate with the primary unit. The IP address can be an IPv4 or an IPv6 address.

Subnet Mask

Depending upon the type of address specified for the **Active IP**, this is a subnet mask (IPv4 addresses) or a prefix length (IPv6 address) for the failover interface address. The name of the field changes depending upon the type of address specified in the **Active IP** field.

Stateful Failover

These optional settings let you configure stateful failover: **Interface**, **Logical Name**, **Active IP**, **Standby IP**, and **Subnet Mask**.

With the exception of the **Interface** field, these properties are identical to those described for the **LAN Failover** section. In this section, you can choose an unused interface to be assigned for Stateful Failover communications. If you choose the same interface specified in the **LAN Failover** section, the parameters in this section are copied from the **LAN Failover** section and cannot be modified.

HTTP Replication

Turn On to allow Stateful Failover to copy active HTTP sessions to the standby firewall. If you do not allow HTTP replication, HTTP connections are disconnected at failover. Disabling HTTP replication reduces the amount of traffic on the state link. However, enabling HTTP replication allows users to browse, stream and download files freely without interruption during a failover.

Key Parameters

The **Enable**, **Type** and **Key** properties let you enable encryption of the communications on the failover link.

- **Enable** – Turn On to enable encryption of communications over the link between the two HA devices. If Off, failover communications, including any passwords or keys in the configuration that are sent during command replication, will be in clear text.
- **Type** – Select **ASCII** or **HEX** to specify the encryption-key type.
- **Key** – Enter the key used to encrypt failover communications. If **ASCII** is the selected **Type**, provide the shared secret string of up to 63 letters, numbers and punctuation. For **HEX**, provide a 32-hexadecimal-character encryption string.

Criteria

The ASA sends “hello” packets out of each data interface to monitor interface health. The appliance also sends hello messages across the failover link to monitor unit health. If the ASA does not receive a hello packet from the corresponding interface on the peer unit for over half of the defined Hold time, then the additional interface testing begins. If a hello packet or a successful test result is not received within that specified Hold time, the interface is marked as failed. Failover occurs if the number of failed interfaces meets the specified **Fail On** criterion.

Decreasing the poll and Hold times enables the ASA to detect and respond to interface failures more quickly, but may consume more system resources. Increasing the poll and Hold times prevents the ASA from failing over on networks with higher latency.

Expand this section to access and define the following failover criteria, which are organized into three sections—**Interface Criteria (Fail On)**; **Poll Time (Unit Failover and Unit Hold Time)**; and **Interface Poll Time (Monitored Interfaces and Interface Hold Time)**:

Fail On

This value defines how many interfaces must fail on the active device in order to trigger failover; the meaning of this number is specified by the Number/Percentage selection. If you select **Number**, the **Fail On** value is the actual number of interfaces (from 1 to 250) that must fail to trigger failover. If you select **Percentage**, this value is the percentage of total interfaces on the device that must fail.

Unit Failover

This value defines the time interval between hello messages sent between the two units. Specify a value between 1 and 15 seconds, or between 200 and 999 milliseconds, depending on your choice in the second/millisecond drop-down menu.

Unit Hold Time

This is the time during which a unit must receive a hello message on the failover link, or else the unit begins the testing process for peer failure. The range is between 1 and 45 seconds, or between 800 and 999 milliseconds, depending on your choice in the second/millisecond drop-down menu. You cannot enter a value that is less than three times the **Unit Failover** poll time.

Monitored Interfaces

The amount of time between interface polls. The range is between 1 and 15 seconds, or 500 to 999 milliseconds, depending on your choice in the second/millisecond drop-down menu.

Interface Hold Time

The time during which a data interface must receive a hello message from a peer; after this interval the peer is declared failed. Valid values are from 5 to 75 seconds. This value must be at least five times the **Monitored Interfaces** value.

MAC Addresses

You can configure virtual MAC addresses for each interface to ensure that the secondary unit uses the correct MAC addresses when it is the active unit, even if it comes online before the primary unit. If you do not specify virtual MAC addresses, the failover pair uses the burned-in NIC addresses as the MAC addresses.

Expand this section to access virtual MAC address assignments for unused physical interfaces.

Click the **Add Interface MAC Address** button to provide Active and Standby MAC addresses for a specific physical interface. Select an existing interface/MAC address entry to edit or delete it—click the appropriate button.

When adding an interface MAC address, choose the interface in the **Physical Interface** field. When adding or editing an interface MAC address, provide an **Active MAC Address** and a **Standby MAC Address**.

Use the **Active MAC Address** field to manually assign a virtual MAC address to the interface. MAC addresses are provided in *H.H.H* format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE. You must also provide a **Standby MAC Address** for the interface.

Interfaces

Expand this section to access a list of monitored interfaces. You can manually configure a standby IP address for each monitored interface; this can be an IPv4 or an IPv6 address. You also can enable or disable health monitoring for each individual interface: click **True** or **False** in the **Monitored** column.



Interface Management

The topics in this section describe configuring and managing device interfaces.

- [Understanding Device Interfaces, page 313](#)
- [Managing Device Interfaces, page 317](#)

Understanding Device Interfaces

An interface is a point of connection between a security device and some other network device. Interfaces are initially disabled; thus, as an essential part of firewall configuration, interfaces must be enabled and configured to allow appropriate packet inspection and forwarding.

There are two types of interface: physical and logical, where a physical interface is the actual slot on the device into which a network cable is plugged, and a logical interface is a virtual port assigned to a specific physical port. Generally, physical ports are referred to as interfaces, while logical ports are referred to as subinterfaces, virtual interfaces, VLANs, or EtherChannels, depending on their function. The number and type of interfaces you can define varies with appliance model and type of license purchased.

Subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs. Because VLANs keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or security appliances. This feature is particularly useful in multiple-context mode, allowing you to assign unique interfaces to each context.

As a general rule, interfaces attach to router-based networks, and subinterfaces attach to switch-based networks. All subinterfaces must be associated with a physical interface that is responsible for routing allowed traffic correctly.

If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. The physical interface must be enabled for the subinterface to pass traffic, but do not name the physical interface to ensure it does not pass traffic. However, if you do want to let the physical interface pass untagged packets, you can name the interface as usual.

See [Managing Device Interfaces, on page 317](#) for additional information.

About EtherChannels

An EtherChannel, also called a port-channel interface, is a logical interface consisting of a bundle of individual Ethernet links (a channel group). This provides increased bandwidth and fault tolerance compared to the individual links. An EtherChannel interface is configured and used in the same manner as a single physical interface. You can configure up to 48 EtherChannels, each of which consists of between one and eight active Fast Ethernet, Gigabit Ethernet, or Ten-Gigabit Ethernet ports. Each interface assigned to an EtherChannel must be of the same type, speed, and duplex mode.

You cannot use a redundant interface as part of an EtherChannel, nor can you use an EtherChannel as part of a redundant interface. You cannot use the same physical interfaces in a redundant interface and an EtherChannel interface. You can, however, configure both types on the ASA if they do not use the same physical interfaces.

EtherChannel MAC Addressing

All interfaces that are part of a channel group share the same MAC address. This makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links. By default, the EtherChannel uses the MAC address of the lowest-numbered member interface as its MAC address.

Alternatively, you can manually configure a MAC address for the port-channel interface. We recommend doing so in case the channel interface membership changes. For example, if you remove the interface that provides the port-channel MAC address, the port-channel is assigned the MAC address of the next lowest numbered interface, causing traffic disruption. Manually assigning a unique MAC address to the EtherChannel interface prevents this disruption. (Note that in multiple-context mode, you can assign unique MAC addresses to interfaces assigned to an individual context, including EtherChannel interfaces.)

Management Only EtherChannel Interfaces

You can specify an EtherChannel group as a management-only interface, but note the following caveats:

- **Routed mode** – You must explicitly configure the EtherChannel to be Management Only. Any non-management interface added to the management-only port-channel is treated as a management port. If you add an interface already defined as management-only to the management-only group, that attribute is ignored on the physical interface. Similarly, you cannot designate an interface as management-only if it is already a member of a management-only port-channel.
- **Transparent mode** – In this mode, members of a management-only EtherChannel can themselves only be management-only ports. Thus, when a management-only member is added to a transparent-mode EtherChannel, the channel inherits the management-only designation, while the designation is removed from the member interface. Conversely, when such an interface is removed from the EtherChannel, the designation is restored on the individual interface.

Using an EtherChannel Interface as a Failover Link

If an EtherChannel interface is specified as a failover link, all state-sync traffic for that link will travel over a single physical interface. Should that physical interface fail, the state-sync traffic will then traverse another physical interface that is part of the EtherChannel aggregated link. If there are no remaining available physical interfaces in the EtherChannel link specified for failover, the ASA falls back to the redundant interface, if one is specified.

While an EtherChannel interface is being used as an active failover link, changes to that EtherChannel configuration are not allowed. You can change the EtherChannel configuration of that link only by disabling either the link or failover, as follows:

- Disable the EtherChannel link while the configuration changes are being made, and then reactivate it (failover will not occur while the link is disabled).
- Disable failover while the configuration changes are being made, and then re-enable it (failover will not occur in the interim).

**Note**

As with any other type of interface assigned as a failover link, the EtherChannel interface cannot be named. Further, none of the EtherChannel's member interfaces can be named.

EtherChannel Load Balancing

Traffic in an EtherChannel is distributed across the individual bundled links in a deterministic fashion; however, the load is not necessarily balanced equally across all the links. Instead, frames are forwarded on a specific link as a result of a hashing algorithm. This algorithm uses a specific field or combination of fields in the packet header to produce a fixed Result Bundle Hash (RBH) value that indicates which link to use.

The algorithm can use one or a combination of the following packet-header fields to determine link assignment: source IP address, destination IP address, source MAC address, destination MAC address, TCP/UDP port numbers, or VLAN IDs. The field combination used by the algorithm is chosen from the **Load Balancing** list in the **Advanced Information** section of the [EtherChannel Properties](#), on page 325 screen.

For example, suppose **Source MAC** is chosen: when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the source MAC address of each incoming packet. Therefore, to provide load balancing, packets from different hosts use different ports in the channel, but packets from the same host use the same port in the channel (and the MAC addresses learned by the device do not change).

Similarly, with destination MAC address forwarding, when packets are forwarded to an EtherChannel, each packet is distributed across the ports in the channel based on the packet's destination host MAC address. Thus, packets to the same destination are forwarded over the same port, and packets to a different destination are sent on a different port in the channel.

Therefore, when choosing a load-balancing option, use the option that provides the greatest variety in your configuration. For example, if most of the traffic on a channel is going only to a single MAC address, choosing the destination MAC address results in most of the traffic always using the same link in the channel. Alternatively, using source addresses or IP addresses might result in better load balancing, while a method that uses the source and destination addresses along with UDP or TCP port numbers can distribute traffic much differently.

Load Balancing Options

When defining an EtherChannel interface, choose one of the following **Load Balancing** options to specify the basis of load distribution:

- **Destination IP** – Load distribution is based on the destination's host IP address only; the source of the packets is not considered. Each packet with the same destination IP address is forwarded over the same link.
- **Destination IP and Layer 4 Port** – Load distribution is based on the destination host IP address and TCP/UDP port. This option offers more granularity and a little more complexity than destination IP address alone.
- **Destination Layer 4 Port** – Distribution is based on the destination port; that is, a TCP or UDP port and not a physical interface.

- **Destination MAC** – Load distribution is based on the destination host MAC address of incoming packets.
- **Source IP** – Based on source host IP address only.
- **Source IP and Layer 4 Port** – Source IP address and TCP/UDP port.
- **Source Layer 4 Port** – Source TCP/UDP port only.
- **Source MAC** – Source MAC address only.
- **Source and Destination IP** – Distribution is based on source and destination IP addresses—source and destination IP addresses are paired for hash calculations. This method provides more granularity than destination IP address; for example, packets to the same destination can be forwarded over different links in a port-channel if they are coming from a different IP source.
- **Source and Destination IP and Layer 4 Port** – Distribution calculation considers source and destination IP addresses, and TCP/UDP ports. Provides even greater granularity and distribution.
- **Source and Destination Layer 4 Port** – Load distribution is based on source and destination TCP/UDP port.
- **Source and Destination MAC** – Calculation is based on source and destination MAC address pairing.
- **VLAN Destination IP** – Destination IP address and VLAN ID pairing.
- **VLAN Destination IP and Layer 4 Port** – Combination of destination IP address, TCP/UDP port, and VLAN ID.
- **VLAN Source IP** – Source IP address and VLAN ID.
- **VLAN Source IP and Layer 4 Port** – Source IP address, TCP/UDP port, and VLAN ID.
- **VLAN Source and Destination IP** – Source and destination IP address, and VLAN ID.
- **VLAN Source and Destination IP and Layer 4 Port** – Source and destination IP address, TCP/UDP port, and VLAN ID.
- **VLAN Only** – VLAN ID only.

About Static Routes

A static route is a specific path to a particular destination network that is manually defined on the current device. Static routes are used in a variety of situations, and can be a quick and effective way to route data from one network to another when there is no dynamic route to the destination, or when use of a dynamic routing protocol is not feasible.

All routes have a value or “metric” that represents its priority of use. (This metric is also referred to as “administrative distance.”) When two or more routes to the same destination are available, devices use administrative distance to decide which route to use.

For static routes, the default metric value is one, which gives them precedence over routes from dynamic routing protocols. If you increase the metric to a value greater than that of a dynamic route, the static route operates as a back-up in the event that dynamic routing fails. For example, Open Shortest Path First (OSPF)-derived routes have a default administrative distance of 100. To configure a back-up static route that is overridden by an OSPF route, specify a metric value for the static route that is greater than 100. This is referred to as a “floating” static route.

There is a special kind of static route known as a default route, or a “zero-zero” route because all zeroes are used for both the destination address and subnet mask. The default static route serves as a catch-all gateway:

if there are no matches for a particular destination in the device's routing table, the default route is used. The default route generally includes a next-hop IP address or local exit interface.

Route Tracking Using SLAs

When you define an interface that uses DHCP or PPPoE, you can configure tracking of the DHCP or PPPoE learned default routes by configuring the security appliance to monitor service level agreements (SLAs). By monitoring the connectivity to a device on another network, you can track the availability of a primary route and install a backup route if the primary route fails.

For example, you can define a default route to an Internet service provider (ISP) gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable. This technique, called Dual ISP, provides security appliances with a form of high availability, which is a vital part of providing customers with the services to which they are entitled.

Without route tracking, there is no inherent mechanism for determining if the route is up or down. A static route remains in the routing table even if the next-hop gateway becomes unavailable, and is removed only if the associated interface on the security appliance goes down.

The security appliance performs route tracking by associating a route with a monitoring target that you specify during interface configuration. It monitors the target using ICMP echo requests, according to the configured parameters. If an echo reply is not received within a specified time period, the SLA monitor is considered down and the associated route is removed from the routing table. A previously configured backup route is used in place of the removed route.

Managing Device Interfaces

The Interfaces page displays the interfaces configured on the selected device, and lets you add, edit and delete them.

Each security device must be configured, and each active interface must be enabled. Inactive interfaces can be disabled. When disabled, the interface does not transmit or receive data, but its configuration information is retained.

If you bootstrapped a new security device, the set-up feature configures only the addresses and names associated with the inside interface. You must define the remaining interfaces on that device before you can specify access and translation rules for traffic traversing that security device.



Note

Transparent firewall mode allows only two interfaces to pass traffic; however, if your platform includes a dedicated management interface, you can use it (either the physical interface or a subinterface) as a third interface for management traffic.

Follow these general steps to manage security-device interface definitions.

Procedure

- Step 1** To manage interface configurations for a specific device, select **Configurations > Policies/Settings**.
- Step 2** Select the desired device: be sure **Devices** is chosen in the **Policies/Settings** view selector, and then select the device you want to manage from the Devices list.
- Step 3** Click the **Interfaces** tab to display the device's Interfaces page.

All interfaces currently defined on the device are displayed as a table.

Note If you intend to use an interface for failover, do not configure it; in particular, do not specify an interface Name, as this parameter disqualifies the interface from being used as the failover link. See [Managing High Availability, on page 308](#) for information about configuring failover interfaces.

Step 4 Add, edit and delete interface definitions, as follows:

- To add a new interface definition, click the Add button at the top of the table and choose:
 - **Add Subinterface** – Opens the [Subinterface Properties, on page 322](#) screen.
 - **Add EtherChannel Interface** – Opens the [EtherChannel Properties, on page 325](#) screen.
 - **Add Redundant Interface** – Opens the [Redundant Interface Properties, on page 328](#) screen.
 - **Add Bridge Group** – Opens the [Bridge Group Properties, on page 332](#) screen.

If an existing entry is highlighted in the table when you make your selection, the new definition is assigned to that interface as a sub-entry. If nothing is selected when you make your selection, the new definition is added to the bottom of the table. Also, depending on the entry selected in the table, one or more of these choices may not be available.

Note Basic physical interface definitions are acquired during device discovery. You cannot add physical interface definitions, but you can edit the existing definitions.

- To edit an interface definition, select the appropriate entry or sub-entry and click the Edit Interface button next to it. The particular edit-properties screen opened depends on the type of interface represented by the entry:
 - Physical Interface – See [Physical Interface Properties, on page 318](#) for more information about this screen.
 - Subinterface – See [Subinterface Properties, on page 322](#) for more information about this screen.
 - EtherChannel Interface – See [EtherChannel Properties, on page 325](#) for more information.
 - Redundant Interface – See [Redundant Interface Properties, on page 328](#) for more information.
 - Bridge Group – See [Bridge Group Properties, on page 332](#) for more information.
- To delete an interface definition, select the appropriate entry or sub-entry and click the Delete Interface button next to it.
You are asked to confirm the deletion.

Physical Interface Properties

The following properties are presented when you edit a physical interface definition.



Note

Basic physical interface definitions are acquired during device discovery. You cannot add physical interface definitions, you can only edit the existing definitions.

Name

Provide an identifier for this interface of up to 48 characters in length. The name should be a memorable name for the interface that relates to its use. However, if you are using failover, do not name interfaces that you are reserving for failover communications; this includes an EtherChannel intended for failover, as well as its member interfaces. Also, do not name interfaces intended for use as a member of a redundant-interface pair.



Note You can change the name of an interface after it has been defined. However, be aware that doing so on a deployed device configuration could affect a number of existing policies and objects. If you are notified of such a conflict when committing an interface name change, be sure to track and update all affected policies and objects.

Certain names are reserved for specific interfaces, in accordance with the interface naming conventions of the security appliance. As such, these reserved names enforce default, reserved security levels, as follows:

- **Inside** – Connects to your internal network. Must be the most secure interface.
- **DMZ** – *Demilitarized zone* attached to an intermediate interface, or perimeter network. Typically, DMZ interfaces are prefixed with “DMZ” to identify the interface type.
- **Outside** – Connects to an external network or the Internet. Must be the least secure interface.

Similarly, a subinterface name typically identifies its associated interface, in addition to its own unique identifier. For example, “DMZoobmgmt” could represent an out-of-band management network attached to the DMZ interface.

Description

An optional description for the interface of up to 240 characters.

Enable Interface

Turn On to enable this interface to pass traffic.

Traffic cannot traverse an interface of any type if the interface is not enabled. If you are defining a logical interface such as a subinterface, enable the physical interface it will be associated with before defining the subinterface. If you are defining a redundant interface or an EtherChannel interface, enable the member interfaces before defining the group interface.

In multiple-context mode, if you allocate a physical or logical interface to a context, the interface is enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, that interface is shut down in all contexts in which it shared.

Management Only

Turn On to reserve this interface for device administration. Only traffic for management of this device is accepted; pass-through traffic for other interfaces and devices is rejected.

You cannot set a Primary or Secondary ISP interface to be Management Only.

Defining a management-only EtherChannel interface has certain member-interface restrictions. See [About EtherChannels](#), on page 314 for more information.



Note Not available on devices in transparent mode.

Security Level

Specify the security level of the interface: enter a value between 0 (least secure) and 100 (most secure). The security appliance lets traffic flow freely from an inside network to an outside network (lower security level). Many other security features are affected by the relative security level of two interfaces.

- Outside interfaces are always 0.
- Inside interfaces are always 100.
- DMZ interfaces are between 1 and 99.

Interface ID

This read-only field displays the interface's physical port identifier, which includes network type, slot and port number, in the form: `type[slot/]port`. This is also the name by which subinterfaces can be associated with the interface

The network type displayed for a physical interface can be either Ethernet or GigabitEthernet; on the ASA 5580 and higher, TenGigabitEthernet is also available.

MTU

Specify the maximum packet size in bytes; that is, the maximum transmission unit (MTU). The value depends on the type of network connected to the interface. Valid values are 300 to 65535 bytes. Default is 1500 for all types except PPPoE, for which the default is 1492. The minimum MTU if configuring IPv6 is 1280. In multiple-context mode, set the MTU in the context configuration.

Interface IPv4 section

Expand this section to access IPv4 addressing options for this interface; these properties are described in [Interface: IPv4 Properties](#), on page 335.

Interface IPv6 section

Expand this section to access IPv6 addressing options for this interface; these properties are described in [Interface: IPv6 Properties](#), on page 339.

Advanced Information section

Expand this section to access the **Active MAC Address**, **Standby MAC Address** and **Enable Pause Frame** fields.

Active MAC Address / Standby MAC Address

You can use the **Active MAC Address** field to manually assign a private MAC address to the interface. MAC addresses are provided in *H.H.H* format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE.

If desired, you also can provide a **Standby MAC Address** for use with device-level failover. If the active unit fails over and the standby unit becomes active, the new active unit begins using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Enable Pause Frame

Turn On to enable pause (XOFF) frames for flow control on 1-Gigabit and 10-Gigabit Ethernet interfaces. The default settings are:

- For 1-Gigabit interfaces, high watermark is 24 KB, low watermark is 16 KB, and pause refresh threshold value is 26624 slots.
- For 10-Gigabit interfaces, high watermark is 128 KB, low watermark is 64 KB, and pause refresh threshold value is 26624 slots.

A “slot” is the amount of time needed to transmit 64 bytes, so the time per unit depends on the link speed. The link partner can resume traffic transmission after receiving an XON frame, or after the XOFF expires, as specified by this timer.

Hardware Configuration section

Expand this section to configure physical parameters for this interface; specifically **Duplex** mode and **Speed**.

By default, an interface uses an auto-detected speed and an auto-negotiated duplex mode. As long as the ASA interface and the connected device are configured with the same settings, the interface will operate using the maximum speed and full-duplex mode. However, you can use these options to statically configure interface speed and duplex mode.

Duplex

Choose the duplex mode for the interface: **Full**, **Half**, or **Auto**, depending on the interface type. (For TenGigabitEthernet interfaces, Duplex is automatically set to Full.)

Speed

Choose the speed (in bits per second) for the physical interface: **10**, **100**, **1000**, **10000** (set automatically for a TenGigabitEthernet interface), or **Auto**. The speeds available depend on the interface type.

Tags

Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.

Ticket ID

A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)

Subinterface Properties

Subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs. Because VLANs keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or security appliances. This feature is particularly useful in multiple-context mode, letting you assign unique interfaces to each context.



Note

If you use subinterfaces, you typically do not also want the physical interface to pass traffic, as the physical interface passes untagged packets. Because the physical interface must be enabled for the subinterface to pass traffic, do not name the physical interface to ensure it does not pass traffic. However, if you do want to let the physical interface pass untagged packets, you can name the interface as usual.

The following properties are presented when you add or edit a subinterface.

Name

Provide an identifier for this interface of up to 48 characters in length. The name should be a memorable name for the interface that relates to its use. However, if you are using failover, do not name interfaces that you are reserving for failover communications; this includes an EtherChannel intended for failover, as well as its member interfaces. Also, do not name interfaces intended for use as a member of a redundant-interface pair.



Note

You can change the name of an interface after it has been defined. However, be aware that doing so on a deployed device configuration could affect a number of existing policies and objects. If you are notified of such a conflict when committing an interface name change, be sure to track and update all affected policies and objects.

Certain names are reserved for specific interfaces, in accordance with the interface naming conventions of the security appliance. As such, these reserved names enforce default, reserved security levels, as follows:

- **Inside** – Connects to your internal network. Must be the most secure interface.
- **DMZ** – *Demilitarized zone* attached to an intermediate interface, or perimeter network. Typically, DMZ interfaces are prefixed with “DMZ” to identify the interface type.
- **Outside** – Connects to an external network or the Internet. Must be the least secure interface.

Similarly, a subinterface name typically identifies its associated interface, in addition to its own unique identifier. For example, “DMZoobmgmt” could represent an out-of-band management network attached to the DMZ interface.

Description

An optional description for the interface of up to 240 characters.

Enable Interface

Turn On to enable this interface to pass traffic.

Traffic cannot traverse an interface of any type if the interface is not enabled. If you are defining a logical interface such as a subinterface, enable the physical interface it will be associated with before defining the subinterface. If you are defining a redundant interface or an EtherChannel interface, enable the member interfaces before defining the group interface.

In multiple-context mode, if you allocate a physical or logical interface to a context, the interface is enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, that interface is shut down in all contexts in which it shared.

Management Only

Reserves this interface for device administration. Only traffic for management of this device is accepted; pass-through traffic for other interfaces and devices is rejected. You cannot set a primary or secondary service-provider interface to be Management Only. Defining a management-only EtherChannel interface has certain member-interface restrictions. See [EtherChannel Properties, on page 325](#) for more information.



Note Not available on devices in transparent mode.

Security Level

Specify the security level of the interface: enter a value between 0 (least secure) and 100 (most secure). The security appliance lets traffic flow freely from an inside network to an outside network (lower security level). Many other security features are affected by the relative security level of two interfaces.

- Outside interfaces are always 0.
- Inside interfaces are always 100.
- DMZ interfaces are between 1 and 99.

Physical Interface

Specify the physical interface to which this subinterface will be assigned—a list of previously defined interfaces is presented. If you do not see a desired interface ID, be sure that interface is defined and enabled.

Subinterface ID

Provide an integer between 1 and 4294967293 as the Subinterface ID. The number of subinterfaces allowed depends on your platform.

For subinterface port identification, this ID is appended to the specified **Physical Interface** Hardware Port. For example, *GigabitEthernet0.4* represents the subinterface assigned an ID of 4, operating on the port GigabitEthernet0.

VLAN ID

Provide a VLAN ID for this subinterface: enter a value between 1 and 4094. The specified VLAN ID must not be in use on any connected device.

Some VLAN IDs might be reserved on connected switches; see the switch documentation for more information. In multiple-context mode, you can only set the VLAN ID in the system configuration.



Note

A value of zero in this field removes the VLAN designation.

MTU

Specify the maximum packet size in bytes; that is, the maximum transmission unit (MTU). The value depends on the type of network connected to the interface. Valid values are 300 to 65535 bytes. Default is 1500 for all types except PPPoE, for which the default is 1492. The minimum MTU if configuring IPv6 is 1280. In multiple-context mode, set the MTU in the context configuration.

Interface IPv4 section

Expand this section to access IPv4 addressing options for this interface; these properties are described in [Interface: IPv4 Properties](#), on page 335.

Interface IPv6 section

Expand this section to access IPv6 addressing options for this interface; these properties are described in [Interface: IPv6 Properties](#), on page 339.

Advanced Information section

Expand this section to access the **Active MAC Address** and **Standby MAC Address** fields.

Active MAC Address / Standby MAC Address

You can use the **Active MAC Address** field to manually assign a private MAC address to the interface. MAC addresses are provided in *H.H.H* format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE.

If desired, you also can provide a **Standby MAC Address** for use with device-level failover. If the active unit fails over and the standby unit becomes active, the new active unit begins using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Tags

Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.

Ticket ID

A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)

EtherChannel Properties

An EtherChannel interface is configured and used in the same manner as a single physical interface. You can configure up to 48 EtherChannels, each of which consists of between one and eight active Fast Ethernet, Gigabit Ethernet, or Ten-Gigabit Ethernet ports. Each interface assigned to an EtherChannel must be of the same type, speed and duplex mode. See [About EtherChannels](#), on page 314 for more information.



Note

You cannot use a redundant interface as part of an EtherChannel, nor can you use an EtherChannel as part of a redundant interface. You cannot use the same physical interfaces in a redundant interface and an EtherChannel interface. You can, however, configure both types on the ASA if they do not use the same physical interfaces.

The following properties are presented when you add or edit an EtherChannel.

Name

Provide an identifier for this interface of up to 48 characters in length. The name should be a memorable name for the interface that relates to its use. However, if you are using failover, do not name interfaces that you are reserving for failover communications; this includes an EtherChannel intended for failover, as well as its member interfaces. Also, do not name interfaces intended for use as a member of a redundant-interface pair.



Note

You can change the name of an interface after it has been defined. However, be aware that doing so on a deployed device configuration could affect a number of existing policies and objects. If you are notified of such a conflict when committing an interface name change, be sure to track and update all affected policies and objects.

Certain names are reserved for specific interfaces, in accordance with the interface naming conventions of the security appliance. As such, these reserved names enforce default, reserved security levels, as follows:

- **Inside** – Connects to your internal network. Must be the most secure interface.
- **DMZ** – *Demilitarized zone* attached to an intermediate interface, or perimeter network. Typically, DMZ interfaces are prefixed with “DMZ” to identify the interface type.
- **Outside** – Connects to an external network or the Internet. Must be the least secure interface.

Similarly, a subinterface name typically identifies its associated interface, in addition to its own unique identifier. For example, “DMZoobmgmt” could represent an out-of-band management network attached to the DMZ interface.

Description

An optional description for the interface of up to 240 characters.

Enable Interface

Turn On to enable this interface to pass traffic.

Traffic cannot traverse an interface of any type if the interface is not enabled. If you are defining a logical interface such as a subinterface, enable the physical interface it will be associated with before defining the subinterface. If you are defining a redundant interface or an EtherChannel interface, enable the member interfaces before defining the group interface.

In multiple-context mode, if you allocate a physical or logical interface to a context, the interface is enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, that interface is shut down in all contexts in which it shared.

Management Only

Reserves this interface for device administration. Only traffic for management of this device is accepted; pass-through traffic for other interfaces and devices is rejected. You cannot set a primary or secondary service-provider interface to be Management Only. Defining a management-only EtherChannel interface has certain member-interface restrictions. See [EtherChannel Properties](#), on page 325 for more information.



Note Not available on devices in transparent mode.

Security Level

Specify the security level of the interface: enter a value between 0 (least secure) and 100 (most secure). The security appliance lets traffic flow freely from an inside network to an outside network (lower security level). Many other security features are affected by the relative security level of two interfaces.

- Outside interfaces are always 0.
- Inside interfaces are always 100.
- DMZ interfaces are between 1 and 99.

EtherChannel ID

Provide an identifier for this EtherChannel; valid IDs are the integers from 1 to 48. This number is appended to “port-channel” to identify the EtherChannel in the Interface column of the table on the Interfaces page.

Add Interfaces

Specify the members of this port-channel group by selecting one or more available interfaces.

You can assign up to 16 interfaces to a channel group. In a standard EtherChannel, up to eight of these interfaces can be active, while the remaining interfaces act as stand-by links in case of individual interface failure. Alternatively, you can create a static EtherChannel by turning On **LACP Mode** (in the **Advanced Information** section, as described below), which means all interfaces in the group can pass traffic.



Note All interfaces in the channel group must be the same type and speed. The first interface added to the channel group determines the correct type and speed.

MTU

Specify the maximum packet size in bytes; that is, the maximum transmission unit (MTU). The value depends on the type of network connected to the interface. Valid values are 300 to 65535 bytes. Default is 1500 for all types except PPPoE, for which the default is 1492. The minimum MTU if configuring IPv6 is 1280. In multiple-context mode, set the MTU in the context configuration.

Interface IPv4 section

Expand this section to access IPv4 addressing options for this interface; these properties are described in [Interface: IPv4 Properties, on page 335](#).

Interface IPv6 section

Expand this section to access IPv6 addressing options for this interface; these properties are described in [Interface: IPv6 Properties, on page 339](#).

Advanced Information section

Expand this section to access the **Load Balancing**, **LACP Mode**, **Active Interface**, **Active MAC Address**, and **Standby MAC Address** fields.

Load Balancing

Choose an EtherChannel load-balancing algorithm; see [EtherChannel Load Balancing, on page 315](#) for more information about this option.

LACP Mode

Select the desired Link Aggregation Control Protocol (LACP) mode; the default is On, which means all interfaces can pass traffic.

Active Interface

Specify the minimum and maximum number of active physical interfaces for this EtherChannel by choosing from and to values.

As mentioned, an EtherChannel can consist of between one and eight active links, with up to 16 assigned to the group. Use these values to indicate the minimum and maximum number of interfaces that can be active in this channel group at any given time.

Active MAC Address / Standby MAC Address

You can use the **Active MAC Address** field to manually assign a private MAC address to the interface. MAC addresses are provided in *H.H.H* format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE.

If desired, you also can provide a **Standby MAC Address** for use with device-level failover. If the active unit fails over and the standby unit becomes active, the new active unit begins using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Hardware Configuration section

Expand this section to configure physical parameters for this interface; specifically **Duplex** mode and **Speed**.

By default, an interface uses an auto-detected speed and an auto-negotiated duplex mode. As long as the ASA interface and the connected device are configured with the same settings, the interface will operate using the maximum speed and full-duplex mode. However, you can use these options to statically configure interface speed and duplex mode.

Duplex

Choose the duplex mode for the interface: **Full**, **Half**, or **Auto**, depending on the interface type. (For TenGigabitEthernet interfaces, Duplex is automatically set to Full.)

Speed

Choose the speed (in bits per second) for the physical interface: **10**, **100**, **1000**, **10000** (set automatically for a TenGigabitEthernet interface), or **Auto**. The speeds available depend on the interface type.

Tags

Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.

Ticket ID

A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)

Redundant Interface Properties

You can define logical “redundant” interfaces to increase security appliance reliability. A redundant interface is a specific pair of physical interfaces, with one designated as active (or primary) and the other as standby (or secondary). If the active interface fails, the standby interface becomes active and starts passing traffic. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover, if desired. You can configure up to eight redundant interface pairs.

A redundant interface functions as a single interface (inside, outside, etc.), with only one of the member pair active at any one time. This redundant interface is configured normally, with a unique interface name, security level and IP address. Note that each member interface must be of the same type (e.g., GigabitEthernet), and

cannot have a name, security level, or IP address assigned. In fact, do not configure any options other than Duplex and Speed on the member interfaces.

The redundant interface uses the MAC address of the first physical interface that you specify. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. Alternatively, you can explicitly assign a MAC address to the redundant interface; this address is then used regardless of the member interface MAC addresses. In either case, when the active interface fails over to the standby, the same MAC address is maintained so that traffic is not disrupted.

The following properties are presented when you add or edit a redundant interface.

Name

Provide an identifier for this interface of up to 48 characters in length. The name should be a memorable name for the interface that relates to its use. However, if you are using failover, do not name interfaces that you are reserving for failover communications; this includes an EtherChannel intended for failover, as well as its member interfaces. Also, do not name interfaces intended for use as a member of a redundant-interface pair.



Note You can change the name of an interface after it has been defined. However, be aware that doing so on a deployed device configuration could affect a number of existing policies and objects. If you are notified of such a conflict when committing an interface name change, be sure to track and update all affected policies and objects.

Certain names are reserved for specific interfaces, in accordance with the interface naming conventions of the security appliance. As such, these reserved names enforce default, reserved security levels, as follows:

- **Inside** – Connects to your internal network. Must be the most secure interface.
- **DMZ** – *Demilitarized zone* attached to an intermediate interface, or perimeter network. Typically, DMZ interfaces are prefixed with “DMZ” to identify the interface type.
- **Outside** – Connects to an external network or the Internet. Must be the least secure interface.

Similarly, a subinterface name typically identifies its associated interface, in addition to its own unique identifier. For example, “DMZoobmgmt” could represent an out-of-band management network attached to the DMZ interface.

Description

An optional description for the interface of up to 240 characters.

Enable Interface

Turn On to enable this interface to pass traffic.

Traffic cannot traverse an interface of any type if the interface is not enabled. If you are defining a logical interface such as a subinterface, enable the physical interface it will be associated with before defining the subinterface. If you are defining a redundant interface or an EtherChannel interface, enable the member interfaces before defining the group interface.

In multiple-context mode, if you allocate a physical or logical interface to a context, the interface is enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, that interface is shut down in all contexts in which it shared.

Security Level

Specify the security level of the interface: enter a value between 0 (least secure) and 100 (most secure). The security appliance lets traffic flow freely from an inside network to an outside network (lower security level). Many other security features are affected by the relative security level of two interfaces.

- Outside interfaces are always 0.
- Inside interfaces are always 100.
- DMZ interfaces are between 1 and 99.

Redundant ID

Provide an identifier for this redundant interface; valid IDs are the integers from 1 to 8.

Primary Interface

Choose the primary member of the redundant interface pair from this list of available interfaces. Available interfaces are presented by hardware port IDs, as named interfaces cannot be used for a redundant interface pair.

Secondary Interface

Choose the secondary member of the redundant interface pair from this list of available interfaces. Available interfaces are presented by hardware port IDs, as named interfaces cannot be used for a redundant interface pair.



Note Member interfaces must be enabled and of the same type (e.g., GigabitEthernet), and cannot have a Name, IP Address, or Security Level assigned. In fact, do not configure any options other than Duplex and Speed on the member interfaces.

MTU

Specify the maximum packet size in bytes; that is, the maximum transmission unit (MTU). The value depends on the type of network connected to the interface. Valid values are 300 to 65535 bytes. Default is 1500 for all types except PPPoE, for which the default is 1492. The minimum MTU if configuring IPv6 is 1280. In multiple-context mode, set the MTU in the context configuration.

Interface IPv6 section

Expand this section to access the **Enforce EUI 64** and **Link-Local Address** options.

Enforce EUI 64

When On, use of Modified EUI-64 format interface identifiers in IPv6 addresses on a local link is enforced.

When this option is enabled on an interface, the source addresses of IPv6 packets received on the interface are verified against the source MAC addresses to ensure that the interface identifiers use the Modified EUI-64 format. If the interface identifier in an IPv6 packet is not in the Modified EUI-64 format, the packet is dropped and the following system log message is generated:

```
%PIX|ASA-3-325003: EUI-64 source address check failed.
```

Address format verification is performed only when a flow is created. Packets from an existing flow are not checked. Additionally, address verification can be performed only for hosts on the local link. Packets received from hosts behind a router will fail the address format verification, and be dropped, because their source MAC address will be the router MAC address and not the host MAC address.

The Modified EUI-64 format interface identifier is derived from the 48-bit link-layer (MAC) address by inserting the hex number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link-layer address. To ensure the chosen address is from a unique Ethernet MAC address, the next-to-lowest order bit in the high-order byte is inverted (universal/local bit) to indicate the uniqueness of the 48-bit address. For example, an interface with a MAC address of 00E0.B601.3B7A would have a 64-bit interface ID of 02E0:B6FF:FE01:3B7A.

Link-Local Address

To override the link-local address that is automatically generated for the interface, enter the desired IPv6 link-local address in this field.

The link-local address is composed of the link-local prefix FE80::/64 and the interface ID in Modified EUI-64 format. For example, an interface with a MAC address of 00E0.B601.3B7A would have a link-local address of FE80::2E0:B6FF:FE01:3B7A. An error will occur if another host is using the specified address.

Advanced Information section

Expand this section to access the **Active MAC Address** and **Standby MAC Address** fields.

Active MAC Address / Standby MAC Address

You can use the **Active MAC Address** field to manually assign a private MAC address to the interface. MAC addresses are provided in *H.H.H* format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE.

If desired, you also can provide a **Standby MAC Address** for use with device-level failover. If the active unit fails over and the standby unit becomes active, the new active unit begins using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Tags

Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.

Ticket ID

A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)

Bridge Group Properties

A transparent firewall connects the same network on its inside and outside interfaces, and supports only the two interfaces per context. However, you can increase the number of interfaces available to a context through use of bridge groups. You can configure up to eight bridge groups, and each group can contain four interfaces.

Each bridge group connects to a separate network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the security appliance—traffic must exit the security appliance to be routed by an external device back to another bridge group in the security appliance.

You might want to use more than one bridge group if you do not want the overhead of security contexts, or want to maximize your use of security contexts. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context.

The following properties are presented when you add or edit a bridge group on a security appliance running in transparent mode.

Bridge Group ID**Description**

An optional description for the interface of up to 240 characters.

IP Address / Subnet Mask

Provide a static **IP Address** (IPv4) and **Subnet Mask** that represents the security device on this interface's connected network. The IP address must be unique for each interface.

The Subnet mask can be expressed in dotted decimal format (for example, 255.255.255.0), or by entering the number of bits in the network mask (for example, 24). Do not use 255.255.255.254 or 255.255.255.255 for an interface connected to the network because this will stop traffic on that interface. If you omit the Subnet Mask value, a "classful" network is assumed, as follows:

- The Class A netmask (255.0.0.0) is assumed if the first octet of the IP Address is 1 through 126 (that is, addresses 1.0.0.0 through 126.255.255.255).
- The Class B netmask (255.255.0.0) is assumed if the first octet of the IP Address is 128 through 191 (that is, addresses 128.0.0.0 through 191.255.255.255).
- The Class C netmask (255.255.255.0) is assumed if the first octet of the IP Address is 192 through 223 (that is, addresses 192.0.0.0 through 223.255.255.255).



Note

Do not use addresses previously used for routers, hosts, or any other firewall device commands, such as an IP address in the global pool or a static NAT entry.

Enable IPv6

Turn On to enable IPv6 addressing on this interface; an IPv6 link-local unicast address is also configured on the interface. You can turn this option Off to disable IPv6 on the interface, but retain the configuration information.

DAD Attempts

To specify the number of consecutive neighbor solicitation messages that are sent on an interface during duplicate address detection (DAD), enter a number from 0 to 600 in this field. Entering 0 disables duplicate address detection on the interface. Entering 1 configures a single transmission without follow-up transmissions; this is the default.

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to **DUPLICATE** and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message similar to the following is issued:

```
%PIX-4-DUPLICATE: Duplicate address FE80::1 on outside
```

If the duplicate address is a global address of the interface, the address is not used and an error message is issued, similar to that shown previously for a duplicate link-local address.

All configuration commands associated with the duplicate address remain as-configured while the state of the address is set to **DUPLICATE**. If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address, and all other IPv6 address associated with the interface are regenerated (that is, duplicate address detection is performed only on the new link-local address).

NS Interval

The interval between IPv6 neighbor solicitation retransmissions, in milliseconds. Valid values range from 1000 to 3600000 milliseconds; the default value is 1000 milliseconds.



Note This value is included in all IPv6 router advertisements sent out on this interface.

Reachable Time

The amount of time, in milliseconds, within which a remote IPv6 node is considered still reachable, after initial reachability was confirmed. Valid values range from 0 to 3600000 milliseconds, the default value is 0. When 0 is used for the value, the reachable time is set as undetermined—it is up to the receiving devices to set and track reachable time.

A configured time enables detection of unavailable neighbors. A shorter time allows detecting unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

Interface IPv6 Addresses section

Expand this section to access the static IPv6 addresses assigned to this interface.

To add an IPv6 address entry to this list, click the **Add more interface IPv6 Address** button and then enter the **Address**. If this address is in EUI-64 format, turn **On** the **EUI-64** property.

Tags

Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.

Ticket ID

A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)

Interface: IPv4 Properties

Each of the various add-interface and edit-interface screens (Physical, Subinterface, and so on) include an **Interface IPv4** section that you can expand to configure IPv4 addressing on that interface. The properties available in the **Interface IPv4** section are described here.

IP Type

Choose a method of address assignment for the interface—**Use Static IP**, **Use DHCP**, or **Use PPPoE**—and then provide related parameters.

- **Use Static IP** – Provide an **IP Address** and **Subnet Mask**.
- **Use DHCP** – Enables Dynamic Host Configuration Protocol (DHCP) for automatic assignment of an IP address from a DHCP server on the connected network. The following options become available: **Use DHCP Type**, **Obtain default route using DHCP**, **DHCP route metric**, **Enable Tracking DHCP**, **DHCP Broadcast Flag**, and **DHCP Monitoring**.
- **Use PPPoE** – Enables Point-to-Point Protocol over Ethernet (PPPoE) for automatic assignment of an IP address from a PPPoE server on the connected network; this option is not supported with failover, and it is available in single-context mode only. The following options become available: **VPDN Group Name**, **PPPoE User Name**, **PPPoE Password**, **Confirm Password**, **PPP Authentication**, **PPPoE Route Metric**, **Enable Route Settings**, and **Store in Flash**.



Note

You can configure DHCP and PPPoE only on the outside interface of a security appliance.

IP Address / Subnet Mask

Provide a static **IP Address** (IPv4) and **Subnet Mask** that represents the security device on this interface's connected network. The IP address must be unique for each interface.

The Subnet mask can be expressed in dotted decimal format (for example, 255.255.255.0), or by entering the number of bits in the network mask (for example, 24). Do not use 255.255.255.254 or 255.255.255.255 for an interface connected to the network because this will stop traffic on that interface. If you omit the Subnet Mask value, a “classful” network is assumed, as follows:

- The Class A netmask (255.0.0.0) is assumed if the first octet of the IP Address is 1 through 126 (that is, addresses 1.0.0.0 through 126.255.255.255).
- The Class B netmask (255.255.0.0) is assumed if the first octet of the IP Address is 128 through 191 (that is, addresses 128.0.0.0 through 191.255.255.255).
- The Class C netmask (255.255.255.0) is assumed if the first octet of the IP Address is 192 through 223 (that is, addresses 192.0.0.0 through 223.255.255.255).



Note

Do not use addresses previously used for routers, hosts, or any other firewall device commands, such as an IP address in the global pool or a static NAT entry.

Use DHCP Type

When **Use DHCP** is the chosen **IP Type**, select the type of address to be used for identification of this device: its **MAC Address** or a **Cisco Interface** generated address.

Select **MAC Address** to force the interface MAC address to be stored inside a DHCP request packet for option 61. Select **Cisco Interface** to use a generated string for option 61; this string is the concatenation of “Cisco” with the interface MAC address, the interface name, and the host name, in the form `Cisco-<MAC_address>-<interface_name>-<host>`.

Obtain default route using DHCP

Select this option to obtain a default route from the DHCP server so that you do not need to configure a default static route.

DHCP Route Metric

Assign an administrative distance to the learned route. Valid values are 1 to 255. The administrative distance for learned routes defaults to 1.

All routes have a value or “metric” that represents its priority of use. (This metric is also referred to as “administrative distance.”) When two or more routes to the same destination are available, devices use administrative distance to decide which route to use.

Enable Tracking DHCP

Turn this option On to enable DHCP route tracking via a specific Service Level Agreement (SLA) monitor. The following options becomes available: **Track ID**, **Track IP Address**, and **SLA ID**.



Note Route tracking is available only in single, routed mode.

Track ID

Required if **Enable Tracking DHCP** is On. Provide a unique identifier for the route-tracking process. Valid values are 1 to 500.

Track IP Address

Required if **Enable Tracking DHCP** is On. Enter the IP address of the destination being tracked. Typically, this would be the IP address of the next hop for the route, but it can be any network object available from this interface.

SLA ID

Required if **Enable Tracking DHCP** is On. Enter the name of the SLA monitor object that defines the route tracking (connectivity monitoring) to be applied to this interface. Valid values are 1 to 2417483647.

DHCP Broadcast Flag

Turn On to set the broadcast flag in the DHCP header to one in discover requests sent by the DHCP client for an IP address. The DHCP server broadcasts the reply if this is On; otherwise the flag is set to zero and replies are unicast.

DHCP Monitoring

Turn On to enable SLA track monitoring.

VPDN Group Name

Enter a name of up to 63 characters for the Virtual Private Dialup Network (VPDN) group that will contain the authentication method and user name/password to use for network connection, negotiation and authentication.

PPPoE User Name

Enter the user name to assign to the VPDN group. The PPPoE user name and password are generally provided by your network service provider.

PPPoE Password

Enter the password to use with the **PPPoE User Name**.

Confirm Password

Re-enter the password.

PPPoE Authentication

Choose the type of authentication used for this PPPoE connection:

- **PAP** – Password Authentication Protocol, with exchange of credentials in clear text.
- **CHAP** – Challenge Handshake Authentication Protocol, with encrypted credential exchange.
- **MS-CHAP** – Microsoft's CHAP, version 1 only.

PPPoE Route Metric

Assign an administrative distance to the learned route. Valid values are 1 to 255; defaults to 1.

All routes have a value or “metric” that represents its priority of use. (This metric is also referred to as “administrative distance.”) When two or more routes to the same destination are available, devices use administrative distance to decide which route to use.

Tracking PPPoE

Turn this option On to enable PPPoE route tracking via a specific Service Level Agreement (SLA) monitor. The following options becomes available: **Track ID**, **Track IP Address**, and **SLA ID**.



Note Route tracking is available only in single, routed mode.

Track ID

Required if **Tracking PPPoE** is On. Provide a unique identifier for the route-tracking process. Valid values are 1 to 500.

Track IP Address

Required if **Tracking PPPoE** is On. Enter the IP address of the destination being tracked. Typically, this would be the IP address of the next hop for the route, but it can be any network object available from this interface.

SLA ID

Required if **Tracking PPPoE** is On. Enter the name of the SLA monitor object that defines the route tracking (connectivity monitoring) to be applied to this interface. Valid values are 1 to 2417483647.

Enable Route Settings

Turn On to enable PPPoE with a fixed IP address, and provide an **IP Address** and **Subnet Mask**. This causes the security device to use the specified address instead of negotiating with the PPPoE server to assign an address dynamically.

Store in Flash

When On, the provided PPPoE user information is stored in the device's local flash memory, ensuring it cannot be inadvertently overwritten.

Interface: IPv6 Properties

Each of the various add-interface and edit-interface screens (Physical, Subinterface, and so on) include an **Interface IPv6** section that you can expand to configure IPv6 addressing on that interface. The properties available in the **Interface IPv6** section are described here.

Enable IPv6

Turn On to enable IPv6 addressing on this interface; an IPv6 link-local unicast address is also configured on the interface. You can turn this option Off to disable IPv6 on the interface, but retain the configuration information.

Enforce EUI 64

When On, use of Modified EUI-64 format interface identifiers in IPv6 addresses on a local link is enforced.

When this option is enabled on an interface, the source addresses of IPv6 packets received on the interface are verified against the source MAC addresses to ensure that the interface identifiers use the Modified EUI-64 format. If the interface identifier in an IPv6 packet is not in the Modified EUI-64 format, the packet is dropped and the following system log message is generated:

```
%PIX|ASA-3-325003: EUI-64 source address check failed.
```

Address format verification is performed only when a flow is created. Packets from an existing flow are not checked. Additionally, address verification can be performed only for hosts on the local link. Packets received from hosts behind a router will fail the address format verification, and be dropped, because their source MAC address will be the router MAC address and not the host MAC address.

The Modified EUI-64 format interface identifier is derived from the 48-bit link-layer (MAC) address by inserting the hex number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link-layer address. To ensure the chosen address is from a unique Ethernet MAC address, the next-to-lowest order bit in the high-order byte is inverted (universal/local bit) to indicate the uniqueness of the 48-bit address. For example, an interface with a MAC address of 00E0.B601.3B7A would have a 64-bit interface ID of 02E0:B6FF:FE01:3B7A.

Link-Local Address

To override the link-local address that is automatically generated for the interface, enter the desired IPv6 link-local address in this field.

The link-local address is composed of the link-local prefix FE80::/64 and the interface ID in Modified EUI-64 format. For example, an interface with a MAC address of 00E0.B601.3B7A would have a link-local address of FE80::2E0:B6FF:FE01:3B7A. An error will occur if another host is using the specified address.

Autoconfiguration

Turn On to enable the device to perform IPv6 stateless address auto-configuration to discover prefixes on the link, and then to add the EUI-64 based addresses to the interface. Addresses are configured depending on the prefixes received in Router Advertisement (RA) messages.

If a link-local address has not been configured, then one is automatically generated for this interface. An error occurs if another host is already using the generated link-local address.

Enable DHCP for Address Configuration

Turn On to allow the interface to learn its IPv6 address dynamically from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server.

Enable DHCP for Non-address Configuration

Turn On to allow the interface to attempt to acquire other non-address configuration information, such as DNS or NTP server addresses, from available DHCPv6 servers.

Interface IPv6 Addresses section

Expand this section to access the static IPv6 addresses assigned to this interface.

To add an IPv6 address entry to this list, click the **Add more interface IPv6 Address** button and then enter the **Address**. If this address is in EUI-64 format, turn **On** the **EUI-64** property.

Interface IPv6 Prefix section

Expand this section to specify IPv6 prefixes (that is, the network portion of the IPv6 addresses) assigned to this interface included in IPv6 Router Advertisements.

To add an IPv6 prefix entry to this list, click the **Add more interface IPv6 Prefix** button and then specify the desired IPv6 **Address**, **Advertisement**, **Off Link**, **Auto-configuration**, **Prefix Lifetime**, **Preferred Lifetime/Date**, and **Valid Lifetime/Date**.

- **Address** – Provide the IPv6 network number to include in Router Advertisement (RA) messages. The Default keyword means default values are used for lifetime and preference expiration.
- **Advertisement** – When Off, RA messages are suppressed, and the remaining options in this section are hidden.
- **Off Link** – When this option is On, the specified prefix is not used for on-link determination.
- **Auto-configuration** – If Off, hosts on the local link cannot use the specified prefix for IPv6 auto-configuration.
- **Prefix Lifetime** – Specify how the specified IPv6 prefix is advertised as preferred and valid: select Duration to enter lengths of time, or select Expiration to provide dates and times at which advertising expires.
- **Preferred Lifetime/Date** – If **Prefix Lifetime** is Duration, enter the amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred. The range is from 60 to 4,294,967,295; the default is 604,800 seconds (7 days). If **Prefix Lifetime** is Expiration, enter the date and time when preferred advertising ends.
- **Valid Lifetime/Date** – If **Prefix Lifetime** is Duration, enter the amount of time (in seconds) that the specified IPv6 prefix is advertised as being valid. The amount of time (in seconds) that the specified IPv6 prefix is advertised as being valid. The range is from 60 to 4,294,967,295; the default is 2,592,000 seconds (30 days). If **Prefix Lifetime** is Expiration, enter the date and time when valid advertising ends.

Settings section

Expand this section to define various Router Advertisement (RA) and neighbor solicitation settings for this interface: **DAD Attempts**, **NS Interval**, **Reachable Time**, **Enable RA**, **RA Lifetime**, and **RA Interval**.

DAD Attempts

To specify the number of consecutive neighbor solicitation messages that are sent on an interface during duplicate address detection (DAD), enter a number from 0 to 600 in this field. Entering 0 disables duplicate address detection on the interface. Entering 1 configures a single transmission without follow-up transmissions; this is the default.

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message similar to the following is issued:

```
%PIX-4-DUPLICATE: Duplicate address FE80::1 on outside
```

If the duplicate address is a global address of the interface, the address is not used and an error message is issued, similar to that shown previously for a duplicate link-local address.

All configuration commands associated with the duplicate address remain as-configured while the state of the address is set to DUPLICATE. If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address, and all other IPv6 address associated with the interface are regenerated (that is, duplicate address detection is performed only on the new link-local address).

NS Interval

The interval between IPv6 neighbor solicitation retransmissions, in milliseconds. Valid values range from 1000 to 3600000 milliseconds; the default value is 1000 milliseconds.



Note This value is included in all IPv6 router advertisements sent out on this interface.

Reachable Time

The amount of time, in milliseconds, within which a remote IPv6 node is considered still reachable, after initial reachability was confirmed. Valid values range from 0 to 3600000 milliseconds, the default value is 0. When 0 is used for the value, the reachable time is set as undetermined—it is up to the receiving devices to set and track reachable time.

A configured time enables detection of unavailable neighbors. A shorter time allows detecting unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

Enable RA

Turn On to enable Router Advertisements (RAs) on this interface.

RA Lifetime

The “router lifetime” value specifies how long nodes on the local link should consider the security appliance as the default router on the link. Valid values range from 0 to 9000 seconds; the default is 1800 seconds. Entering 0 indicates that the security appliance should not be considered a default router on the selected interface.

Any non-zero value should not be less than the following RA Interval value.

**Note**

This value is included in all IPv6 router advertisements sent out on this interface.

RA Interval

The interval between IPv6 router advertisement transmissions on this interface. Valid values range from 3 to 1800 seconds, (or from 500 to 1800000 milliseconds if the following RA Interval in Milliseconds option is checked); the default is 200 seconds.

The interval between transmissions should be less than or equal to the RA Lifetime value if it is non-zero. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the desired value.



Configuring Network Address Translation

The topics in this chapter describe defining and managing Network Address Translation (NAT) rules.

- [Address Translation Overview, page 343](#)
- [Managing NAT Rules, page 347](#)

Address Translation Overview

Address translation substitutes the real address in a packet with a mapped address that is routable on the destination network. As part of the process, the device also records the substitution in a translation database; these records are known as “xlate” entries. The appropriate xlate entry must exist to allow address translation on return packets—the substitution of the original real address for the mapped address; this procedure is sometimes referred to as “untranslation.” Thus, network address translation (NAT) actually consists of two steps: the translation of a real address into a mapped address, and the reverse translation for returning traffic.

Cisco devices support both NAT, which provides a globally unique address for each outbound host session, and Port Address Translation (PAT), which provides one address combined with a unique port number, for up to 64,000 simultaneous outbound or inbound host sessions. The global addresses used for NAT come from a pool of addresses specifically designated for address translation. The unique global address that is used for PAT can be either one global address, or the IP address of a given interface.

A security device translates an address when an existing NAT rule matches a specific traffic flow. If no NAT rule matches, processing for the packet continues. The exception is when you enable NAT control—NAT control requires that packets traversing from a higher security interface (inside) to a lower security interface (outside) match a NAT rule, or processing for the packet stops.

Cisco devices can perform NAT or PAT on both inbound and outbound connections. This ability to translate inbound addresses is called “Outside NAT” because addresses on the outside, or less secure, interface are translated to a usable inside IP address. Just as when you translate outbound traffic, you may choose dynamic NAT, static NAT, dynamic PAT, or static PAT. If necessary, you can use outside NAT together with inside NAT to translate the both source and destination IP addresses of a packet.

**Note**

In this document, all types of translation are generally referred to as NAT; see [Address Translation Definitions](#), on page 344 for descriptions of the various types. When describing NAT, the terms inside and outside represent the security relationship between any two interfaces. The higher security level is inside and the lower security level is outside.

Address Translation Definitions

The release of ASA version 8.3 introduced a simplified approach to configuring network address translation (NAT), as compared to earlier ASA versions and other devices. Configuration of NAT was simplified by replacing the earlier flow-based scheme with an “original packet” to “translated packet” approach.

NAT rules are no longer dependent on security levels. A global address space consisting of all interfaces is available, and is specified using the keyword “any.” All Interface fields default to any, so unless a specific interface is provided, the rule is applicable to all interfaces.

The following table briefly describes the available types of address translation.

Table 7: Types of Address Translation

Element	Description
Static NAT	Fixed translation of real source addresses to specific mapped addresses—each source address is always translated to the same mapped address, regardless of IP protocol and port number. A “bi-directional” rule is a static rule that operates as two paired rules, one each for outgoing and incoming translation of the specified source and destination values.
Static PAT	Fixed translation of real source addresses with specific TCP or UDP port numbers, to specific mapped addresses and ports. That is, each source address/port is always translated to the same mapped address/port.
Dynamic NAT	Dynamic translation of real source addresses to mapped addresses obtained from a pool of shared addresses. Each source address can be mapped to any available address in the pool.
Dynamic PAT	Translation of real source addresses to a single mapped address; singularity is provided by dynamic translation of related port numbers. That is, each real address/port combination is translated to the same mapped address, but assigned a unique port. This is sometimes referred to as “overloading.”
Policy Static NAT	Fixed translation of real source addresses to specific mapped addresses. Destination networks/hosts are also specified, and the service is always IP.

Element	Description
Policy Static PAT	Fixed translation of real source addresses with specific TCP or UDP port numbers, to specific mapped addresses and ports. Destination networks/hosts and services are also specified.
Policy Dynamic NAT	Dynamic translation of specific source-address/destination-address/service combinations on a given interface, using a pool of shared addresses. Translation direction—outbound or inbound—is also specified.
Identity NAT	Identity NAT lets you translate a real address to itself, essentially bypassing NAT. In other words, the specified address is effectively not translated. Used to exempt a subset of addresses when a network or other large group of addresses is being translated. Applies to outbound connections only; necessary for remote-access VPN.

Network Object NAT

You also can define NAT properties on Network objects, such that corresponding NAT rules are applied automatically to the designated security device. Using these objects means you need enter the necessary IP addresses, services, and interfaces only once. These automatically generated, object-based rules are referred to as “Network Object NAT” rules.

Destination Translation

With manual static rules, in addition to source address translation, you also can configure destination address translation. Source and destination translation are defined at the same time, in the same screen. Again, while source translation can be static or dynamic, destination translation is always static, and is only available with manual rules.

Twice NAT

Creating a manual static rule will produce an entry in the rules table that actually represents two static NAT rules, encompassing both translation directions. That is, a static rule is created for the specified source/translated address pairing, along with a mirror rule for the translated address/source pairing. This is referred to as “Twice NAT” because only one look-up is required to fetch and process what is in effect two rules.

PAT Pools and Round Robin Allocation

Adaptive Security Appliances, version 8.4.2 and later, include two features that let you alter how port address translation (PAT) occurs: you can explicitly define a pool of IP addresses specifically for PAT, and you can select a “round robin” algorithm for port allocation during PAT processing.

These features simplify configuration of large numbers of PAT addresses, and help prevent a large number of connections from a single PAT address, which can appear to be part of a DoS attack.

Explicit PAT Pool Definition

Prior to version 8.4.2, when you defined a Dynamic NAT and PAT rule, you provided a “pool” of IP addresses (in the Original packet Source field of the [Twice NAT Rule Properties](#), on page 348) to be used for translation. This pool could consist of individual IP addresses, ranges of addresses, Network objects, or Network Group objects, and combinations thereof.

Ranges and objects with more than one IP address were considered to be in the “NAT Pool,” while individual IP addresses and group objects consisting of one or more individual addresses were considered to be part of the “PAT Pool.”

Address translation on the device would work its way through the NAT Pool until all available addresses were exhausted. Port address translation would then begin using the PAT Pool—assigning ports on the first IP address in the PAT Pool until all ports (approximately 64,000) are assigned, then assigning ports on the next address in the pool, and so on. When all ports are fully subscribed on all IP addresses in the PAT Pool, no further translation could occur.

On version 8.4.2 and later ASA devices, you can explicitly define a separate PAT Pool for a Dynamic NAT and PAT rule. If you do so, the first collection of addresses (defined in the Original packet Source field) is considered the NAT Pool, while the PAT Pool addresses are specified in the Translated packet Source field.

**Note**

If you do not explicitly specify a PAT Pool, address translation takes place as described for pre-8.4.2 devices.

Refer to [Managing NAT Rules](#), on page 347 for more information about the defining translation rules.

Round Robin Port Assignment

On version 8.4.2 and later ASA devices, you also can specify an alternate method of port assignment during PAT processing. As mentioned earlier, PAT port numbers are assigned to a single IP address in succession until the final port number is assigned, and then the process begins again with the next available IP address in the pool.

However, a new parameter on 8.4.2 and later devices—**Use round robin allocation**—lets you specify “round robin” cycling through available IP addresses and port numbers. This method assigns an address/port combination using each successive address in the pool; it then uses the first address again with a different port, proceeds to the second address again, and so on.

Further, the round-robin algorithm incorporates two additional principles it will attempt to adhere to when assigning address/port combinations during PAT processing:

- If a specific source-to-destination mapping already exists, the algorithm attempts to use the existing translation for the new connection. If this is not possible (for example, when all ports for that IP address have been exhausted), the algorithm proceeds with standard round-robin cycling.
- If possible, the original source port number is used as the mapped port number. That is, if the port number of the address/port combination to be translated is 4904, for example, and 4904 is available with the next IP address in the PAT Pool, the translated address will be PAT_address/4904. If this is not possible (that port is not available with the next PAT address), the algorithm proceeds with standard round-robin cycling.

**Note**

If you do not explicitly specify Round Robin Allocation, port-allocation cycling occurs as described for pre-8.4.2 devices.

Managing NAT Rules

You can add, edit and delete NAT rules that are available to the entire device repository, and you can add, edit and delete the rules assigned to an individual device. Repository rules are assigned to all the devices in the inventory.

Procedure

-
- Step 1** To manage NAT rules, select **Configurations > Policies/Settings**.
- Step 2** Select the desired device: be sure **Devices** is chosen in the **Policies/Settings** view selector, and then select the device you want to manage from the Devices list.
- Step 3** Click the **NAT policies** tab to view the NAT rules table.
As described in [The NAT Rules Table](#), this table consist of three sections: the Twice NAT (Before Object NAT) rules, the Network Object rules (these are the “automatic” rules), and the Twice NAT (After Object NAT) rules. The Before and After rules are processed before and after the “automatic” rules, respectively.
- Step 4** Add, edit, delete, duplicate, and enable/disable specific rules, as necessary. (General policy management is described in [Policy Basics](#), on page 107.)
- To add a NAT rule, click the Add button to the left of the table and then choose **Add Twice NAT (Before Object NAT)**, **Add Network Object NAT**, or **Add Twice NAT (After Object NAT)** to display the appropriate creation screen.
See [Twice NAT Rule Properties](#), on page 348 for descriptions of the Twice NAT (Before and After) options. See [Object NAT Rules](#), on page 351 for descriptions of the Object NAT options.
 - To edit a NAT rule, select the rule and then click the Edit button to the left of the table to display the appropriate edit screen: Edit Twice NAT Policy (before), Edit Object NAT Policy, or Edit Twice NAT Policy (after).
 - To delete a NAT rule, select the rule and then click the Delete button to the left of the table. You are asked to confirm the deletion.
 - To duplicate a NAT rule, select the rule and then click the Duplicate button to the left of the table. The Duplicate NAT Rule screen opens, containing the same parameters as the selected rule. Change the parameters as necessary, and save the new rule. See [Twice NAT Rule Properties](#), on page 348 for descriptions of the Twice NAT (Before and After) options. See [Object NAT Rules](#), on page 351 for descriptions of the Object NAT options.
 - To enable or disable a rule in the Twice NAT Before or Twice NAT After sections, select the rule and then click the Enable/Disable button to the left of the table; the rule is enabled or disabled according to its current state, but it remains in the table. This is a shortcut to editing the rule and changing the Enable Rule option. This button is not available when a Network Object NAT rule is selected.
- Step 5** If necessary, move the policy so that it is in priority order.
Policies are applied on a first-match basis, so you must ensure that policies with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.
- To move a policy set or rule, you click and hold the Move icon (the vertical double-headed arrow on the left margin) and drag it to the policy after which you want to insert it. You can also simply edit the sequence number and change it to the desired value.

Twice NAT Rule Properties

The following properties are presented when you add or edit a Twice NAT rule (that is, a Before Auto Rule or an After Auto Rule).

Twice NAT Properties

Description

An optional description of the rule of up to 200 characters.

Enable Rule

You can enable or disable this rule without removing it from the table: select **On** or **Off**.

Source NAT type

Specify the type of address translation for this override: choose **Static** or **Dynamic**.

- **Static** – Provides static assignment of real addresses to mapped addresses.
- **Dynamic** – Provides dynamic assignment of multiple local addresses to a single global IP address and a unique port number, in effect “hiding” the local addresses behind the one global address. Choosing this option also adds the **PAT Pool** option to the available properties. On devices operating in routed mode, this option also provides the fall-through option described below.



Note This property applies only to the specified source translation; destination translation is always static.

Source interface

Enter or select the name of the interface on the specified device from which a packet may originate; this is the “real” interface. Defaults to **Any**, which represents all interfaces.



Note In transparent firewall mode, you must specify this property.

Destination interface

Enter or select the name of the interface on which a packet may terminate; this is the “mapped” interface. Defaults to **Any**, which represents all interfaces. If **Dynamic** is the chosen **Source NAT type**, entering an interface name adds the **Fallthrough to interface PAT** option to the available properties.



Note In transparent firewall mode, you must specify this property.

PAT Pool

The **PAT Pool** option appears when you choose **Dynamic** as the **Source NAT type**. The related parameters let you specify a “pool” of IP addresses to be used for specifically for port address translation, as well as change the algorithm used for PAT mapping. (See [PAT Pools and Round Robin Allocation](#) , on page 345 for more information.) If you select **On**, these options appear: **Translated address**, **Round Robin**, **Extended PAT table**, **Flat port range**, and **Include reserve ports**.

Translated address

Enter or select the name of one of more Network and Network Group objects to use as the PAT pool.

If you enter or select the name of an interface the **Fallthrough to interface PAT** and **IPv6 Source** options appear in the **Additional Information** section, and the **Extended PAT table** option disappears.

Round Robin

Available only when **PAT Pool** is **On**. Turn this option **On** to use a “round-robin” approach to mapping addresses/ports. See [PAT Pools and Round Robin Allocation](#) , on page 345 for more information about this option.

Extended PAT table

Available only when **PAT Pool** is **On**. Turn this option **On** to enable extended PAT. Extended PAT uses 65535 ports per service, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80.

Flat port range

Available only when **PAT Pool** is **On**. Turn this option **On** to enable use of the entire 1024 to 65535 port range when allocating ports. When choosing the mapped port number for a translation, the ASA uses the real source port number if it is available. However, without this option, if the real port is not available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also turn **On Include reserve ports**.

Include reserve ports

Available only when **PAT Pool** and **Flat port range** are **On**. Turn this option **On** to include the reserve ports, 1 to 1023, in the PAT range.

Additional Information

The following additional options related to NAT processing may be available depending on the type of rule you are creating and the chosen **Source NAT type**:

- **Unidirection**
- **Translate DNS replies**
- **IPv6 Source**
- **One-to-one address translation**
- **Do not proxy ARP**
- **Fallthrough to interface PAT**
- **Perform route lookup**

Unidirection

Available only when **Static** is the chosen **Source NAT Type** (dynamic rules are uni-directional by default). This feature lets you configure a static NAT rule in a single direction only, as specified by the other options in this screen. When Off, both directions of the translation are performed.

IPv6 Source

Available only when you enter a single interface into the **Original Packet Destination** field. Turn On to use an IPv6 destination interface address.

One-to-one address translation

Turn On to restrict translations to one-to-one mappings. Generally used for NAT 46 (IPv4 to IPv6 addresses).

Do not proxy ARP

Available only when **Static** is the chosen **Source NAT type**. Turn On to disable proxy ARP on the specified Destination Interface.

By default, all NAT rules include proxy ARP on the egress interface. A NAT Exempt rule is used to bypass NAT for both ingress and egress traffic, relying on route look-up to locate the egress interface. Thus, proxy ARP should be disabled for NAT Exempt rules. (NAT Exempt rules always take priority.)



Note You also can disable Proxy ARP on individual interfaces.

Fallthrough to interface PAT

Available only when **Dynamic** is the chosen **Source NAT Type** on devices operating in routed mode, and it appears when you provide an interface name in the **Translated address** field. When On, dynamic PAT back-up is enabled. When the pool of dynamic NAT addresses is depleted, port address translation is performed, using the address pool specified in the Translated Address field.

Perform route lookup

Available only when **Static** is the chosen **Source NAT type**, and appears when you provide an interface name in the **Destination Interface** field. If this option is On, the egress interface is determined using route look-up instead of using the specified Destination Interface. Be sure this is On for a NAT Exempt rule. This option is supported only for Static Identity NAT.



Note This option is not available on devices operating in transparent mode.

Object NAT Rules

You can configure network address translation (NAT) overrides on a Network object in order to override the destination address of specific packets. This is referred to as “Object NAT,” and it is considered a device-level override. NAT overrides apply to ASA devices only. Each network address translation (NAT) rule defined here will appear in the Network Object NAT Rule section of the NAT rules table for that device.



Note You cannot configure NAT overrides on Network objects incorporating fully qualified domain names (FQDNs).

To configure a NAT rule on a Network object and assign it to the selected device, click the Add rule button on the NAT policies page, and choose **Add Object NAT policy**. The **Create Object NAT Policy** screen appears. Fill in the Object NAT Policy Properties.

You can edit an existing Object NAT rule by opening it (select the rule on the NAT policies page for the selected device and click the Edit NAT policy button) and updating the Object NAT policy properties.

To delete an existing Object NAT rule, select it and click the Delete NAT policy button.

Object NAT Policy Properties

Description

An optional description of the rule of up to 200 characters.

Network object

Enter or select the name of the Network Object this rule is to be associated with; you also can create a new object from this field.

Source NAT type

Specify the type of address translation for this override: choose **Static** or **Dynamic**.

- **Static** – Provides static assignment of real addresses to mapped addresses.
- **Dynamic** – Provides dynamic assignment of multiple local addresses to a single global IP address and a unique port number, in effect “hiding” the local addresses behind the one global address. Choosing this option also adds the **PAT Pool** option to the available properties. On devices operating in routed mode, this option also provides the fall-through option described below.



Note This property applies only to the specified source translation; destination translation is always static.

Source interface

Enter or select the name of the interface on the specified device from which a packet may originate; this is the “real” interface. Defaults to **Any**, which represents all interfaces.



Note In transparent firewall mode, you must specify this property.

Destination interface

Enter or select the name of the interface on which a packet may terminate; this is the “mapped” interface. Defaults to **Any**, which represents all interfaces. If **Dynamic** is the chosen **Source NAT type**, entering an interface name adds the **Fallthrough to interface PAT** option to the available properties.



Note In transparent firewall mode, you must specify this property.

Original packet

Available only when **Static** is the chosen **Source NAT type**. You can add Static port address translation (PAT) to the override by providing Original Packet information:

- **Service** – Enter a protocol/port combination for traffic entering the device.

Translated packet

Use these fields to add port address translation (PAT) to the rule—translation of specific source-address/destination-address/service combinations.

- **Source** – Enter or select the name of the interface, Network object, or Network Group object representing the PAT address pool.
- **Service** – Available only when Static is the chosen Source NAT type. Enter the port number which is to replace the original port number.

PAT Pool

The **PAT Pool** option appears when you choose **Dynamic** as the **Source NAT type**. The related parameters let you specify a “pool” of IP addresses to be used for specifically for port address translation, as well as change the algorithm used for PAT mapping. (See [PAT Pools and Round Robin Allocation](#), on page 345 for more information.) If you select **On**, these options appear: **Translated address**, **Round Robin** and **Extended PAT table**.

Translated address

Enter or select the name of one of more Network and Network Group objects to use as the PAT pool.

Round Robin

Available only when **PAT Pool** is On. Turn this option On to use a “round-robin” approach to mapping addresses/ports. See [PAT Pools and Round Robin Allocation](#), on page 345 for more information about this option.

Extended PAT table

Available only when **PAT Pool** is On. Turn this option On to enable extended PAT. Extended PAT uses 65535 ports per service, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80.

Flat port range

Available only when **PAT Pool** is On. Turn this option On to enable use of the entire 1024 to 65535 port range when allocating ports. When choosing the mapped port number for a translation, the ASA uses the real source port number if it is available. However, without this option, if the real port is not available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also turn On **Include reserve ports**.

Include reserve ports

Available only when **PAT Pool** and **Flat port range** are On. Turn this option On to include the reserve ports, 1 to 1023, in the PAT range.

Additional Information

The following additional options related to NAT processing may be available depending on the type of rule you are creating and the chosen **Source NAT type**:

- **Unidirection**
- **Translate DNS replies**
- **IPv6 Source**
- **One-to-one address translation**
- **Do not proxy ARP**
- **Fallthrough to interface PAT**
- **Perform route lookup**

Translate DNS replies

When On, addresses embedded in DNS replies that match this rule are rewritten.

For DNS replies traversing from a mapped interface to a real interface, the Address (or “A”) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the A record is rewritten from the real value to the mapped value. Note that DNS inspection must be enabled to support this functionality.

One-to-one address translation

Turn On to restrict translations to one-to-one mappings. Generally used for NAT 46 (IPv4 to IPv6 addresses).

Do not proxy ARP

Available only when **Static** is the chosen **Source NAT type**. Turn On to disable proxy ARP on the specified Destination Interface.

By default, all NAT rules include proxy ARP on the egress interface. A NAT Exempt rule is used to bypass NAT for both ingress and egress traffic, relying on route look-up to locate the egress interface. Thus, proxy ARP should be disabled for NAT Exempt rules. (NAT Exempt rules always take priority.)



Note You also can disable Proxy ARP on individual interfaces.

Fallthrough to interface PAT

Available only when **Dynamic** is the chosen **Source NAT Type** on devices operating in routed mode, and it appears when you provide an interface name in the **Translated address** field. When On, dynamic PAT back-up is enabled. When the pool of dynamic NAT addresses is depleted, port address translation is performed, using the address pool specified in the Translated Address field.

Perform route lookup

Available only when **Static** is the chosen **Source NAT type**, and appears when you provide an interface name in the **Destination Interface** field. If this option is On, the egress interface is determined using route look-up instead of using the specified Destination Interface. Be sure this is On for a NAT Exempt rule. This option is supported only for Static Identity NAT.



Note This option is not available on devices operating in transparent mode.

Tags

Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.

Ticket ID

A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)



Configuring Access Policies

The topics in this chapter describe configuring inbound and outbound access policies for ASA devices.

- [About Access Policies, page 357](#)
- [Managing ASA Access Policies, page 358](#)

About Access Policies

Access policies define the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. You can use access policies, or rules, in routed and transparent firewall mode to control IP traffic. An access rule permits or denies traffic based on the protocol, a source and destination IP address or network, and optionally the users and user groups.

Each packet that arrives at an interface is examined to determine whether to forward or drop the packet based on criteria you specify. If you define access rules in the out direction, packets are also analyzed before they are allowed to leave an interface.

Access policies are applied in order. That is, when the device compares a packet to the rules, it searches from top to bottom of the access policies list, and applies the policy for the first matched rule, ignoring all subsequent rules (even if a later rule is a better match). Thus, you should place specific rules above more general rules to ensure those rules are not skipped.

Carefully consider the other types of firewall rules you intend to create when you define access rules. Do not create a blanket denial in an access rule for traffic that you really want to inspect. On the other hand, if you know that you will never allow a service from or to a specific host or network, use an access rule to deny that traffic.

Default behavior is to permit traffic from a higher-security interface to a lower-security interface. Otherwise, all traffic is denied.

If an access rule allows TCP/UDP traffic in one direction, the appliance automatically allows return traffic (you do not need to configure a corresponding rule for the return traffic), except for ICMP traffic, which does require a return rule (where you permit the reverse source and destination).

**Note**

Configuring access policies on CX modules is described in [Configuring Context-Aware Access Policies, on page 250](#).

Universal Access Policies

Traditionally, access rules are applied to device interfaces. However, you also can create global, or “universal,” access policies that are applied to all devices in the repository.

Universal rules are best used for rules that you want to apply to all traffic on a device regardless of interface. For example, there might be a specific host or subnet that you always want to deny or permit. You can create these as universal rules, so they are configured once on the device instead of being configured individually on each device.

You can add universal rules to the “Universal Top” or “Universal Bottom” policy sets. These are then assigned and applied before or after the policies specific to each device.

See [Managing Policies, on page 103](#) for general information about working with policies and policy sets.

Managing ASA Access Policies

You can add, edit and delete ASA-specific access policies that are available to the entire device repository, and you can add, edit and delete the policies assigned to an individual device. Repository access rules are assigned to all devices in the inventory.

**Note**

Configuring access policies on CX modules is described in [Configuring Context-Aware Access Policies, on page 250](#).

Access rules always use real IP addresses when determining an access rule match, even if you configure NAT. For example, if you configure NAT for an inside server, 10.1.1.5, so that it has a publicly routable IP address on the outside, 209.165.201.5, an access rule to allow outside traffic to access the inside server needs to reference the server’s real IP address (10.1.1.5), and not the mapped address (209.165.201.5).

Inbound and Outbound Rules

The ASA supports two types of access policies:

- **Inbound** – Inbound access rules apply to traffic entering an interface. Global access rules are always inbound.
- **Outbound** – Outbound access rules apply to traffic exiting an interface.

An outbound access policy is useful, for example, if you want to allow only certain hosts on the inside networks to access a web server on the outside network. Rather than creating multiple inbound rules to restrict access, you can create a single outbound rule that allows only the specified hosts. The outbound rule prevents any other hosts from reaching the outside network.

**Note**

The terms *inbound* and *outbound* in this context refer to the application of an access rule on an interface, either to traffic entering the ASA on an interface, or to traffic exiting the ASA on an interface. They do not refer to the movement of traffic from a lower-security interface to a higher-security interface, also commonly referred to as “inbound,” or from a higher- to lower-security interface, commonly referred to as “outbound.”

Follow these general steps to manage inbound and outbound ASA access policies.

Procedure

-
- Step 1** Select **Configurations > Policies/Settings** and then open the **Access Policies** page.
- Step 2** Choose whether to manage repository-wide or device-specific access rules:
- To manage repository-wide access policies, choose **Repository** from the **Policies/Settings** view selector.
 - To manage device-specific access policies, choose **Devices** from the **Policies/Settings** view selector. Select the device you want to manage from the device list.
- Step 3** Specify the type of access policies you want to manage: click the **ASA inbound policies** button, or the **ASA outbound policies** button, at the top of the **Access Policies** page to display the appropriate rules table.
- Step 4** Open the desired policy set.
Access policies are grouped into named policy sets; expand a policy set entry to view the individual rules contained in that set. Refer to [Configuring Policy Sets, on page 108](#) for more information about managing policy sets.
- Step 5** Add, edit, delete, and move individual access policies, as needed.
- Moving and deleting access policies, and general policy management, are described in [Policy Basics, on page 107](#).
 - The properties presented when you add or edit an access rule are described in [Access Policy Properties, on page 359](#).
-

Access Policy Properties

The following properties are presented when you add or edit an inbound or outbound ASA access policy or “rule.”

**Note**

Configuring access policies on CX modules is described in [Configuring Context-Aware Access Policies, on page 250](#).

ASA Access Policy Properties

Policy Intention

You can enter a description of the intent underlying this policy.

Enable Policy: On/Off

Whether the policy is enabled. You can turn a policy off to temporarily disable it without deleting the policy. Disabled policies are never applied to traffic.

Policy Action

Whether the policy allows or denies network access. Denied traffic is dropped.

Logging

You can turn logging for this particular policy On or Off. If On, syslog messages are generated for the policy, as defined by the **Level** and **Logging Interval** properties, which appear when you turn **Logging** On.

- **Level** – Choose the desired logging level. If you choose **default**, when a packet is denied, message 106023 is generated. If a packet is permitted, no syslog message is generated. The default logging interval is 300 seconds.

For all levels other than **default**, syslog message 106100 is generated.

- **Logging Interval** – When you choose a logging **Level** other than **default**, you can specify the **Logging Interval**, which can range from 1 to 600 seconds. This is the interval between transmission to the syslog server of messages logged for this policy.



Note You must have a syslog server configured to capture these messages. See [ASA Syslog Server Properties](#), on page 195 for more information.

Source Object

Use this field to provide specific traffic sources as part of this policy—enter any combination of one or more network objects, network object groups, interface names, and interface role objects. The default is **Any** traffic source. You can also specify **any4** to match any IPv4 address and **any6** to match any IPv6 address.

Source User

To include consideration of the users from which traffic originates, enter any combination of user names, user groups, and ASA identity objects into this field.

- Enter groups in the *DOMAIN\group* format, where you enter the AD domain plus the group name, separated by a double \ mark.
- Enter user names in the *DOMAIN\name* format, where you enter the AD domain plus the user name, separated by a single \ mark. For users defined on the ASA, use LOCAL as the domain name.

Destination

To limit the policy to specific traffic destinations, enter any combination of one or more network objects, network object groups, interface names, and interface role objects. The default is **Any** traffic source. You can also specify **any4** to match any IPv4 address and **any6** to match any IPv6 address.

Service

Use this field to limit the policy to specific service protocols by entering any combination of one or more service objects and service object groups.

Interface Roles

The Interface Role objects or interface names that identify the interfaces to which this policy applies. The default is **Any**, which means that the policy is not restricted to a specific interface. Choose interface names or objects to limit the policy to specific interfaces.

For an Inbound policy, to match the policy, traffic must enter the device on one of the identified interfaces or on an interface that matches a selected role. For an Outbound policy, traffic must leave on one of the interfaces.

When you deploy the policy to the device, separate ACLs are created for each interface. These ACLs combine (in order) all policies that include the interface name explicitly or by way of interface role matching. Thus, if you use the default Any, there will be an individual ACL for each interface on the device. However, for policies in the Universal Bottom policy set, policies that apply to Any interface can be used to generate the global ACL. A rule will be placed in the global ACL if there are no subsequent policies in the policy set that specify interfaces.



Tip If you specify Interface Role objects, and no interfaces on the device match the interface names defined in the role, the policy will never apply to any traffic on the device. Additionally, interface names are available for selection in Device view only; in Repository view, you will see interface roles only.

Shared/Local

(Multiple Device mode only.) The devices on which to configure this policy. If you leave this field blank, the policy is configured on all devices that share the policy set that contains the policy. If you want to limit this policy to a subset of the devices that share the policy set, select those devices here; the policy will not be configured on any unlisted devices that otherwise share the policy set. The devices available for selection are constrained to those that currently share the policy set.

For example, you can use this setting to create a handful of policies specific to a device that otherwise should use the same policies as a group of devices.

Time Ranges

You can choose a time range object to limit this policy to specific times of day, and days of the week, such as during working hours. See [Time Range Objects](#), on page 152 for more information.

Tags

Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.

Ticket ID

A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)



APPENDIX

A

System Maintenance and Troubleshooting

The following topics explain general maintenance and troubleshooting for CX devices and PRSM servers. In many cases, the procedures are the same, but there are cases where procedures differ based on the system platform.

- [Managing Users, page 363](#)
- [Installing a Server Certificate, page 373](#)
- [Configuring Network Participation, page 375](#)
- [Configuring an HTTP Proxy, page 376](#)
- [Basic Troubleshooting, page 377](#)
- [Maintaining the System, page 385](#)

Managing Users

You can create user accounts to allow multiple people access to the system. Using role-based access control (RBAC), you can provide these users with different levels of access. Thus, your help desk personnel can view events, dashboards, and policies without being able to change policies.

The following topics explain user management in more detail.

Overview of the Users Page

The Users page lists all user accounts that are allowed to log into the web interface. The page lists the pre-defined **admin** account plus any accounts you created. These users can be defined locally on the system or remotely in a directory realm.

To open the Users page, select **Administration > Users**.

The Users page includes the following items:

- **I Want To**—Contains the following commands:

- **Select Global Realm for Remote Users**—To identify the directory realm that contains users you want to add as remote users. You do not need to select a realm to create local users. For more information, see [Configuring the Directory Realm for Remote Users](#), on page 368.
- **Select Global Realm for SSO Users**—(Multiple Device mode only.) To identify the directory realm that contains users you want to add as single-sign-on users. The SSO directory enables integration between PRSM and supported network management applications other than Cisco Security Manager. For more information, see [Configuring SSO Directories and Users](#), on page 371.
- **Configure CSM SSO**—To configure single sign-on (SSO) with a Cisco Security Manager (CSM) server. This allows CSM users to directly access the web interface using their CSM username and credentials. For more information, see [Configuring Single Sign-On for Cisco Security Manager](#), on page 370.
- **Role and User Lists**—Users are organized in folders based on the role assigned to the account. The role, used in role-based access control (RBAC), defines the user's privileges in the system and controls what the user can see and what the user can change. In the order of most access to least access, the roles are Administrator, Security Administrator, System Administrator, Help Desk, and Reporting Administrator. For complete details on the access rights for these roles, see [User Roles and Privileges](#), on page 364.

To see the commands related to a role or user, mouse over the role header or the user row. The following are the available commands:

- **Create User**—(Role command.) To add a new user. Although you select this command when mousing over a specific role, you can create users for any role.
- **Delete User**—(User command.) To delete the user. You cannot delete the admin user or your own user name (the one used to log into the system).
- **Edit User**—(User command.) To edit the user account.

User Roles and Privileges

The following are the roles that you can assign to a user. These roles apply to the web interface. You cannot create users who can access the system CLI.

- **Administrator**—Super Administrators are responsible for managing the system and have access to all product features.
- **Security Administrator**—Security administrators are responsible for configuring security policies on network devices. They have read-write access to policies and some device configuration features.
- **System Administrator**—System administrators are responsible for device and system setup and management. They have read-write access to some device configuration features but not to policies.
- **Reporting Administrator**—Reporting administrators are responsible for analyzing system reports and comparing network usage to the organization's acceptable use policy. They can view dashboards and events but cannot change any configuration.
- **Help Desk User**—Help desk users troubleshoot problems reported by network users. They can view dashboards, events, policies, and device configurations, but cannot change any policies or settings.

The following table shows privileges for these user roles based on the application menus.

Table 8: User Roles and Privileges

Menu	Role				
	Administrator	Security Administrator	System Administrator	Reporting Administrator	Help Desk
Dashboard , all items	Yes	Yes	Yes	Yes	Yes
Events	Yes	Yes	Yes	Yes	Yes
Configurations > Policies/Settings	R/W	Access rights differ by tab. The permissions are explained in the following rows.		No	RO
— Overview tab in Single Device mode; Device view in Multiple Device mode.	R/W	The groups displayed are controlled by your access rights, which are explained in the following rows.		No	RO
— Overview tab in Repository view in Multiple Device mode.	R/W	R/W	R/W	No	RO
— Access Policies tab	R/W	R/W	No	No	RO
— NAT Policies tab	R/W	R/W	No	No	RO
— ASA CX Logging tab	R/W	R/W	R/W	No	RO
— Syslog Settings tab	R/W	R/W	R/W	No	RO
— Packet Capture tab	R/W	R/W	R/W	No	RO
— Interfaces tab	R/W	R/W	R/W	No	RO
— High Availability tab	R/W	R/W	R/W	No	RO
— Traffic Redirection tab	R/W	R/W	R/W	No	RO
— Intrusion Prevention tab	R/W	R/W	R/W	No	RO
— Malware Protection tab	R/W	R/W	R/W	No	RO
— Decryption Settings tab	R/W	R/W	R/W	No	RO
— Decryption Policies tab	R/W	R/W	No	No	RO
— AD Agent tab	R/W	R/W	R/W	No	RO

Menu	Role				
	Administrator	Security Administrator	System Administrator	Reporting Administrator	Help Desk
—Auth Settings tab	R/W	R/W	R/W	No	RO
—Identity Policies tab	R/W	R/W	No	No	RO
Configurations > Certificates	R/W	R/W	RO	No	RO
Configurations > Updates	R/W	R/W	R/W	No	RO
Configurations > HTTP Proxy	R/W	R/W	R/W	No	RO
Configurations > Monitor-only Mode	R/W	R/W	R/W	No	No
Components > Objects	R/W	R/W	No	No	RO
Components > Directory Realm	R/W	R/W	R/W	No	RO
Components > Applications	R/W	R/W	No	No	RO
Components > Threats	R/W	R/W	No	No	RO
Components > Web Filtering Categories	R/W	R/W	No	No	RW
Administration > Users	R/W all accounts	R/W own account	R/W all accounts	R/W own account	R/W own account
Administration > Licenses	R/W	R/W	R/W	No	RO
Administration > PRSM Logs	R/W	R/W	R/W	No	RO
Administration > Server Certificates	R/W	No	R/W	No	No
Administration > Database Backup	R/W	R/W	R/W	No	No
Administration > Upgrade	R/W	R/W	R/W	No	No
Administration > Change History	Yes	Yes	Yes	No	Yes

Menu	Role				
	Administrator	Security Administrator	System Administrator	Reporting Administrator	Help Desk
Administration > Out-of-band Settings	R/W	R/W	R/W	No	RO
Administration > End User Notification	R/W	R/W	R/W	No	RO
Administration > Network Participation	R/W	RW	RW	No	RO
Administration > About PRSM	Yes	Yes	Yes	Yes	Yes
Commit and Deploy Changes	R/W	R/W	R/W	No	No

Legend

- Yes—User can use a feature that does not have read-write characteristics.
- No—User has no access to the feature.
- R/W—User has read-write access to the feature.
- RO—User has read-only access to the feature.

Using the Pre-Defined Admin User

The **admin** user is pre-defined in the system and has special characteristics.

- You cannot delete the admin user account.
- This is the only user allowed to log into the CLI.
- This is the only username you can specify when adding a CX device to the PRSM Multiple Device mode inventory.
- The password for this user is never synchronized between a CX device and the PRSM server that manages it, if any. For all other users, if you add a CX device to the PRSM inventory, all users defined on the CX device are deleted and replaced with those defined on the PRSM server. However, the password for the admin user remains unchanged, so you can have different passwords for the admin account on the PRSM server and on each managed device.



Note

If you can the password, ensure that you update it in the inventory for the device.

- You can change the admin password using the web interface or the CLI. Whichever way you use, the password for both the web interface and CLI is changed.
- If a CX device is being managed by a PRSM server, the admin user is the only one who can log into the ASA CX managed mode home page.

Configuring the Directory Realm for Remote Users

Before you can add remote users, that is, users defined in your network directory, to the system, you must identify the directory that contains the user accounts.

Procedure

-
- Step 1** If the directory realm you want to use is not yet defined, create it.
- a) Select **Components > Directory Realm** to create the realm and add the directory servers.
 - b) Commit your changes. You cannot select the realm as the global realm for remote users until you commit it.
- Step 2** Select **Administration > Users**.
- Step 3** Select **I Want To > Select Global Realm for Remote Users**.
If you are identifying the single-sign-on (SSO) realm to use for SSO users, select **I want to > Select Global Realm for SSO Users**.
- Step 4** Select the directory realm.
Select **None** to remove support for remote user definitions.
- Step 5** Click **Save**.
-

Configuring Users

You can define user accounts to allow access to the web interface. The usernames you define cannot gain access to the product's CLI.

You can define the following types of users:

- **Locally defined**—These users exist in the configuration database only. Users must remember their PRSM username and password to gain access to the web interface, and they must change their passwords in the web interface.
- **Remote (directory) users**—These users are defined in an external directory server. Typically, you are adding users from your standard network directory. By adding a directory user, you allow users to log in using their normal username and password, for example, the one they use to log into their Windows workstation. Users change their passwords using your standard password changing procedure.
Directory users can log in as: DOMAIN\username (e.g. EXAMPLE\user1), username@domain (e.g. user1@example.com), or just username.
- **SSO (single-sign-on) users**—(Multiple Device mode only.) Except for Cisco Security Manager users, these users are defined in an external SSO directory, which enables integration between PRSM and

supported network management applications. For Cisco Security Manager, define users as normal local or remote users.

Procedure

Step 1 Select **Administration > Users**.

Step 2 Do one of the following:

- Mouse over any of the role names and click **Create User**. It does not matter which role you mouse over; you can choose a different role when you define the user.
- Mouse over a username and click **Edit User**.

Step 3 In the User Properties form, select the type of user you are creating, then fill in the user characteristics as defined in [User Properties](#), on page 369.

Step 4 Click **Save**.
The user account is immediately ready for use.

User Properties

PRSM and CX users have the following properties:

User Type

You can define the following types of users:

- Locally defined—These users exist in the configuration database only. Users must remember their PRSM username and password to gain access to the web interface, and they must change their passwords in the web interface.
- Remote (directory) users—These users are defined in an external directory server. Typically, you are adding users from your standard network directory. By adding a directory user, you allow users to log in using their normal username and password, for example, the one they use to log into their Windows workstation. Users change their passwords using your standard password changing procedure.

Directory users can log in as: DOMAIN\username (e.g. EXAMPLE\user1), username@domain (e.g. user1@example.com), or just username.

- SSO (single-sign-on) users—(Multiple Device mode only.) Except for Cisco Security Manager users, these users are defined in an external SSO directory, which enables integration between PRSM and supported network management applications. For Cisco Security Manager, define users as normal local or remote users.

User Name

The account name, which is the name used to log into the web interface. You cannot edit the name after you create the user. To specify the username:

- Local—Type in the user name, up to 15 characters.
- Remote—Start typing the user name, and a list of names from the server is returned as you type. Select the name. Note that the user name field will allow you to select more than one name, but the last name selected is the only one used.
- SSO—Type in a username defined in the SSO directory.

First Name, Last Name

The user's first and last name. For remote users, the names are retrieved from the directory.

E-mail

The user's E-mail account, for example, username@example.com. For remote users, the address is retrieved from the directory.

Active: On/Off

Whether the account is active (**On**), meaning the user can log into the web interface.

Role

The user's role, which controls which features the user can view or modify. In the order of most access to least access, select one of admin, security admin, system admin, help desk, reporting admin. For complete details on the access rights for these roles, see [User Roles and Privileges](#), on page 364.

Password

(Local users only.) The user's password. The password must be at least 8 characters long and must contain at least one uppercase letter (A-Z), at least one lowercase letter (a-z) and at least one digit (0-9). You cannot save the password unless it passes the test.

When editing a user account, click **Change** to change the password.

Configuring Single Sign-On for Cisco Security Manager

If you use Cisco Security Manager (CSM) to manage some of your ASA devices, you can configure a single-sign-on relationship between CSM and PRSM. This allows users to access PRSM from CSM without separately logging into PRSM.

For example, if you try to configure a CX module from CSM, the CSM command will log into the device to open the web interface. If the CX is managed by PRSM Multiple Device mode, the login is redirected to the appropriate PRSM server (unless there is a NAT boundary between the CX device and PRSM server).

This configuration requires CSM 4.5 as a minimum release.

Procedure

- Step 1** Select **Administration > Users**.
- Step 2** Select **I want to > Configure CSM SSO** and identify the CSM server using the following fields. Click **Save** when finished.
- **CSM Server Name**—The display name of the server.
 - **Server Hostname/IP: Port**—The DNS hostname or IP address, and HTTPS port, of the CSM server. The port is normally 443.
 - **Shared Key**—The 128-bit AES shared key defined on the CSM server, written as a 32-byte hexadecimal string. You generate this key in the CSM client on the page for PRSM under **Tools > Security Manager Administration**.
 - **CSM Certificate**—Click **Get** to retrieve the server certificate, and **View** to review it and verify that it is the expected certificate. You can refresh the certificate when viewing it.
- Step 3** Configure the users you want to allow single-sign-on access.
Each CSM user must exist in the PRSM database with the same username. You can configure them as **local** or **remote** users.
- Assign each user an appropriate role. Regardless of the user's role in CSM, their actions in PRSM will be controlled by the PRSM role.
- Tip** The **admin** user is a special user. You cannot use single sign-on if you log into CSM as "admin."

Configuring SSO Directories and Users

(Multiple Device mode only.) Use a single-sign-on (SSO) directory to enable integration between PRSM and supported network management applications. Single-sign-on makes it possible for you to go seamlessly from the other application to PRSM for tasks such as importing devices and objects, without having to log into PRSM. In fact, you might be required to use an SSO username for certain tasks such as importing objects or devices from the other application.

For information on the specific applications supported, see the release notes at <http://www.cisco.com/c/en/us/support/security/asa-next-generation-firewall-services/products-release-notes-list.html>.



Tip This generic SSO configuration does not work for Cisco Security Manager.

The following procedure explains how to identify the SSO server and configure SSO users to enable this cross-product integration.

Procedure

- Step 1** Configure the SSO directory realm.
- a) Select **Components > Directory Realm**.

- b) Select **I want to > Add Realm**.
- c) Select **SSO** for the Directory Type and fill in the following fields:
 - **Name**—The name of the directory realm. This name is used internally and does not need to match anything configured on the SSO directory.
 - **Hostname/IP**—The hostname or IP address of the other application's SSO directory.
 - **Port**—The SSO directory port number, which should be 443.
- d) Click **Save**.
PRSM fetches the server certificate and presents it to you. Click **Accept** if the certificate is what you expected.
- e) Click the **Changes Pending** link in the menu bar and commit your changes.

Step 2 Identify the realm as the one to use for SSO users.

- a) Select **Administration > Users**.
- b) Select **I want to > Select Global Realm for SSO Users**.
- c) Select your SSO realm and click **Save**.

Step 3 Identify SSO users who should have access to PRSM.

- a) Mouse over the admin role and click **Create User**.
 - b) Select **SSO** for User Type.
 - c) Enter the username defined in the SSO directory, and fill in the other required fields.
 - d) Click **Save**.
-

Changing Your Password

All users who have locally-defined usernames can change their own password, even if they do not otherwise have access to any part of the Users page. Unless you have the appropriate Administrator privileges, your password is the only thing you can change when editing your user account.

If your username is not locally-defined, that is, it is your usual directory username, you cannot change your password using the application. Instead, use your normal procedures for changing your password, and you can then use your new password to log into the application.

The following procedure applies to locally-defined usernames only.

Procedure

Step 1 Select **Administration > Users**.

Step 2 Mouse over your username and click **Edit User**.

Step 3 Click **Change Password**, then type in your old and new passwords.
The password must be at least 8 characters long and must contain at least one uppercase letter (A-Z), at least one lowercase letter (a-z) and at least one digit (0-9). You cannot save the password unless it passes the test.

Step 4 Click **Save**.

Deleting Users

You can delete user accounts that you no longer need. However, you cannot delete the **admin** account or the account you used to log in.

Alternatively, you can temporarily disable a user account if you think you will need it later. To disable an account, edit it and select **Active: Off**.

When you delete a user, all pending changes for the user are discarded.

Procedure

-
- Step 1** Select **Administration > Users**.
 - Step 2** Mouse over the account and click **Delete User**.
You are asked to confirm the deletion.
-

Installing a Server Certificate

When you log into the web interface, the system uses a digital certificate to secure communications using HTTPS. The default certificate is not trusted by your browser, so you are shown an Untrusted Authority warning and asked whether you want to trust the certificate. Although you can save the certificate to the Trusted Root Certificate store, you can also upload a new certificate that browsers are already configured to trust.

Before You Begin

Obtain a digital certificate from a Certificate Authority as described in [Obtaining a Server Certificate](#), on page 374.

When using a certificate signed by a third-party, you must create a PEM file that contains all certificates. Concatenate the certificates starting from the server certificate at the top of the file, then add the CA certificate used to sign that certificate, then add any other certificates in the signing chain up to the root certificate, which would be the last certificate in the file. Obtain these additional certificates from the CA.

For example, if the server certificate was signed by a root certificate, the file would look like the following (parts of the example are redacted as indicated; do not include the annotations):

```
-----BEGIN CERTIFICATE----- <!-- This is the server certificate -->
MIIDzjCCArag
... (bulk of server certificate redacted) ...
ng5lGTCSkEJz48Xkh3npPynf
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- <!-- This is the CA root certificate -->
MIID2TCCAsGg
... (bulk of CA root certificate redacted) ...
9DT4XfXcg+A0EaYl/Gq8eaP2HFj2otge4JW4KV8=
-----END CERTIFICATE-----
```

Procedure

-
- Step 1** Select **Administration > Server Certificates**.
This page does not show whether you have already uploaded a certificate or information about the server certificate currently in use.
- Step 2** Click **Browse** for each of the following fields and select the appropriate file:
- **Certificate**—The CA certificate file. When uploading a third-party certificate, select the file that contains the entire certificate chain, in order, from the server certificate at the top to the root certificate at the bottom.
 - **Key**—The decrypted RSA private key file for the selected server certificate. Do not select an encrypted key file. If you are uploading a certificate chain, the key is for the server certificate, not for any of the CA certificates used in the signing chain.
- Step 3** Click **Upload** to copy the files to the system.
The server certificate details are displayed. When uploading a certificate chain, you do not see the details for the entire chain.
- Step 4** Verify that you selected the right certificate and click **Install and Restart Server**.
The certificate is installed. You need to restart the web server component of the system to enable the certificate. For CX devices, restarting the web server does not affect traffic flowing through the device.
- Step 5** Click **Restart** to restart the web server and complete the installation.
At this point, you will lose your connection to the web interface. Wait for the message that indicates the web server has restarted, then refresh (reload) the browser window. If you uploaded a certificate your browser recognizes, you will not see a certificate warning.
-

Obtaining a Server Certificate

The certificate you upload to the appliance must meet the following requirements:

- It must use the X.509 standard.
- It must include a matching private key in PEM format. DER format is not supported.
- The private key must be unencrypted.
- It can be a root certificate or an intermediate certificate.

You cannot generate Certificate Signing Requests (CSR) for the certificates from the system. Therefore, to have a certificate created for the system, you must issue the signing request from a UNIX workstation. Save the PEM-formatted key from this UNIX workstation because you will need to install it on the system later.

You can use any UNIX machine with a recent version of OpenSSL installed. Be sure to put the CX device or PRSM server hostname in the CSR. Use the guidelines at [openssl.org](https://www.openssl.org) for generating a CSR using OpenSSL; the procedure below summarizes the process.

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.

**Tip**

You can also generate and sign your own certificate. Tools for doing this are included with OpenSSL, free software from <http://www.openssl.org>.

Procedure

Step 1 Using OpenSSL, create an unencrypted RSA private key for the system.

Example:

The following commands create an RSA key file named `server.key`, and a decrypted PEM version of the RSA private key called `server.key.decrypted`. Remember the pass phrase you enter when creating the key.

```
$ openssl genrsa -des3 -out server.key 1024
$ openssl rsa -in server.key -out server.key.decrypted
```

Step 2 Generate a PEM formatted Certificate Signing Request using the RSA private key.

Example:

The following example uses the encrypted key file to generate the signing request file `server.csr`. When you are prompted for the Common Name, enter the fully-qualified domain name (FQDN) for the system. For example, if you configured the DNS name as `prsm.example.com`, so that you can open `https://prsm.example.com`, the Common Name should be `prsm.example.com`.

```
$ openssl req -new -key server.key -out server.csr
```

Step 3 Submit the CSR to a CA to obtain the signed certificate.
You can use a commercial CA, or you can create your own CA and sign the certificate yourself. Consult the OpenSSL documentation about creating your own CA.

What to Do Next

Upload the certificate and decrypted private key file using the **Administration > Server Certificates** page.

Configuring Network Participation

You can choose to provide attack and other telemetry information to Cisco to help Cisco stop web-based threats. In Multiple Device mode, your selection applies to all managed devices; you cannot select different settings per device.

Data is collected, encrypted, and sent every five minutes. There must be a path from the management interface to the Internet, or you must configure an HTTP proxy, for the transmission to succeed. Data is collected for the following general areas:

- Threat details, such as signature ID, threat score, attacker, application, web category, web reputation.

- Operational data about your device configuration and performance.

When you initially log in after installing the product, you are prompted to select your participation level. You can change it using the following procedure.

Procedure

-
- Step 1** Select **Administration > Network Participation**.
- Step 2** Select **Enable Cisco Network Participation: Yes** to participate, or **No** to decline participation.
- Step 3** If you decide to participate, select one of the following options:
- **Standard**—Detailed information is sent to Cisco, including specific IP addresses and hostnames.
 - **Partial**—Summary information is sent to Cisco, such as protocol attributes, attack type, connecting IP address and port, and summary performance statistics.
- Step 4** If you need to use an HTTP proxy to reach the Internet, click **Edit** in proxy field and configure the settings. Click **Help** in the HTTP Proxy window for more information.
- Step 5** Click **Save**.
-

Configuring an HTTP Proxy

The system needs Internet access to download updates to components and to send telemetry information if you enable network participation. Thus, the system's management address must have a route to the Internet, or you must configure an HTTP proxy that the system can use for Internet communication.

Procedure

-
- Step 1** Do any of the following:
- Select **Configurations > HTTP Proxy**.
 - Edit the proxy settings on the Updates or Network Participation pages.
- Step 2** Configure these settings:
- **HTTP Proxy Server**. Select **Enable** to configure settings and use the proxy. Select **Disable** to not use a proxy or to temporarily stop using the proxy.
 - **Proxy IP**—The IP address or fully-qualified domain name of the proxy server. For example, 10.100.10.10 or proxy.example.com.
 - **Port**—The port on which the proxy server is listening. Typical ports are 80, 3128, or 8080. Consult the configuration of the proxy server to determine the correct port number.
 - **Username, Password**—The credentials required to log into the proxy server and pass traffic through it, if any are needed.

You can click **Test Connection** to verify that the system can use the proxy.

Step 3 Click **Save**.

Basic Troubleshooting

The following topics provide tips on basic system troubleshooting. You can usually find troubleshooting related to specific policies and features next to the topics that explain those policies and features.

Checking System Connectivity

The tools for checking the connectivity between a system and other hosts on the network is the same for PRSM and CX. Assuming your physical media is healthy (wires are unbroken and securely connected to network ports), the following procedure explains the commands you can use to check connectivity.

For the CX device, keep in mind that connectivity is being checked between the management interface and the host. The management network must have a gateway to the networks between the system and the remote host, such as the PRSM server or the update servers.

Procedure

- Step 1** Log into the CLI using the console or an SSH session.
Log in as the admin user. For Cisco Prime Security Manager, access the console using the vSphere Client application.
- For the ASA CX software module, open a console session using the **session cxsc console** command in the ASA CLI.
- Step 2** Enter any combination of the following commands to check connectivity.
- **ping**—To check whether the host can respond to a simple ICMP echo request. Note that the host or intervening routers might prevent ICMP responses from a host that is otherwise reachable. For example, **ping 10.100.10.1** or **ping www.example.com**. Use Ctrl+C to stop the ping.
 - **traceroute**—To check the pathway between the system and a host. You can see the hops between the system and the host. As with ping, intervening routers might prevent the ICMP responses from a host that is otherwise reachable. For example, **traceroute 10.100.10.1** or **traceroute www.example.com**. If you start seeing * (asterisk) as the response, use Ctrl+C to stop the traceroute, because a hop is not responding. Either that hop is the problem, or the node is configured to not respond to ICMP echo requests.
 - **nslookup**—To check whether a DNS host name can be resolved to an IP address by the DNS servers that you have configured. Use the **show dns** command to check DNS settings.
 - **show route**—To check the routing table. You must have a default route (0.0.0.0) with the right gateway. Try pinging the gateway if you are not sure packets are leaving the subnet. If the gateway address is not correct, run the **setup** command and enter the correct gateway when prompted.

- **show interfaces**—To check whether the receive (RX) and transmit (TX) packet counts are incrementing. The management IP address should be defined for the eth0 interface, and packet counts should increase as you ping, trace routes, or do other network activity. If the IP address or mask is incorrect, run the **setup** command and enter the correct values when prompted.

Capturing Packets

On CX devices, you can capture packets for traffic traversing the device using the following methods:

Access policy

You can select **Capture Packets: On** on individual access policies to selectively capture packets for traffic flows that match the policy. Edit the access policy to select this option. Consider the following recommendations and limitations:

- The **Capture Packets** option works for access policies that use Layer 3 or Layer 4 (L3/L4) criteria only, or the default Any criteria. If you use any other match criteria, packets will not be captured. L3/L4 criteria are network objects and service objects.
- When you view the policies list, an icon indicates that packet capture is enabled for the policy. Mouse over icons to see the meaning of each icon.
- The packet capture file is not created until you edit the policy and select **Capture Packets: Off**. The capture file uses the policy name as the file name, with the extension .pcap. If an old capture file exists, it is overwritten.

Global setting

You can select **Dropped Packets, Capture: On** to capture packets that match Deny access policies with L3/L4 match criteria only and packets dropped due to any L3/L4 checks, for example, because they are malformed or because they do not conform to the current TCP state, such as a TCP reset that is outside the window. Malformed or non-conforming packets are dropped regardless of the access policy the traffic matches.

The packet capture file is not created until you select **Dropped Packets, Capture: Off**. The capture file is asdrop.pcap. If an old capture file exists, it is overwritten.



Note

You cannot capture traffic on the management port. Packet capture is available for traffic redirected to the CX device only.

The following procedure explains how to set up both types of packet capture and then upload the files containing the captures.

Procedure

- Step 1** Select **Configurations > Policies/Settings** and open the **Packet Capture** tab to configure the following global settings.

- **Maximum Buffer Size**—The maximum amount of memory that the capture can use to store packets. The default is 1 MB. You can select KB or MB as the unit of measure, and there is no fixed valid size range.
- **Circular Buffer: On/Off**—Whether to use a circular buffer for packet captures. If you select **On**, the capture will begin writing over the oldest packets when the maximum buffer size is reached.

(Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Click **Save** if you make changes.

- Step 2** To configure the global capture of dropped packets, do the following:
- Select **Configurations > Policies/Settings** and open the **Packet Capture** tab.
 - Select **Capture: On** in the Dropped Packets section.
 - Click **Save** to save your changes.
 - Click the **Changes Pending** link in the menu bar, then the **Commit** button on the Commit and Deploy Changes page, to commit your changes.
 - Perform the network activity whose packets you are trying to capture.
 - Edit the packet capture settings again, but this time select **Capture: Off**. Save your changes.
 - Commit your changes.
The packet capture file is written to disk.
- Step 3** To configure packet capture for individual access policies, do the following:
- Select **Configurations > Policies/Settings** and open the **Access Policies** tab.
 - Select the policy and click the **Edit Policy** button.
 - Select **Capture Packets: On**.
 - Click **Save Policy**.
When the policy is saved, you are returned to the policy list. You should see a packet capture icon on the policy.
 - Click the **Changes Pending** link in the menu bar, then the **Commit** button on the Commit and Deploy Changes page, to commit your changes.
 - Perform the network activity whose packets you are trying to capture.
 - Edit the policy again, but this time select **Capture Packets: Off**. Save your changes.
 - Commit your changes.
The packet capture file is written to disk.
- Step 4** When you are ready to examine packet captures, or to provide them to the Cisco Technical Assistance Center for analysis, log into the CLI and use the **support diagnostic** command to select the packet capture files and upload them to a server.

Example:

The following example shows how to upload the packet capture for a policy. The packet capture is put into a ZIP file whose name includes the date and time. To upload additional captures, you simply select more than one file when selecting files; you can combine them all into a single upload file. Note that file names are case sensitive; you must type capital letters when necessary when selecting files.

```
asacx> support diagnostic
===== Diagnostic =====
```

1. Create default diagnostic archive
2. Create diagnostic archive for advanced troubleshooting
3. Manually create diagnostic archive

Please enter your choice (Ctrl+C to exit): **3**

=== Manual Diagnostic ===

1. Add files and directories to package
2. View files in package
3. Upload package

Please enter your choice (Ctrl+C to exit): **1**

=== Add files and directories to package | Manual Diagnostic ===

1. Logs
2. Core dumps
3. Packet captures
4. Reporting data
5. Eventing data
6. Update data
- b. Back to main menu

Please enter your choice (Ctrl+C to exit): **3**

=====

Directory: /var/local | 514 KB

-----files-----

2012-03-20 18:37:28 | 524134 | Allow All.pcap

2012-03-20 18:52:11 | 1922 | aspdrop.pcap

([b] to go back or [m] for the menu or [s] to select files to add)

Type a sub-dir name to see its contents: **s**

Type the partial name of the file to add ([*] for all, [<] to cancel)

> **allow**

No file named 'allow'

Type the partial name of the file to add ([*] for all, [<] to cancel)

> **Allow**

Allow All.pcap

Are you sure you want to add these files? (y/n) [Y]: **y**

=== Package Contents ===

[Added] Allow All.pcap

=====

=====

Directory: /var/local

-----files-----

2012-03-20 18:37:28 | 524134 | Allow All.pcap

2012-03-20 18:52:11 | 1922 | aspdrop.pcap

([b] to go back or [m] for the menu or [s] to select files to add)

Type a sub-dir name to see its contents: **m**

=== Manual Diagnostic ===

1. Add files to package
2. View files in package
3. Upload package

Please enter your choice (Ctrl+C to exit): **3**

Creating archive

Enter upload url (FTP or TFTP) or [Ctrl+C] to exit

Example: ftp://192.168.8.1/uploads

> **ftp://10.69.43.239/diagnostics**

Uploading file cx_asacx_03_20_2012_19_12_15.zip [size: 524280]

You need to authenticate with the server to upload/download file

```

Username: ftpusername
Password: (typing not displayed)
Uploading file cx_asacx_03_20_2012_19_12_15.zip [size: 524280]
Uploading the file to /diagnostics on the remote server.
....
Successfully Uploaded ftp://10.69.43.239/diagnostics/cx_asacx_03_20_2012_19_12_15.zip

asacx>

```

Managing System Processes

Some system processes used by CX devices and Cisco Prime Security Manager are the same, others differ. However, you use the same techniques to check system process status and if necessary, to stop and restart them. You need to manage these processes only if you are getting unexpected behavior from the system, in which case checking the process status can help identify if there is a system-level problem that needs to be resolved.

The following procedure explains how to check status and restart processes, if necessary.

Tips:

- When troubleshooting CX devices, you can also use the **config advanced autorestart off** command to disable automatic process restart.
- Even if all processes are shown as healthy, your system might still be experiencing problems. If system behavior remains abnormal, reboot the system.

Procedure

- Step 1** Log into the CLI using the console or an SSH session.
Log in as the admin user. For Cisco Prime Security Manager, access the console using the vSphere Client application.
- For the ASA CX software module, open a console session using the **session cxsc console** command in the ASA CLI.
- Step 2** Enter the **show services status** command to see current system process status.

Example:

If the processes are functioning correctly, the Up status for all processes should indicate True. The following example shows that the HTTP Inspector process is down.

```

asacx> show services status
=====
Process           | PID   | Up    | Up Time
=====
HTTP Server       | 2223  | True  | 00:08:08
Capability Daemon | 2411  | True  | 00:07:58
Data Plane        | 2513  | True  | 00:07:46
AD Interface      | 2527  | True  | 00:07:45
PDS               | 2348  | True  | 00:08:07
Message Nameserver| 2264  | True  | 00:08:08
HTTP Auth Daemon  | 2373  | True  | 00:08:06
Management Plane  | 2385  | True  | 00:08:05

```

```

HTTP Inspector      | NA      | False | 00:00:00
HPM Monitor         | 2518    | True  | 00:07:46
Support Tunnel      | 2296    | True  | 00:08:08
Updater            | 2422    | True  | 00:07:58
Card Manager        | 2181    | True  | 00:08:08
ARP Daemon          | 2368    | True  | 00:08:06
Event Server        | 2404    | True  | 00:07:58
TLS Proxy           | 2493    | True  | 00:07:49
=====

```

Step 3 If the summary status indicates a problem, enter the **show services status all** command to see the detailed status.

The detailed status shows all processes, even those that are disabled intentionally. When reviewing the table, look for processes that have True for Enabled status, but something other than RUNNING for the State.

Many states are transitory. Any of the DOWN states, and RESTART_TIMEOUT, indicate that the process is not running but that the system is probably trying to start it; the process might eventually start correctly. The TRY_START and various WAIT statuses indicate the process start is in progress.

There are two end states: RUNNING, which is the desired state for an enabled process, and DISABLED, which is the desired state for a disabled process. If you see DISABLED for an enabled process, you need to stop and restart processes.

Example:

The following example shows that the HTTP Inspector process is down. The table shows that the process is enabled, but its state is DISABLED, indicating that the system has repeatedly tried to restart the process and failed. Given this output, you should stop services, then restart them. If the problem persists, reboot the system. Note that in this example, the CXSC Client process is also DISABLED, but its Enabled status is False, so in this case the process is intentionally disabled and this status line is normal.

```

hostname> show services status all
=====
Process                | PID    | Enabled | State           | Up    | Up Time
=====
HTTP Server            | 2223   | True    | RUNNING         | True  | 00:08:16
Capability Daemon      | 2411   | True    | RUNNING         | True  | 00:08:07
Data Plane             | 2513   | True    | RUNNING         | True  | 00:07:54
AD Interface           | 2527   | True    | RUNNING         | True  | 00:07:54
PDS                    | 2348   | True    | RUNNING         | True  | 00:08:16
Message Nameserver     | 2264   | True    | RUNNING         | True  | 00:08:16
HTTP Auth Daemon       | 2373   | True    | RUNNING         | True  | 00:08:15
Management Plane       | 2385   | True    | RUNNING         | True  | 00:08:13
CXSC Client            | NA     | False   | DISABLED        | False | 00:00:00
HTTP Inspector         | NA     | True    | DISABLED        | False | 00:00:00
HPM Monitor            | 2518   | True    | RUNNING         | True  | 00:07:54
Support Tunnel         | 2296   | True    | RUNNING         | True  | 00:08:16
Updater                | 2422   | True    | RUNNING         | True  | 00:08:07
Card Manager           | 2181   | True    | RUNNING         | True  | 00:08:17
ARP Daemon             | 2368   | True    | RUNNING         | True  | 00:08:15
Event Server           | 2404   | True    | RUNNING         | True  | 00:08:07
TLS Proxy              | 2493   | True    | RUNNING         | True  | 00:07:57
=====
hostname>

```

Step 4 If a process status is persistently down, restart all processes.

Example:

This example shows how to stop and then restart processes.

```

hostname> services stop
Are you sure you want to stop all services? [N]: y

```



```

.....
hostname> show services status
Process Manager Not Running
hostname> services start
Process Manager starting
hostname> show services status all
=====
Process          | PID   | Enabled | State           | Up    | Up Time
=====
HTTP Server      | 7223  | True    | RUNNING         | True  | 00:00:16
Capability Daemon | 7411  | True    | RUNNING         | True  | 00:00:07
Data Plane       | 7513  | True    | RUNNING         | True  | 00:00:54
AD Interface     | 7527  | True    | RUNNING         | True  | 00:00:54
PDTS             | 7348  | True    | RUNNING         | True  | 00:00:16
Message Nameserver | 7264  | True    | RUNNING         | True  | 00:00:16
HTTP Auth Daemon | 7373  | True    | RUNNING         | True  | 00:00:15
Management Plane | 7385  | True    | RUNNING         | True  | 00:00:13
CXSC Client      | NA    | False   | DISABLED        | False | 00:00:00
HTTP Inspector   | 7399  | True    | RUNNING         | True  | 00:00:00
HPM Monitor      | 7518  | True    | RUNNING         | True  | 00:00:54
Support Tunnel   | 7296  | True    | RUNNING         | True  | 00:00:16
Updater          | 7422  | True    | RUNNING         | True  | 00:00:07
Card Manager     | 7181  | True    | RUNNING         | True  | 00:00:17
ARP Daemon       | 7368  | True    | RUNNING         | True  | 00:00:15
Event Server     | 7404  | True    | RUNNING         | True  | 00:00:07
TLS Proxy        | 7493  | True    | RUNNING         | True  | 00:00:57
=====
hostname>

```

What to Do Next

If restarting processes does not resolve the problem, try the following commands before contacting the Cisco Technical Assistance Center (TAC):

- **system reload**, to reboot the system.
- **system shutdown**, to completely shut down the system. You will need to manually restart the device or virtual machine (VM).

Creating a Diagnostics File for the Cisco Technical Assistance Center

Cisco Technical Assistance Center (TAC) personnel might ask you to submit system log information when you submit a problem report. This information assists them with diagnosing the problem. You do not need to submit a diagnostics file unless asked to do so.

Before you create the diagnostic file, perform the actions that lead to the problem you are reporting. If necessary, you can control the level of detail in the diagnostic information by changing the minimum logging levels for various system components.

The following procedure explains how to set the logging levels and download the diagnostics file.

Procedure

- Step 1** If necessary, change the logging levels for system components and recreate the activity that leads to the problem you are diagnosing.
- Do one of the following:

- PRSM—Select **Administration > PRSM Logs**.
- CX—Select **Configurations > Policies/Settings** and open the **ASA CX Logging** tab. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

- b) Adjust the logging levels as described in [Logging Configuration Properties \(CX, PRSM\)](#), on page 384.
- c) Commit your changes.
- d) Recreate the network activity or other action that leads to the problem for which you are collecting log information.

Step 2 Click **Download Logs** on the page where you configured logging levels to download a zip file that contains all of the system logs.
For a managed CX, you can also log into the device and click the link to download logs that appears on the home page.

Note When you download logs, the system automatically runs the **show tech-support** command to generate a report that is included with the logs. The report is named `tech_support_report.txt`.

Logging Configuration Properties (CX, PRSM)

Use the logging configuration properties to set the logging level for system logging. These levels apply to the platform you are configuring, either the CX device or the PRSM management platform. Use the logging settings to control the messages generated while you are creating a diagnostic file to help Cisco Technical Assistance Center (TAC) personnel troubleshoot a problem that you are having trouble resolving.

You can change the minimum logging levels for various system components. You can select from the following logging levels, which are ordered from the level that generates the most messages to the one that generates the least messages. When you select a level, you get messages for that level and all lower levels.

- TRACE—System trace information for debugging purposes.
- DEBUG—Low level system information for debugging purposes.
- INFO—Informational messages about general system activity. This is the default logging level.
- WARNING—Information describing minor problems that are not currently affecting system operation. These problems could become significant issues.
- ERROR—Information describing major problems, ones that could have a negative impact on system operation.
- CRITICAL—Information describing critical problems, ones that could cause system-wide failures.

You can control the logging level for the following components:

- **Management Plane**—(CX, PRSM.) The component that runs the user-visible features, such as the web interface.
- **Eventing**—(CX, PRSM.) The Event Server, used for collecting events from the device and displaying them in Event Viewer.
- **HTTP Inspection Engine**—(ASA CX only.) The Security Application Scanner engine that performs deep inspection on HTTP packets.

- **Data Plane**—(ASA CX only.) The component that handles data traffic and applies policies.
- **Data Plane Syslog**—(CX.) How to handle syslog diagnostic message logging in `stdout_dp_smp.log`. The data plane sends some diagnostic information as syslog messages. The default is that data plane syslog is disabled. You can select a syslog message level to control the amount of logging. From most severe (and thus, the fewest messages) to least severe, the levels are Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug.
- **TLS Decryption Engine**—(ASA CX only.) The engine that decrypts TLS/SSL traffic flows.
- **Authentication**—(CX, PRSM.) The Authentication process, which controls the authentication service.
- **ASA-BE**—(PRSM only.) The ASA Back End process, which controls discovery from and deployment to ASA devices.

Downloading Logs

Click **Download Logs** on the page where you configured logging levels to download a zip file that contains all of the system logs.

For a managed CX, you can also log into the device and click the link to download logs that appears on the home page.

**Note**

When you download logs, the system automatically runs the **show tech-support** command to generate a report that is included with the logs. The report is named `tech_support_report.txt`.

Maintaining the System

The following topics provide information on basic system maintenance.

Backing Up and Restoring the Database

You can create backups of the configuration database and restore one if you need to. Consider creating backups before making major changes to your device and policy configurations.

The database backup-restore process is the same for the PRSM server and CX devices.

Consider the following points before doing backup and restore:

- Typically, you can restore a database backup only if the backup was from the same software version currently running on the system. However, there might be cases where the database from an older backup is compatible with a new software version.
- In Multiple Device mode, do not back up and restore individual managed CX devices. The PRSM backup includes the configurations for managed devices, so redeploying configurations should restore a device to the desired state. If you must restore a managed device from backup for an unusual disaster recovery purpose, ensure that you first switch to Single Device mode.
- When you restore a backup to a PRSM Multiple Device mode server, the policies and configuration defined in the restored database for a managed device might differ from the policies and configuration currently running on the device. That is, you might have deployed changes to a device between the time the backup was taken and the current time. In this case, you will see a Version Mismatch alert in PRSM,

and this will be visible the first time you log into the restored PRSM server. For each device with a Version Mismatch alert, the recommended action is to log into the device's managed mode home page and click the re-synchronize link. If you want to preserve the currently running configuration, delete the device from the PRSM inventory and rediscover it.

**Caution**

During backup, you are asked whether you want to clear passwords. Clear passwords only if you intend to share the backup with others, such as the Cisco Technical Assistance Center. If you recover a backup that has cleared passwords, you will have to delete all devices from the PRSM Multiple Device mode inventory and add them back to reset the passwords. In all modes, you will have to define all of the following passwords: local users (except the admin user), AD/LDAP directory, CDA or AD agent, and signature updater HTTP proxy username. After recovering a database in which passwords have been cleared, you will be able to log in as the admin user only.

The following procedure shows both the backup and the restore steps.

Procedure

- Step 1** Log into the CLI using the console or an SSH session.
Log in as the admin user. For Cisco Prime Security Manager, access the console using the vSphere Client application.
- For the ASA CX software module, open a console session using the **session cxsc console** command in the ASA CLI.
- Step 2** Use the **config backup** command to create the database backup.

Example:

The following example backs up the database to the backups folder on the FTP server. Note that you do not specify the name of the backup file; the generated file name includes the system type, hostname, and the date and time information in month_day_year_hour_minutes_seconds format (24-hour clock).

```
hostname> config backup ftp://10.69.43.239/backups
Starting the database backup process....
Please note that eventing/reporting data will not be backed up
If you are creating a backup to share with others for system Troubleshooting,
you can clear device passwords to maintain security.
A backup with cleared passwords is not suitable for system recovery.
Do you want to clear the passwords in the backup database(y/n)?[n]:n
Uploading file prsm_prsm-vm_1.0.0_04_02_2012_16_25_30.pkg to
ftp://10.69.43.239/backups
You need to authenticate with the server to upload/download file
Username: ftpusername
Password: (typing not displayed)
Backup of the database is completed.
hostname>
```

- Step 3** Use the **config restore** command to recover a backup.

Example:

The following example restores the specified backup file. You must include the file name in the URL. The note about checking for Version Mismatch alerts applies to PRSM Multiple Device mode only.

```
hostname> config restore ftp://10.69.43.239/backups/
prsm_prsm-vm_1.0.0_04_02_2012_16_25_30.pkg
```

```

Downloading: ftp://10.69.43.239/backups/prsm_prsm-vm_1.0.0_04_02_2012_16_25_30.pkg
You need to authenticate with the server to upload/download file
Username: ftpusername
Password: (typing not displayed)
Starting the database restore process....
Please note that existing eventing and reporting data will not be restored.
NOTE: The restore process removes the present configuration replacing it with
the backed up configuration.
Do you want to proceed with restore?(y/n)?[n]: y
Stopping Cisco Services for restoring Database

The database has been restored to a backup version.
NOTE: Log into PRSM and check the inventory for Version Mismatch alerts.
These alerts indicate that a managed ASA CX is running a different
configuration than the one defined in the PRSM database. You must
correct the mismatch. Either log into each ASA CX home page and
click the resynchronize link to revert to the old configuration, or
remove the device from the inventory and rediscover it to preserve
the current configuration.

Restarting Cisco Services after restoring Database
.....
hostname>

```

Scheduling Database Backups

You can configure periodic backups of the configuration database to an FTP server.

The backup schedule applies to the device you are configuring only. In PRSM Multiple Device mode, this applies to the PRSM server but not to any managed device, because the configuration of managed devices is maintained in the PRSM server's database.

If you enable scheduled backups on a device, and then add it to the PRSM server's inventory, the schedule is disabled on the discovered device.

Procedure

- Step 1** Select **Administration > Database Backup**.
The Database Backup Settings page shows your current backup schedule, if any, and the status of the last backup if known.
- Step 2** Select **Periodic Backup: On**.
You can disable the backup schedule by selecting **Periodic Backup: Off**.
- Step 3** In **Backup Periodicity**, enter the frequency, in hours, for the backup schedule.
The periodicity can be between 1 and 168 whole hours. The default is 24 hours.
This frequency will be related to the time you save your changes. You cannot select a start time or a backup window.
- Step 4** Identify the FTP server using the following fields:
 - **Server Host Name / IP Address**—The DNS name or IP address of the FTP server.
 - **Server Port**—The port on which the server listens for FTP connections. The default is 21.
 - **User Name, Password**—The username and password for logging into the FTP server to upload files.

- **Backup File Location on Server**—The server path where you want to upload backup files. For example, / for the root folder, **/backup/** for the backup folder.

Step 5 Click **Save**.

A backup is initiated when you save your changes, and subsequent backups occur according to your schedule. Use the **config restore** command in the CLI to recover a backup.

Backing Up and Restoring the PRSM VM



Note

VM backup and restore is available for PRSM Multiple Device mode only. You cannot use this procedure to back up and restore an individual CX system.

To make backups of the PRSM Multiple Device mode virtual machine (VM), including the database and configuration settings, use the VMware snapshot feature. You can create snapshots in addition to creating backups of the configuration database within the VM using the **config backup** command. If you create both snapshots and database backups, you can determine the most appropriate way to recover your system in case of problems.

The following steps explain the overall snapshot (backup) and restore process. However, you should read the VMware documentation on snapshots to understand the process and the specific steps required. All actions are done in the VMware vSphere client.

Procedure

- Step 1** Ensure that the primary disk is the only disk that will be included in the snapshot. Each secondary disk should have **Independent-Persistent** mode selected (right click the PRSM VM, select **Edit Settings**, then select each secondary disk to see whether the option is selected). These selections ensure that the disks that contain event and report data are not included in the snapshot, so your backups are not needlessly large. The point of the snapshot is to back up the database and other configuration settings so that you can return to a previously known good state if necessary.
- If the option is not selected for one or more secondary disks, open the console, log into the PRSM CLI, and enter the **system shutdown** command to shut down the system. Then, in the vSphere client, power down the VM. You can then select the **Independent-Persistent** mode options and power on the VM. If you change the disk mode option, you should also use the VMware Snapshot Manager to delete any existing snapshots that you have taken.
- Step 2** To create a snapshot, right click the PRSM VM and select **Snapshot > Take Snapshot**. You are prompted to provide a name and description and to select additional options. You should select both the **Snapshot the Virtual Machine's Memory** and **Quiesce Guest File System** options to ensure the best snapshot quality.
- Step 3** To restore the system to a backup, open the Snapshot Manager, select the desired snapshot, and click **Go To**. You are asked to confirm that you want to go back to the system state contained in the selected snapshot.

Reclaiming Disk Space

Over time, the size of the configuration database can grow as you continually edit policies and other objects, because each successive version of the object is retained. You can periodically reclaim space by pruning the database of these older versions. During the pruning process, the database is also optimized for performance. You can perform pruning in all modes.

When pruning the database, you can either remove versions older than a particular date, or you can simple retain a specified number of previous versions (3 or higher). If you elect to prune by date, no current version of a policy or object is deleted, even if it has not been changed since before that date. Pruning never compromises your currently-active versions.



Note

For a managed CX device, the database is automatically pruned to retain only the most recent three versions of any item. Thus, if you prune the database, it is optimized only, data is not deleted.

Procedure

- Step 1** Log into the CLI using the console or an SSH session.
Log in as the admin user. For Cisco Prime Security Manager, access the console using the vSphere Client application.
- For the ASA CX software module, open a console session using the **session cxsc console** command in the ASA CLI.
- Step 2** Enter the **config prune** command and follow the instructions.
For example, the following session shows how to prune the database

```
prsm-vm> config prune
  WARNING: You are about to prune the configuration database which may result
           in removal of inactive versions of objects. To continue, all
           services will be stopped; once pruning is completed, all services
           will be restarted.

Are you sure you want to proceed? [y/n]: y
Stopping services...
Pruning configuration database...

Please select which criteria to prune:
  1) Prune records prior to a specified date (default)
  2) Retain the last X number of committed changes

Choice [1]:
Prune eligible records prior to date (MM-DD-YYYY): 05-06-2013
There are 117 commit records eligible for removal. Do you want to continue? [y/n]: y
117 commit records were successfully pruned!
Running vacuum on database...
Finished vacuuming database...
Starting services...
prsm-vm>
```

Resetting the Admin Password

If you forget the password for the **admin** user, you can reset it. The following procedure explains the process. Before using this procedure, consider the following:

- You must use the console. You cannot log in as the recovery user from an SSH session.
- If you know the password and you simply want to change it, use the **config passwd** command from the console or an SSH session.
- For an ASA CX hardware module, you can also recover the password through the parent ASA using one of the following commands (which reset the password to “Admin123”) or by rebooting the boot image.
 - **hw-module module 1 password-reset**
 - **session 1 do password-reset**
- For an ASA CX software module, you can also recover the password through the parent ASA using one of the following commands (which reset the password to “Admin123”) or by rebooting the boot image.
 - **sw-module module cxsc password-reset**
 - **session cxsc do password-reset**

Before You Begin

You can also use this procedure to reset the database to factory defaults, which erases all policies that you have configured, event and report data, and the setup configuration, such as IP address, mask, gateway, DNS, and NTP.

Procedure

Step 1 Do one of the following:

- (Cisco Prime Security Manager.) Open the VMware console using the vSphere Client.
- (ASA CX hardware module.) Open the device console through the Console port.
- (ASA CX software module.) Open a console session using the **session cxsc console** command in the ASA CLI.

Step 2 Log in using the **recovery** user name at the login prompt.

If the console session is already active, enter the **exit** command to get to the login prompt. The recovery user does not have a password. You are prompted to select the action you want to take.

Example:

```
hostname login: recovery
1) Reset admin password.
```



```

2) Reset to factory defaults.
3) Exit.
#?

```

Step 3 Enter 1 to reset the password, then enter the new password twice when prompted.

Example:

```
#? 1
```

```

Changing password for admin
New password: (typing not displayed)
Retype password: (typing not displayed)
Password for admin changed by service
Press any key to exit.

```

You are returned to the login prompt when you press any key. You can now log in as the admin user.

Resetting to Factory Defaults



Caution

Resetting the database to factory defaults erases all policies and configuration settings defined through the web interface, and all collected events and report data. You cannot recover from this action. Follow this procedure only if you are certain that you do not want to keep any of your configurations. For Cisco Prime Security Manager, we recommend that you first remove all devices from the inventory before proceeding.

If you want to erase all policies, device configurations, event, and report data, and return the system to its factory defaults, you can use one of the following methods:

- The **config reset** command. Resetting the database using this command does not reset the device settings that you configured through the CLI. For example, the management IP address and mask, gateway, DNS configuration, NTP configuration, and time settings. These values are preserved so that the system remains accessible on your network. Use the **setup** and other **config** commands if you want to also change these settings.
- Log into the CX console or the PRSM Multiple Device mode vSphere Client console using the **recovery** username. Resetting the database using this method also removes the setup configuration. The setup wizard will start after the reset completes so that you can configure the system. The recovery user account prompts you for your selection; you can also reset the admin password.

The following example shows how to use the **config reset** command.

Procedure

- Step 1** Log into the CLI using the console or an SSH session.
Log in as the admin user. For Cisco Prime Security Manager, access the console using the vSphere Client application.
- For the ASA CX software module, open a console session using the **session cxsc console** command in the ASA CLI.

Step 2 Enter the **config reset** command and enter Y when asked to confirm.

Example:

The following example shows how to reset PRSM. The warning differs slightly based on the system you are resetting.

```
hostname> config reset
WARNING: You are about to erase all policy and device configurations.
Before proceeding, remove all devices from the inventory.
Otherwise, you must unmanage each managed ASA CX from its home page.
The database will be reset to factory defaults.
System setup configuration will be preserved.
You cannot undo this action.
Are you sure you want to proceed? [y/n]: y
Stopping services...
Removing settings...
Initializing database...
Generating certificates...
Starting services...
The system has been successfully reset to factory defaults.

hostname>
```



Installing Software

The following topics explain how to install system software images and upgrade packages.

- [Image and Software Packages, page 393](#)
- [Cisco Prime Security Manager Installation, page 394](#)
- [Upgrading the System, page 402](#)
- [Reimaging the ASA 5585-X CX SSP, page 407](#)
- [Reimaging the ASA CX Software Module, page 410](#)
- [Open CX and PRSM Ports, page 414](#)

Image and Software Packages

There are several different types of software packages for CX and Cisco Prime Security Manager (PRSM):

ASA CX

- ASA CX Boot Image, which you install when you need to completely reimage the ASA CX. If you partition the device, all user data is lost. Normally you would install this image for disaster recovery purposes only. You must install a System Software package after installing a boot image.

Boot image file names follow these patterns:

- **asacx-boot-*<version>*.img**, for the Cisco ASA 5585-X CX Security Services Processor.
- **asacx-5500x-boot-*<version>*.img**, for the ASA CX software module.
- ASA CX System Software, which includes the operating system and applications. The system software upgrade always requires a reboot. ASA CX system software package file names follow this pattern: **asacx-sys-*<version>*.pkg**.

PRSM

- PRSM Virtual Machine (VM), in the form of an OVA file. Because you install this package as a new VM, there is no user data to preserve; you start from a fresh installation. PRSM OVA file name follow this pattern: **prsm-vm-*<version>*.ova**.
- PRSM System Software, which includes the operating system and applications. The system software upgrade always requires a reboot. PRSM system software package file names follow this pattern: **prsm-sys-*<version>*.pkg**.

Cisco Prime Security Manager Installation

Cisco Prime Security Manager (PRSM) runs on VMware. The following sections explain the VMware setup and how to install and manage the PRSM virtual machine (VM). You must learn how to use VMware to effectively manage a PRSM Multiple Device mode server.

Preparing the Server for PRSM Installation

PRSM Multiple Device mode uses VMware as the base operating environment. You must select a server that meets the VMware installation requirements and follow the VMware documentation to install and configure VMware correctly prior to installing PRSM.



Tip

At minimum the hardware platform should be Intel Xeon Dual Core 64-bit processor with Intel VT-x support, 6GB RAM, 500 GB hard drive (RAID 5 recommended), and one or more Gigabit or 10 Gigabit Ethernet controllers. The server you select should appear on the VMware list of compatible hardware for ESXi, <http://www.vmware.com/resources/compatibility/search.php>. You must ensure that Intel Virtualization Technology (VT-x) is enabled in BIOS on the ESXi host.

Install the following VMware software:

- VMware vSphere Hypervisor (ESXi) 5.0 or 4.1 Update 2.
You are responsible for obtaining the required VMware licenses to implement your desired configuration.
- (Optional, but recommended.) VMware vCenter Server compatible with ESXi.
- VMware vSphere Client compatible with ESXi. You must install the client on your workstation, which should have at least 2 GB RAM.

Although PRSM does not have special requirements for the VMware installation, you should consider the following PRSM VM sizing recommendations when selecting an appropriate server based on the number of devices you will manage with PRSM. These are the recommended sizes for the virtual machine (VM) that you configure for PRSM. The default values shown are those that are initially configured when you install the application.

Table 9: Recommended PRSM Virtual Machine Sizing

Characteristic	Default Values	10 Devices	25 Devices	100 Devices
Cores (virtual CPUs)	2	4	6	8
Memory	4 GB	8 GB	12 GB	15 GB
Disk Space The large size is required for storing event and report data.	Two disks, 276 GB total: • 40 GB primary disk (disk 1) for application and database. • 256 GB secondary disk (disk 2) for event and report data.	2 TB secondary disk space.	3 TB secondary disk space.	3 TB secondary disk space.

Important Considerations

VMware allows you to configure a number of settings for a VM, but not all settings are meaningful for PRSM. Keep the following in mind:

- Virtual NICs (network interface cards)—PRSM uses a single network interface. Adding virtual NICs will have no effect on system performance or behavior. A single interface is used and additional interfaces will not be detected or available.
- SCSI controller—Do not change the SCSI controller type. The LSI Logic Parallel controller is the only supported type.

Installing the PRSM Virtual Machine

These installation instructions assume that you have installed the required VMware software and that you have verified that the software is functioning correctly (see [Preparing the Server for PRSM Installation, on page 394](#)). The instructions also assume that you have added the server that will host PRSM to the vCenter Server, if you use that software.

Before You Begin

During the VM installation and startup, the setup wizard will ask for the information required to make the PRSM server operational. Before you start the installation, be sure you determine the correct input for the following values:

Host name for the system.

The hostname must be fewer than 65 characters and can contain characters, numbers, and hyphens only. The first and last character must be a letter or number and the hostname cannot be all numbers.

The type of addressing to use for the management IP address.

You can configure the following types of address: static IPv4, DHCP for IPv4, static IPv6, IPv6 stateless autoconfiguration. For the ASA CX software module, the address must be on the same subnet as the ASA management address, and the ASA management interface must be up and available. You can configure both IPv4 and IPv6 addressing. Do the following:

- IPv4 static address—Determine the IPv4 management IP address, subnet mask, and gateway.
- DHCP—Ensure there is a DHCP server that will respond on the management network.



Note DHCP is not recommended. The system will stop functioning correctly if DHCP changes the assigned address due to lease expiration or other reasons. We suggest you use static addressing instead.

- IPv6 static address—Determine the IPv6 management IP address and prefix length and gateway.
- IPv6 stateless autoconfiguration—IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link.



Note IPv6 stateless autoconfiguration assigns a global address based on network prefix and a device identifier. Although this address is unlikely to change, if it does change, the system will stop functioning correctly. We suggest you use static addressing instead.

DNS information.

If you do not use DHCP, you need to specify the IP addresses (IPv4 or IPv6) of the primary and optionally, secondary, DNS servers and the local domain name. If you configure both IPv4 and IPv6 management addresses, you can enter DNS addresses in either or both formats; otherwise, you must match the format of the management address.

You can also enter a comma-separated list of search domains, which are sequentially appended to host names that are not fully qualified in an attempt to resolve the name to an IP address. For example, a search domain list would allow you to ping `www` instead of a fully-qualified name such as `www.example.com`.

NTP information.

You can decide whether to configure Network Time Protocol (NTP) for system time. When using NTP, specify the NTP server names or IPv4 addresses.

You will be asked if you want to use NTP symmetric key authentication. Authentication is useful if you want to ensure your time source is trusted. If you configure authentication, follow the prompts to add the key number (e.g. 2), key type, key, and then assign the keys to your servers based on key number. Supported key types include MD, MD2, MD5 SHA, SHA1, MDC2, and RIPEMD160. Because the key must first be defined on the NTP server, obtain the keys from the server administrator. If you own the NTP server, consult the server documentation to learn how to configure authentication.

**Note**

It is critical that system time be consistent among the CX device, its parent device, and PRSM management server. The best solution is to use NTP servers to maintain consistent time; time zones can be different, but the relative time must be equivalent. If there is a significant time mismatch, PRSM might not be able to add a device to the inventory, for example, if the start time of the CX CA certificate generated during the installation process is later than the current time on the PRSM server. Also, event and dashboard data can be skewed.

Procedure

- Step 1** Either download the PRSM VM image (an OVA file) to your workstation, or place it on an HTTP server that is accessible from your vSphere Client.
- Step 2** Log into the vSphere client, connecting to the vCenter Server on which you will install the PRSM VM.
- Step 3** Add the PRSM VM:
- Select **File > Deploy OVF Template** to start the wizard. The wizard steps can vary depending on how you have configured the server; the following steps might be slightly different on your system, including additional steps or skipping some steps mentioned here.
 - On the Source page, enter the URL of the OVA file or click **Browse** to select the file from your workstation. Click **Next**.
 - On the OVF Template Details page, view the product details and click **Next**.
 - On the End User License Agreement page, click **Accept** and then click **Next**.
 - On the Name and Location page, enter the name you want to give the VM and click **Next**. The name you select has no operational impact on PRSM.
 - On the Disk Format page, we recommend you select **Thick Provisioned Format**, which should provide better performance, but you can use thin provisioned if you prefer. Make your selection and click **Next**.
 - On the Network Mapping page, select the required mapping for your network (if it is not already selected correctly). The source network will be Bridged and the destination network should be the network corresponding to the management network mapping configured on the VMware server. Click **Next**.
 - On the Ready to Complete page, verify the configuration and click **Finish**.
The Deploying status dialog should appear, showing you the progress and estimated time to complete the installation and deployment of the OVF template. Wait for the Deployment Completed Successfully message before continuing.
- Step 4** (Optional but recommended.) When the template deployment process completes, edit the VM settings to adjust them for your requirements. Right-click the PRSM VM from the list of VMs on the server and select **Edit Settings**.
The settings to consider are mainly the following:
- **Memory**—The default is 4 GB. The vSphere client provides recommendations on the ideal settings; increase the allocation as desired to improve performance.
 - **CPUs**—The default is 2 virtual CPUs. You can increase this number to improve performance.
 - **Hard Disks**—The installation creates the following disks:
 - **Hard Disk 1**—This primary disk contains the application and the configuration database. It is a fixed size. You should regularly take snapshots of this drive so that you can restore the system if necessary.

- **Hard Disk 2**—This secondary disk is used for storing event and report data. Any disks that you add to the VM are treated as extensions of this disk, which is referred to as /var/data when you use the **show diskusage** command in the CLI. Click the **Add** button to add new disks. For more information, see [Managing PRSM Disk Space](#), on page 400.

Note Ensure that you mark all secondary disks to run in Independent-Persistent mode, so that they are not included in snapshots.

Step 5 Select the PRSM VM from the list of VMs on the server, and open the VM Console, either in the right pane or as a separate window (by clicking the **Launch Virtual Machine Console** button in the toolbar or selecting **Inventory > Virtual Machine > Open Console**).

Step 6 Power on the VM by clicking the **Power On (Play)** button in the main or Console window, or by selecting **Inventory > Virtual Machine > Power On**.

You will see the boot messages for PRSM in the Console window. Because the time required for disk initialization during initial boot is proportional to the amount of space you have allocated, the initial PRSM boot can take a long time. For example, initialization of a 5 TB disk can take 1-2 hours. Wait until you see the following message about configuring the admin password:

```
Press Enter to configure the password for 'admin' user ...
```

Step 7 Press Enter and specify the password for the admin user; your typing is not displayed.

Example:

```
The password must be at least 8 characters long and must contain
at least one uppercase letter (A-Z), at least one lowercase letter
(a-z) and at least one digit (0-9).
```

```
Enter password: (type password)
Confirm password: (retype password)
SUCCESS: Password changed for user admin
```

```
Welcome to Cisco Prime Security Manager Setup
[hit Ctrl-C to abort]
Default values are inside [ ]
```

```
Enter a hostname [prsm-vm]:
```

Step 8 You are now at the first prompt for the system setup wizard, which will guide you through the initial setup. You can rerun this wizard later using the **setup** command.

Example:

Enter the values that you determined prior to VM installation. The following example shows the configuration of both IPv4 and IPv6 static addresses.

```
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management
interface? (y/n) [N]: N
Enter an IPv4 address [192.168.8.8]: 10.89.31.65
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 10.89.31.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: Y
Enter an IPv6 address: 2001:DB8:0:CD30::1234/64
Enter the gateway: 2001:DB8:0:CD30::1
Enter the primary DNS server IP address [ ]: 10.89.47.11
Do you want to configure Secondary DNS Server? (y/n) [N]: N
Do you want to configure Local Domain Name? (y/n) [N]: Y
Enter the local domain name: example.com
```



```

Do you want to configure Search domains? (y/n) [N] Y
Enter the comma separated list for search domains: example.com
Do you want to enable the NTP service?(y/n) [N]: Y
Enter the NTP servers separated by commas: 1.ntp.example.com, 2.ntp.example.com
Do you want to enable the NTP symmetric key authentication? [N]: N
Please review the final configuration:
Hostname:                prsm-vm
Management Interface Configuration

IPv4 Configuration:      static
    IP Address:          10.89.31.65
    Netmask:              255.255.255.0
    Gateway:              10.89.31.1

IPv6 Configuration:      static
    IP Address:           2001:DB8:0:CD30::1234/64
    Gateway:              2001:DB8:0:CD30::1

DNS Configuration:
    Domain:                example.com
    Search:                 example.com
    DNS Server:            10.89.47.11

NTP servers:
    1.ntp.example.com      2.ntp.example.com

Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Restarting network services...
Restarting NTP service...
Done.
Generating self-signed certificate, the web server will be restarted after that
...
Done.
Press ENTER to continue...

```

Step 9 Press Enter to continue.

The system places you at the login prompt and displays the URL you can use to open the web interface. Use your browser to log in as admin (with the password you configured) and begin using the application.

Tip If your web browser cannot open the URL, because it cannot find the server or the server is taking too long to respond, go to the PRSM console, log in as admin, and use the **ping** command to ping your workstation IP address. Then, retry the browser connection. Also, verify that you are using **https://** instead of **http://**.

Step 10 If necessary, configure the time settings.

Use the **show time** command to determine the current date, time, and time zone for the system. The default is to use the UTC time zone.

If you are using NTP, you can configure the local time zone using the **config timezone** command. If you are not using NTP, also configure the local time using the **config time** command.

Managing PRSM Disk Space


Note

PRSM Single Device mode, the built-in management application for the CX device, automatically manages its disk space and you cannot modify disk usage.

When you install PRSM Multiple Device mode, the image contains the following disks:

- Hard Disk 1—The primary disk, which is used for the product and the configuration database. You cannot change the size of this disk.
- Hard Disk 2—The secondary disk, which is used for event and report data. When you use the **show diskusage** command in the CLI, this disk is represented as the /var/data disk. You can expand or contract the storage allocated to this disk, or add additional disks that will be used in conjunction with this disk; that is, the storage on the added disks will become part of /var/data and be used to store event and report data.

As data fills the secondary storage, older data is automatically deleted to make room for newer data.


Note

The maximum allowed disk size and your ability to change disk size is controlled by VMware and the block size that you configured for the datastore.

Use the VMware vSphere client to manage secondary disk space. You can do any of the following, and PRSM automatically detects the change during boot, formats or repartitions disks as necessary, and starts using any added space for event and report data.

- Change the size of an existing secondary disk—You can expand or contract the space on a disk if that disk is running in Independent mode (which means that it is not enabled for snapshots). All secondary disks should run in Independent mode.
- Add an additional secondary disk—Depending on the blocking factors on your hard disks, the maximum size of a virtual disk has an upper limit. However, you can create multiple secondary disks to collectively supply the amount of space you want for event and report data storage. PRSM automatically uses the additional space for event and report data.


Caution

Do not delete any disks. When you delete a secondary disk, all data that was on /var/data is lost, even data contained on disks you are not deleting. This can remove data required for the proper functioning of the system. If you inadvertently delete a disk, you must install a system software package to repair the system. Alternatively, you can recover a VMware snapshot.

The following procedure provides the detailed steps to accomplish these changes.

Procedure

- Step 1** Open the VMware vSphere client and select the PRSM VM.
- Step 2** The VM must be powered off to modify storage. If the VM is currently powered on, do the following:

- a) Right click and select **Open Console**.
- b) Log into the PRSM CLI using the admin username and password.
- c) Enter the **system shutdown** command to shut down PRSM services. Wait for the shutdown to complete.
- d) In the vSphere Client main window, right click the PRSM VM and select **Power > Power Off**.

Step 3 Right click the PRSM VM and select **Edit Settings** to open the VM Properties dialog box.

Step 4 To add space to an existing secondary disk:

- a) Select the disk.
- b) Ensure that **Independent** mode is selected. You cannot change the size of a disk that is enabled for snapshots. (The VM must be powered down to change this option.)
- c) Use the **Provisioned Size** disk provisioning fields to specify the new size.
- d) Click **OK**.

Step 5 To add a new secondary disk:

- a) Click **Add** to start the new device wizard.
- b) Follow the wizard to add the drive, ensuring that you select at least the following options:
 - Device Type—Select **Hard Disk**.
 - Disk Provisioning (Create a Disk page)—We recommend that you select the **Support Clustering Features Such As Fault Tolerance** option for the best thick-provisioning performance. However, thin provisioning is supported if you would rather take that approach.
 - Virtual Device Node (Advanced Options page)—Select an open SCSI slot.
 - Mode (Advanced Options page)—Select the **Independent** and **Persistent** options, so that the disk is not included in snapshots.
- c) Click **Finish** in the wizard to create the disk. The new disk will be formatted, provisioned, and automatically used in conjunction with all existing secondary disks to provide expanded event and report data storage when you restart the VM.

Step 6 When you are finished with your storage changes, click **OK** in the VM Properties dialog box to save the changes.

Step 7 In the vSphere Client console window for the PRSM VM, click the **Power On** button to restart PRSM. Wait until you see the login prompt, which indicates the restart is completed. During the restart, your storage changes are recognized and PRSM performs the actions required to integrate your changes into the system. You should see a message that the system is initializing the new disk and expanding the data volume.

Step 8 Log into the PRSM CLI and enter the **show diskusage** command. Your changes should be visible in the disk space metrics for the /var/data file system.

If it appears your changes have not been recognized, verify that the disk space changes are reflected in the vSphere settings for the VM, then use the **system reload** command in the console to reboot the system and check again.

Upgrading the System

The upgrade process for CX devices and PRSM is the same: you apply a System Software package to the system (the file extension is .pkg). There are unique System Software packages for each product.

You should back up the database before installing an upgrade package.

As a general rule, the software version running on the PRSM Multiple Device mode server must be the same version that is running on all CX devices being managed by the server. You should first upgrade the PRSM server before upgrading the managed devices (this rule is enforced if you use the web interface to apply upgrades). If the systems are running incompatible versions, you will see Version Mismatch alerts in PRSM Multiple Device mode for the device. While a version mismatch exists, PRSM cannot deploy changes to those devices. Thus, plan on upgrading all systems within a short time window.

**Note**

For information on the supported upgrade paths for System Software packages, see *Cisco CX and Cisco Prime Security Manager Compatibility* at http://www.cisco.com/c/en/us/td/docs/security/asacx/compatibility/cx_prsm_comp.html.

The PRSM server automatically detects when a managed device has been upgraded to a compatible software version. When this happens, the Version Mismatch state is removed and you can deploy changes to the device.

Although you can unmanage a device that is in the Version Mismatch state so that you can make configuration changes directly to the device, unmanaging the device means that you will have to delete it from the PRSM device inventory and add it back if you want to manage the device through the PRSM server again. Unmanage the device as a last resort.

Tips for System Upgrade

- When upgrading ASA CX, the device will not process traffic during the upgrade. The effect on your network depends on whether you configured fail-open or fail-close in the policy that redirects traffic to the ASA CX. If you selected fail-close, all traffic is dropped during the upgrade; if you selected fail-open, the parent ASA will pass all traffic that meets its access policy requirements.
- If two ASA CX devices are operating in ASAs configured for high availability, you should first upgrade the standby ASA CX. Do not upgrade the primary device until the upgrade on the standby device is complete.

The following topics explain system upgrade in more detail.

Installing System Upgrades from the CLI

You can upgrade the system by logging into its command line interface (CLI) and installing an upgrade package. You can use this procedure with managed or unmanaged devices as well as the PRSM server.

Procedure

- Step 1** Place the upgrade package on a server that is accessible from the management interface. You can use HTTP, HTTPS, or FTP for downloading the package.
- Step 2** Log into the CLI using the console or an SSH session.
Log in as the admin user. For Cisco Prime Security Manager, access the console using the vSphere Client application.
- For the ASA CX software module, open a console session using the **session cxsc console** command in the ASA CLI.
- Step 3** Enter the **system upgrade** command with the URL to the package file.

Example:

The following example applies the system upgrade named prsm-sys-9.0.2.pkg from the upgrades.example.com web server. In this example, the web server does not require authentication; you are prompted for a username and password if the server requires authentication.

```
prsm-vm> system upgrade http://upgrades.example.com/packages/prsm-sys-9.0.2.pkg
Verifying
Downloading
Extracting
Package Detail
      Description:          Cisco Prime Security Manager 9.0.2 System Upgrade
      Requires reboot:      Yes

NOTE: You must upgrade all ASA CX managed by this PRSM server to same version
or you will not be able to deploy configurations to those devices.

Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Extracting the upgrade image
Updating the system and network configuration

Reboot is required to complete the upgrade. Press Enter to reboot the system.
(press Enter)

Broadcast message from root (pts/0) (Tue May 15 22:50:17 2012):

The system is going down for reboot NOW!
```

- Step 4** Log back into the CLI after the system reboots.
- Step 5** Verify the installation by doing the following:
- In the CLI, enter the **show services status** command and verify that all processes are up.
 - Log into the web interface to verify that it is accessible.
 - Use Event Viewer or other features to verify that the system is functional.

What to Do Next

If you need to, you can uninstall the upgrade and return to the previously installed package, if there is a previously installed package. To return to the previous package, log into the CLI console and use the **system revert** command.

Applying Upgrades from the Web Interface

The following topics explain how to apply upgrades using the web interface.

The Upgrade Manager

You can use the Upgrade Manager to apply System Software packages to CX devices and PRSM systems. When operating in Single Device mode, upgrades apply to the system you are logged into only. When operating in Multiple Device mode, you can upgrade managed devices and also the PRSM server itself.



Tip

When upgrading managed devices, the PRSM server must already be upgraded to the version you want to apply to the devices. That is, you must upgrade the PRSM server first, then upgrade the managed devices. You will be prevented from applying packages at a higher level than the one running on the PRSM server.

You cannot use the Upgrade Manager to apply upgrades to an ASA device.

To open the Upgrade Manager, select **Administration > Upgrade**.

The Upgrade Manager page has two tabs. On the **Upgrade Packages** tab, you upload and apply packages. On the **Upgrade Status** tab, you can view the status of previous or current upgrades.

Upgrade Packages Tab

The **Upgrade Packages** tab includes the following:

- **I Want To**—Contains the following commands:
 - **Upload an Upgrade Package**—To upload package files to the device. You must upload a package before you can apply it to a system.
- **Package List**—Shows each package available on the system. The package title explains the type of package and the system type to which it applies. Also shown are the package version and file size, the date when the package was uploaded, and the user who uploaded it.

To see commands related to a package, mouse over it. The following are the available commands:

- **Upgrade**—To start applying it to a device. You are presented with the list of devices to which the package applies.
- **Delete**—To delete the package from storage. Deleting a package does not uninstall it from any system.

Upgrade Status Tab

The **Upgrade Status** page lists all devices in the system. In Single Device mode, this is the device itself. In Multiple Device mode, this includes all managed devices and the PRSM server.

Information includes the device name, IP address, and device model, the upgrade status, the current software version running on the device, and the start and finish time of the last upgrade.

Uploading Upgrade Packages

Before you can apply an upgrade package to a system, you must upload it to the device (in Single Device mode) or the PRSM server (when upgrading a managed device or the server itself).

Download the package file to your workstation or to another server from which you can select the file. You cannot use a URL to upload the file to the system through the web interface.

Procedure

-
- Step 1** Select **Administration > Upgrade**.
 - Step 2** Select the **Upgrade Packages** tab.
 - Step 3** Select **I want to > Upload an Upgrade Package**.
 - Step 4** Drag a package file from your file system into the upload box (if supported), or click the box to select the file. Wait for the upload to complete. You can cancel the upload by clicking the **X** on the right of the status line.
You can upload more than one package at a time.
-

Installing System Upgrades from the Web Interface

The method for applying an upgrade to the system you are logged into, either in Single Device mode or when upgrading the PRSM server, is very similar to applying upgrades to managed devices from the PRSM server. The following procedure explains both cases.

Before You Begin

Upload the package you want to install.

Procedure

-
- Step 1** Select **Administration > Upgrade**.
 - Step 2** Select the **Upgrade Packages** tab.
 - Step 3** Mouse over the package you want to install and click **Upgrade**.
The system evaluates the package and determines which devices can support it. When the evaluation is finished, eligible devices are listed. Information about each device includes the device name, IP address, current software version, device model, and system status.
In Single Device mode, and for PRSM server packages, a single device is listed, the one you are logged into.
 - Step 4** Select the device you want to upgrade.
Clicking a device toggles between selecting and deselecting the device. Selected devices are highlighted.
 - Step 5** Click **Upgrade**.
You are asked to confirm that you want to start the upgrade on the selected devices.
 - Step 6** Click **Start Upgrade**.
The system starts processing the upgrade request.

If the upgrade fails, the system automatically reverts to the previously installed version.

What to Do Next

After you start an upgrade, what happens next depends on the type of upgrade you are applying:

Applying upgrades to the system you are logged into (Single Device mode, or PRSM server upgrades)

During the upgrade process, the web interface shows the status of the upgrade. Wait until the process completes. You can then click the link to log into the device. You cannot use the system during the upgrade.

When you log in using the link from the upgrade status page, you are taken to the About PRSM page. This page shows the date of the last upgrade and the status of the upgrade. Verify that the status says the upgrade completed successfully.

Applying upgrades to managed devices from the PRSM server

Wait for the Upgrade Started message, which indicates that the systems have begun to upgrade themselves. You can click the **View Status** button to open the **Upgrade Status** tab, where you can track the status of the upgrades. You can also use other features on the PRSM server while the managed devices are upgrading themselves.

Troubleshooting System Upgrades

Following are some tips on troubleshooting system upgrades:

After upgrade, the web interface does not behave as expected.

Go to your browser options and clear the browser cache, particularly the Java cache. Leftovers from the previous version might be affecting the application.

File upload fails during upload.

If your connection is particularly slow, such as a remote access VPN connection, the browser might fail to upload a package. You might see “unexpected error” in the upgrade manager, or an indication that a response was not received. In this case, either try again from a better network connection, or use the **system upgrade** command in the CLI to upgrade each system.

File upload fails due to lack of space.

The device has a limited amount of space to store packages. Delete older packages that you no longer need.

No selectable devices are listed when you select a package in Multiple Device mode.

Following are some of the reasons this might happen:

- If the package is at a higher level than the PRSM server, you cannot apply it to any managed device. Upgrade the PRSM server to this version first, then try upgrading the managed devices.
- A device to which the upgrade would otherwise apply is currently unreachable, for example, there is a lack of connectivity, the device is currently processing an upgrade, or you just added it to the inventory and device discovery is still in progress. This might be a temporary problem or the device might need your attention. Refresh the list if some devices are temporarily ineligible.
- There are no devices of the device type to which the package applies in the inventory.

Reimaging the ASA 5585-X CX SSP

If you need to reimage the Cisco ASA 5585-X CX Security Services Processor for any reason, you need to install both the Boot Image and an ASA CX System Software package, in that order. You must install both packages to have a functioning system. Under normal circumstances, you do not need to reimage the system to install upgrade packages.

To install the boot image, you need to TFTP boot the image from the Management-0 port on the ASA CX SSP by logging into the ASA CX SSP Console port. Because the Management-0 port is on an SSP in the first slot, it is also known as Management1/0, but rommon recognizes it as Management-0 or Management0/1.

To accomplish a TFTP boot, you must:

- Place the software image on a TFTP server that can be accessed through the Management1/0 interface on the ASA CX SSP.
- Connect Management1/0 to the network. You must use this interface to TFTP boot the ASA CX Boot Image.
- Configure rommon variables. Press Esc to interrupt the auto-boot process so that you can configure rommon variables.

Once the boot image is installed, you install the ASA CX System Software package. You must place the package on an HTTP server that is accessible from the ASA CX.

The following procedure explains how to install the boot image and then install the ASA CX System Software package.

Procedure

-
- Step 1** Connect to the Console port. Use the console cable included with the ASA product to connect your PC to the console using a terminal emulator set for 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control. See the hardware guide for your ASA for more information about the console cable.
- Step 2** Enter the **system reload** command to reboot the system:

Example:

```
asacx-host > system reload
Are you sure you want to reload the system? [N]: y
```

```
Broadcast message from root (pts/0) (Mon May 14 23:07:55 2012):
The system is going down for reboot NOW!
```

Step 3 Press Esc to interrupt the boot process so that you can configure rommon variables. You must configure at least the following variables:

- **ADDRESS**—The IP address of the ASA CX SSP.
- **SERVER**—The IP address of the TFTP server.
- **GATEWAY**—The gateway address to the TFTP server. If the TFTP server is directly attached to Management1/0, use the IP address of the TFTP server.
- **IMAGE**—The ASA CX Boot Image path and image name on the TFTP server. For example, if you place the file on the TFTP server in /tftpboot/asacsimages/filename.img, the IMAGE value is asacximages/filename.img.

Example:

Following is an example of configuring the variables. Before entering the sync command, you can enter the set command to view the rommon variables and to confirm that they are correct.

Note Type these parameters as shown in all upper case letters. This syntax does not work if you use lower case. Include the full name of the image file.

```
rommon #1> ADDRESS=172.20.12.60
rommon #2> SERVER=172.20.12.51
rommon #3> GATEWAY=172.20.12.2
rommon #4> IMAGE=asacximages/asacx-boot.img
rommon #5> sync
```

```
Updating NVRAM Parameters...
```

Step 4 Initiate the TFTP boot:

Example:

```
rommon #6> tftp
```

The boot process can take a few minutes.

Step 5 Log in as **admin** (default password is **Admin123**).

Step 6 Create the required partitions.

Example:

```
asacx-boot> partition
....
Partition Successfully Completed
asacx-boot>
```

Step 7 Use the setup command to configure the system:

Example:

```
asacx-boot> setup
```

When you complete the wizard, you are shown a summary of the configuration. Enter **Y** to save the configuration.

- Step 8** Use the **system install** command to install the ASA CX System Software package. You must first ensure that the package is on an HTTP/HTTPS/FTP server that is accessible to the ASA CX.

Example:

For example, the following command will upgrade the system with the asacx-sys-9.0.2.pkg package. Enter **Y** to install the upgrade.

```
asacx-boot> system install https://upgrades.example.com/packages/asacx-sys-9.0.2.pkg
You need to authenticate with the server to download the package.
  Username: username
  Password: (typing not displayed)
Verifying
Downloading
Extracting
Package Detail
  Description:          Cisco ASA CX System Upgrade
  Requires reboot:      Yes

Do you want to continue with upgrade? [y]: Y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Stopping all the services ...
Starting upgrade process ...

Reboot is required to complete the upgrade. Press Enter to reboot the system.
```

- Step 9** Press Enter to reboot the system.
- During the reboot process, you will see the following boot options. Option 0, Cisco ASA CX Image, is the option that will automatically boot, and it is the option you want. The other option is for disaster recovery. Allow the system to automatically boot with the default option 0, or manually select option 0 and press Enter.

```
-----
0: Cisco ASA CX Image
1: Cisco ASA CX Boot Image
-----
```

- Step 10** Log in as the **admin** user with the password **Admin123**.
- Step 11** If necessary, configure the time settings.
- Use the **show time** command to determine the current date, time, and time zone for the system. The default is to use the UTC time zone.
- If you are using NTP, you can configure the local time zone using the **config timezone** command. If you are not using NTP, also configure the local time using the **config time** command.
- Step 12** Use the **config passwd** command to change the password for the admin user. You are prompted for the new password.
- Step 13** The device is now ready for use.

Use a browser to open the web interface using **https://server_address**.

You can log out of the CLI by entering the **exit** command.

Note For information on the other commands available in the CLI, enter **help** or **?**.

Reimaging the ASA CX Software Module

If you need to reimage the ASA CX software module available on the ASA 5500-X series for any reason, you need to install both the Boot Image and an ASA CX System Software package, in that order. You must install both packages to have a functioning system. Under normal circumstances, you do not need to reimage the system to install upgrade packages.



Note

You would also use this procedure if you install a new ASA CX drive in an ASA 5500-X chassis. This procedure assumes that you have already correctly installed the required drives in the device. The procedure also assumes that you have installed an ASA image that supports the ASA CX software module.

You must download the appropriate ASA CX Boot Image to the ASA flash from a TFTP server. Place the image on a TFTP server you can access from the ASA management port.

The free space on flash should be at least 3GB plus the size of the boot image.

Procedure

Step 1 Open a CLI session to the ASA using the console or SSH.

Step 2 Download the appropriate ASA CX image to the ASA flash.

Example:

In the following example, replace <TFTP Server> with the address of your server and use the correct image name for the file you are downloading.

```
ciscoasa# conf t
ciscoasa(config)# copy tftp://<TFTP SERVER>/asacx-5500x-boot-9.1.1-28.img disk0:/
```

Step 3 Remove any existing ASA CX image and shut down IPS if necessary.

If the system has an existing ASA CX image, uninstall it. If you ever enabled the IPS software module, ensure that it is shut down and uninstalled.

Tip If you have an active service policy redirecting traffic to an IPS module, you must remove that policy. For example, if the policy is a global one, you would use **no service-policy ips_policy global**.

Example:

The following example uninstalls an ASA CX image and verifies that the IPS module is shut down before uninstalling it. Verify that the state of the IPS module in the show module output is "Down." This example

does not show a required command sequence; omit any commands that are not necessary for your device. If you must uninstall a module, reload the device. (Output is omitted.)

```
ciscoasa(config)# sw-module module cxsc uninstall
ciscoasa(config)# sw-module module ips shutdown
ciscoasa(config)# sh module ips
ciscoasa(config)# sw-module module ips uninstall
ciscoasa(config)# reload
```

- Step 4** Install the boot image.
The image requires at least 5-15 minutes to boot.

Example:

In the following example, use the name of the image you downloaded to disk0.

```
ciscoasa(config)# sw-module module cxsc recover configure image
disk0:/asacx-5500x-boot-9.1.1-28.img
ciscoasa(config)# sw-module module cxsc recover boot
```

- Step 5** Open a console session to ASA CX using the **session cxsc console** command.
Log in as **admin** (default password is **Admin123**).
To leave the console session and return to the ASA CLI, press Ctrl-^ (typically Ctrl-Shift-6), then press x.

Example:

```
ciscoasa# session cxsc console
Establishing console session with slot 1
Opening console session with module cxsc.
Connected to module cxsc. Escape character sequence is 'CTRL-SHIFT-6 then x'.
cxsc login: admin
Password: Admin123
```

- Step 6** Create the required partitions.

Example:

```
asacx-boot> partition
Disk /dev/sda doesn't contain a valid partition table
WARNING: You are about to erase all policy configurations and data.
You cannot undo this action.
Are you sure you want to proceed? [y/n]: y

....
Partition Successfully Completed
asacx-boot>
```

- Step 7** Use the **setup** command to configure the system:

Example:

```
asacx-boot> setup
```

Before you start the setup wizard, be sure you determine the correct input for the following values (the default host name is asacx):

Host name for the system.

The hostname must be fewer than 65 characters and can contain characters, numbers, and hyphens only. The first and last character must be a letter or number and the hostname cannot be all numbers.

The type of addressing to use for the management IP address.

You can configure the following types of address: static IPv4, DHCP for IPv4, static IPv6, IPv6 stateless autoconfiguration. For the ASA CX software module, the address must be on the same subnet as the ASA management address, and the ASA management interface must be up and available. You can configure both IPv4 and IPv6 addressing. Do the following:

- IPv4 static address—Determine the IPv4 management IP address, subnet mask, and gateway.
- DHCP—Ensure there is a DHCP server that will respond on the management network.

Note DHCP is not recommended. The system will stop functioning correctly if DHCP changes the assigned address due to lease expiration or other reasons. We suggest you use static addressing instead.

- IPv6 static address—Determine the IPv6 management IP address and prefix length and gateway.
- IPv6 stateless autoconfiguration—IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link.

Note IPv6 stateless autoconfiguration assigns a global address based on network prefix and a device identifier. Although this address is unlikely to change, if it does change, the system will stop functioning correctly. We suggest you use static addressing instead.

DNS information.

If you do not use DHCP, you need to specify the IP addresses (IPv4 or IPv6) of the primary and optionally, secondary, DNS servers and the local domain name. If you configure both IPv4 and IPv6 management addresses, you can enter DNS addresses in either or both formats; otherwise, you must match the format of the management address.

You can also enter a comma-separated list of search domains, which are sequentially appended to host names that are not fully qualified in an attempt to resolve the name to an IP address. For example, a search domain list would allow you to ping `www` instead of a fully-qualified name such as `www.example.com`.

NTP information.

You can decide whether to configure Network Time Protocol (NTP) for system time. When using NTP, specify the NTP server names or IPv4 addresses.

You will be asked if you want to use NTP symmetric key authentication. Authentication is useful if you want to ensure your time source is trusted. If you configure authentication, follow the prompts to add the key number (e.g. 2), key type, key, and then assign the keys to your servers based on key number. Supported key types include MD, MD2, MD5 SHA, SHA1, MDC2, and RIPEMD160. Because the key must first be defined on the NTP server, obtain the keys from the server administrator. If you own the NTP server, consult the server documentation to learn how to configure authentication.

When you complete the wizard, you are shown a summary of the configuration. Enter **Y** to save the configuration.

- Step 8** Use the **system install** command to install the ASA CX System Software package. You must first ensure that the package is on an HTTP/HTTPS/FTP server that is accessible to the ASA CX.

Example:

For example, the following command will upgrade the system with the `asacx-sys-9.1.1.pkg` package. Enter **Y** to install the upgrade.

```
asacx-boot> system install https://upgrades.example.com/packages/asacx-sys-9.1.1.pkg
You need to authenticate with the server to download the package.
  Username: username
  Password: (typing not displayed)
Verifying
Downloading
Extracting
Package Detail
  Description:          Cisco ASA CX System Upgrade
  Requires reboot:      Yes

Do you want to continue with upgrade? [y]: Y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Stopping all the services ...
Starting upgrade process ...

Reboot is required to complete the upgrade. Press Enter to reboot the system.
```

- Step 9** Press Enter to reboot the system.
Rebooting the system closes the console session. Allow 10-15 minutes for the system to reboot.

- Step 10** Open a console session and log in as the **admin** user.

Example:

```
ciscoasa# session cxsc console
```

- Step 11** If necessary, configure the time settings.
Use the **show time** command to determine the current date, time, and time zone for the system. The default is to use the UTC time zone.

If you are using NTP, you can configure the local time zone using the **config timezone** command. If you are not using NTP, also configure the local time using the **config time** command.
- Step 12** Use the **config passwd** command to change the password for the admin user. You are prompted for the new password.
- Step 13** The device is now ready for use.
Use a browser to open the web interface using `https://server_address`.

You can log out of the CLI by entering the **exit** command.

Note For information on the other commands available in the CLI, enter **help** or **?**.

Open CX and PRSM Ports

The firewall on the management interface for CX devices and the PRSM server close almost all ports for incoming connections. The following lists explain which ports remain open and their use.

CX Devices

- ICMP echo requests (ping)—icmp/8
- SSH—tcp/22
- HTTPS—tcp/443
- CDA or AD Agent communications—udp/3799

PRSM Server

- ICMP echo requests (ping)—icmp/8
- SSH—tcp/22
- HTTPS—tcp/443
- CX Event Reception—tcp/4466
- Syslog—udp/514
- CDA or AD Agent communications—udp/3799



INDEX

A

- AAA server [226, 231, 233](#)
 - LDAP/AD directory properties (CX) [231](#)
 - LDAP/AD directory search base (CX) [233](#)
 - supported (CX) [226](#)
- abandoning changes [30](#)
- About page [29](#)
- access policies, ASA [357, 358, 359](#)
 - about [357](#)
 - configuring [357](#)
 - managing [358](#)
 - properties [359](#)
- access policies, context-aware [249, 250, 253, 257, 258, 259, 261, 263, 264, 265, 266, 267, 268, 269, 271, 272, 276, 277, 279, 281](#)
 - application filtering [266, 267, 268, 269, 279, 281](#)
 - compared to URL filtering [267](#)
 - configuring updates [279](#)
 - controlling [268](#)
 - decryption requirements [269](#)
 - overview [266](#)
 - tips [269](#)
 - troubleshooting updates [281](#)
 - applying rate limits [258](#)
 - configuring [250](#)
 - configuring IPS filtering [276](#)
 - configuring IPS settings [277](#)
 - controlling network access [249](#)
 - default behavior [250](#)
 - enforcing Safe Search [259](#)
 - Next Generation IPS filtering [279, 281](#)
 - troubleshooting updates [281](#)
 - configuring updates [279](#)
 - notifying end users of blocks [259, 261, 263, 264, 265](#)
 - customizing [263](#)
 - editing message [263](#)
 - importing message [264](#)
 - overview [259](#)
 - reference [261](#)
 - variables [265](#)
 - when sent [259](#)
 - overview [249](#)
- access policies, context-aware (*continued*)
 - properties [253](#)
 - URL filtering [266, 267, 271, 272, 279, 281](#)
 - controlling URL access [271](#)
 - determining URL Category [272](#)
 - compared to application filtering [267](#)
 - configuring updates [279](#)
 - overview [266](#)
 - troubleshooting updates [281](#)
 - warning policies [257](#)
- active authentication [240](#)
 - enabling [240](#)
- Active Directory (AD) [231, 233](#)
 - properties (CX) [231](#)
 - search base [233](#)
- Active Directory (AD) agent [53, 245](#)
 - configuring passive authentication [53](#)
 - identifying [245](#)
- active MAC address [321, 324, 328, 331](#)
- add [318](#)
 - interface [318](#)
- address translation [343](#)
- admin user [367, 390](#)
 - characteristics [367](#)
 - resetting password [390](#)
- alerts [26, 176](#)
 - icons [26](#)
 - responding to [176](#)
- AnyConnect [67](#)
 - monitoring and controlling clients [67](#)
- application objects [138](#)
 - reference [138](#)
- application service objects [140](#)
 - reference [140](#)
- Application Visibility and Control (AVC) [51, 67, 71, 266, 267, 268, 269, 270, 279, 281](#)
 - controlling applications [51, 268](#)
 - controlling applications for Secure Mobility clients [67](#)
 - filtering overview [266](#)
 - license [71](#)
 - viewing application details [270](#)
 - compared to URL filtering [267](#)

Application Visibility and Control (AVC) *(continued)*

- configuring updates [279](#)
- decryption requirements [269](#)
- tips on application filtering [269](#)
- troubleshooting updates [281](#)

applications [51, 67, 266, 267, 268, 269, 270, 279, 281](#)

- filtering [51, 67, 266, 267, 268, 269, 279, 281](#)
 - controlling [51, 67, 268](#)
 - compared to URL filtering [267](#)
 - configuring updates [279](#)
 - controlling [51, 67, 268](#)
 - decryption requirements [269](#)
 - overview [266](#)
 - tips [269](#)
 - troubleshooting updates [281](#)
- viewing details [270](#)

applications with malicious transactions [179](#)

- dashboard [179](#)

ASA [9, 12, 13, 357, 358, 359](#)

- altering access rules for ASA CX [13](#)
- altering configuration for ASA CX [12](#)
- altering inspection rules for ASA CX [13](#)
- configuration restrictions for ASA CX [9](#)
- access policies [357, 358, 359](#)
 - about [357](#)
 - configuring [357](#)
 - managing [358](#)
 - properties [359](#)

ASA CX [1, 3, 7, 9, 12, 13, 14, 16, 17, 18, 23, 41, 46, 393, 402, 405, 406, 407, 410](#)

- altering ASA configuration [12](#)
- ASA configuration restrictions [9](#)
- configuring ASA access rules [13](#)
- configuring ASA inspection rules [13](#)
- configuring monitor-only mode [16](#)
- features [3](#)
- initial setup [7](#)
- installation [393, 407, 410](#)
 - boot image (5585-X) [407](#)
 - boot image (software modules) [410](#)
 - overview of packages [393](#)
- installing upgrades [402, 405, 406](#)
 - CLI [402](#)
 - troubleshooting [406](#)
 - web interface [405](#)
- introduction [1](#)
- logging in [23](#)
 - CLI console [23](#)
- monitoring mode [46](#)
- overview [3](#)
- preparing for management [7](#)
- redirecting traffic to [14, 16, 17, 18](#)
 - configuring monitor-only mode [16](#)
 - overview [14](#)

ASA CX *(continued)*

- redirecting traffic to *(continued)*
 - troubleshooting PRSM [18](#)
 - using ASA CLI [14](#)
 - using PRSM [17](#)
- setting up software [9](#)
- transparent mode [41](#)
- use cases [41](#)

ASA devices [14, 16, 17, 18, 81, 83, 84, 85, 87, 91, 93, 94, 95, 97, 99, 194](#)

- actions requiring delete, re-import [87](#)
- adding HA to inventory [94](#)
- adding to inventory [91, 93](#)
- converting to full management [97](#)
- discovery [84, 85](#)
- managing [81](#)
- preparing for management [83](#)
- redirecting traffic to ASA CX [14, 16, 17, 18](#)
 - configuring monitor-only mode [16](#)
 - overview [14](#)
 - troubleshooting PRSM [18](#)
 - using ASA CLI [14](#)
 - using PRSM [17](#)

- troubleshooting discovery [99](#)
- troubleshooting import and discovery [95](#)
- logging properties [194](#)

authentication services (ASA CX) [53, 56](#)

- configuring passive authentication [53](#)
- controlling access by user group [56](#)

authentication services (CX) [225, 226, 227, 228, 230, 231, 233, 234, 235, 236, 240, 241, 242, 243, 246](#)

- configuring [227](#)
- configuring directory realms [230](#)
- configuring identity policies [235](#)
- configuring settings [246](#)
- deleting directories [234](#)
- deleting directory realms [234](#)
- directory properties [231](#)
- directory realm overview [228](#)
- directory search base [233](#)
- enabling active authentication [240](#)
- enabling transparent authentication [241](#)
- enabling transparent authentication (Firefox) [243](#)
- enabling transparent authentication (Internet Explorer) [243](#)
- identity policy properties [236](#)
- identity types [226](#)
- managing [225](#)
- overview [225](#)
- supported servers and methods [226](#)
- transparent authentication requirements [242](#)
- what to tell users [227](#)

B

- backup [385, 387, 388](#)
 - database [385](#)
 - PRSM virtual machine [388](#)
 - scheduling database [387](#)
- basic authentication [241](#)
- Bidirectional NAT [344](#)
- blacklist blocking [277](#)
 - enabling [277](#)
- bootstrapping [7, 83](#)
 - ASA CX [7](#)
 - ASA devices, for management [83](#)
- bridge group [332](#)
 - properties [332](#)
- browser [21](#)
 - requirements [21](#)

C

- CA certificates [293](#)
 - ASA CX [293](#)
 - downloading, installing the CA certificate [293](#)
- category (URL) [271, 272, 279, 281](#)
 - configuring updates [279](#)
 - descriptions [272](#)
 - determining [272](#)
 - filtering [271](#)
 - troubleshooting updates [281](#)
- certificates [98, 291, 293, 294, 373, 374](#)
 - configuring decryption certificate [291](#)
 - configuring supplemental trusted [294](#)
 - converting certificate formats [293](#)
 - installing server [373](#)
 - obtaining server [374](#)
 - refreshing device [98](#)
- change history [35, 37](#)
 - viewing [35](#)
 - when changes become active [37](#)
- Cisco Technical Assistance Center [383](#)
 - creating diagnostic file [383](#)
- columns [169](#)
 - dashboard and report [169](#)
- Commit and Deploy Changes page [30, 32, 33, 35, 37](#)
 - committing changes [30](#)
 - discarding changes [30](#)
 - managing jobs [33](#)
 - overview [32](#)
 - viewing change history [35](#)
 - when changes become active [37](#)
- configuration [97](#)
 - re-importing [97](#)

- configurations [99](#)
 - troubleshooting discovery [99](#)
- connectivity (system) [377](#)
 - checking [377](#)
- console [23](#)
 - logging into ASA CX [23](#)
 - logging into PRSM [23](#)
- Context Directory Agent [53, 245](#)
 - configuring passive authentication [53](#)
 - identifying [245](#)
- context-aware access policies [249, 250, 253, 257, 258, 259, 261, 263, 264, 265, 266, 267, 268, 269, 271, 272, 276, 277, 279, 281](#)
- application filtering [266, 267, 268, 269, 279, 281](#)
 - compared to URL filtering [267](#)
 - configuring updates [279](#)
 - controlling [268](#)
 - decryption requirements [269](#)
 - overview [266](#)
 - tips [269](#)
 - troubleshooting updates [281](#)
- applying rate limits [258](#)
- configuring [250](#)
- configuring IPS filtering [276](#)
- configuring IPS settings [277](#)
- controlling network access [249](#)
- default behavior [250](#)
- enforcing Safe Search [259](#)
- Next Generation IPS filtering [279, 281](#)
 - troubleshooting updates [281](#)
 - configuring updates [279](#)
- notifying end users of blocks [259, 261, 263, 264, 265](#)
 - customizing [263](#)
 - editing message [263](#)
 - importing message [264](#)
 - overview [259](#)
 - reference [261](#)
 - variables [265](#)
 - when sent [259](#)
- overview [249](#)
- properties [253](#)
- URL filtering [266, 267, 271, 272, 279, 281](#)
 - controlling URL access [271](#)
 - determining URL Category [272](#)
 - compared to application filtering [267](#)
 - configuring updates [279](#)
 - overview [266](#)
 - troubleshooting updates [281](#)
- warning policies [257](#)
- Context-Aware Security [1, 21](#)
 - getting started [21](#)
 - overview [1](#)
- CX devices [1, 22, 30, 71, 72, 74, 75, 76, 78, 81, 84, 87, 91, 94, 95, 226, 363, 377, 378, 385, 387, 389, 390, 391, 393, 402, 405, 414](#)
 - actions requiring delete, re-import [87](#)

CX devices (*continued*)

- adding HA to inventory [94](#)
- adding to inventory [91](#)
- backing up database [385](#)
- capturing packets [378](#)
- checking connectivity [377](#)
- committing changes [30](#)
- discarding changes [30](#)
- discovery [84](#)
- installing upgrades [393, 402, 405](#)
 - overview of packages [393](#)
 - overview [402](#)
 - uploading packages [405](#)
- introduction [1](#)
- licenses [71, 72, 74, 75, 76, 78](#)
 - applying [76](#)
 - revoking [78](#)
 - uploading [75](#)
 - assigning [76](#)
 - implications of expiration [72](#)
 - overview [71](#)
 - renewing [76](#)
 - using evaluation [74](#)
- logging in [22](#)
 - overview [22](#)
 - web interface [22](#)
- maintaining [363](#)
- managing [81](#)
- managing in multiple device mode [81](#)
- managing licenses [71](#)
- open management ports [414](#)
- pruning database [389](#)
- resetting admin password [390](#)
- resetting to factory defaults [391](#)
- restoring database [385](#)
- scheduling database backups [387](#)
- supported AAA servers and methods [226](#)
- troubleshooting [363](#)
- troubleshooting import and discovery [95](#)

D

- dashboards [157, 160, 162, 164, 166, 167, 169, 173, 174, 176, 179, 180, 181](#)
 - ASA traffic [181](#)
 - changing time range [166](#)
 - columns [169](#)
 - controlling data [167](#)
 - data collection and quality [162](#)
 - descriptions [160](#)
 - drilling into [164](#)
 - malware traffic [179](#)
 - monitoring health and performance [174](#)

dashboards (*continued*)

- network overview [173](#)
- NG Intrusion Prevention [180](#)
- overview [157](#)
- responding to alerts [176](#)
- using [162](#)
- viewing [157](#)
- database [388, 389, 391](#)
 - pruning [389](#)
 - resetting to factory defaults [391](#)
 - VMware snapshots [388](#)
- decryption policies [77, 283, 285, 286, 287, 288, 289, 291, 293, 294, 295, 297, 300, 302](#)
 - 3DES/AES K9 license [77](#)
 - bypassing [300](#)
 - configuration overview [288](#)
 - configuring [295](#)
 - configuring decryption certificate [291](#)
 - configuring settings [289](#)
 - configuring supplemental trusted certificates [294](#)
 - converting certificate formats [293](#)
 - decrypted traffic flow [286](#)
 - do not decrypt traffic flow [287](#)
 - downloading, installing the CA certificate [293](#)
 - managing [283](#)
 - overview [283](#)
 - properties [297](#)
 - purpose of decryption [285](#)
 - tips, limitations [288](#)
 - troubleshooting [302](#)
- deployment jobs [30, 32, 33, 35, 37](#)
 - Commit and Deploy Changes page [32](#)
 - committing changes [30](#)
 - discarding changes [30](#)
 - managing [33](#)
 - status [37](#)
 - viewing history [35](#)
 - when changes become active [37](#)
- Deployment Manager [30, 32, 33, 35, 37](#)
 - Commit and Deploy Changes page [32](#)
 - committing changes [30](#)
 - discarding changes [30](#)
 - managing jobs [33](#)
 - viewing change history [35](#)
 - when changes become active [37](#)
- destination object groups [142](#)
 - reference [142](#)
- devices [36, 37, 81, 84, 87, 89, 91, 93, 94, 95, 97, 98, 99, 104, 106](#)
 - actions requiring delete, reimport [87](#)
 - adding HA to inventory [94](#)
 - adding to inventory [89, 91, 93](#)
 - changing management IP [98](#)
 - configuring policies [104](#)
 - converting to full management [97](#)

devices (*continued*)

- deleting from inventory [99](#)
- deployment status [37](#)
- managing [81](#)
- managing CX [81](#)
- object name conflicts [91](#)
- policy and setting overview [106](#)
- refreshing certificate [98](#)
- restrictions [89](#)
- troubleshooting discovery [99](#)
- troubleshooting import and discovery [95](#)
- understanding discovery [84](#)
- updating credentials [97](#)
- viewing inventory [89](#)
- viewing licenses [97](#)
- out-of-band changes [36](#)

diagnostics file [383, 384](#)

- creating [383](#)
- logging properties [384](#)

directory [228, 230, 231, 233, 234, 370, 371](#)

- configuring realms [230](#)
- configuring SSO for CSM [370](#)
- configuring SSO realms [371](#)
- deleting [234](#)
- overview [228](#)
- properties [231](#)
- search base [233](#)

directory realm [228, 230, 234, 370, 371](#)

- configuring [230](#)
- configuring SSO [371](#)
- configuring SSO for CSM [370](#)
- deleting [234](#)
- overview [228](#)

directory realms [368](#)

- configuring global for user management [368](#)

discovery [84, 85, 95](#)

- ASA [85](#)
- CX [84](#)
- troubleshooting [95](#)
- understanding [84](#)

disk [389](#)

- reclaiming space [389](#)

disk space (PRSM VM) [400](#)

- managing [400](#)

documentation overview [3](#)

Dynamic NAT [344, 348](#)

E

edit [318](#)

- interface [318](#)

end user notifications [259, 261, 263, 264, 265](#)

- customizing [263](#)
- editing notification page [263](#)
- importing notification page [264](#)
- overview [259](#)
- reference [261](#)
- variables [265](#)
- when sent [259](#)

Enforce EUI-64 [331, 339](#)

EtherChannel [314, 315, 325](#)

- about [314](#)
- load balancing [315](#)
- properties [325](#)

EUI-64 [331, 339](#)

Event Viewer [183, 187, 188, 189, 190, 191, 196, 201, 214](#)

- filter rules [189](#)
- filtering events [188, 190](#)
- message reference [196, 201, 214](#)
 - columns [214](#)
 - Context-Aware Security traffic events [196](#)
 - CX, PRSM system events [201](#)
 - overview [196](#)
- overview [183](#)
- working with events [191](#)
- views [187, 188](#)
 - configuring custom [187](#)
 - deleting custom [187](#)
 - switching between real time and historical [188](#)
 - using [187](#)

events [183, 187, 188, 189, 190, 191, 196, 201, 214, 400](#)

- filter rules [189](#)
- filtering [188](#)
- filtering performance [190](#)
- managing PRSM storage space [400](#)
- reference [196, 201, 214](#)
 - columns [214](#)
 - Context-Aware Security traffic events [196](#)
 - CX, PRSM system events [201](#)
 - overview [196](#)
- viewing [183](#)
- views [187](#)
- working with individual [191](#)

F

failover [44, 307, 308](#)

- about [307](#)
- configuring [44, 308](#)
- devices [308](#)
- managing [308](#)

feature licenses [71, 72, 74, 75, 76, 78](#)

- applying licenses [76](#)

feature licenses (*continued*)

- deleting [78](#)
- overview [71](#)
- renewing licenses [76](#)
- revoking licenses [78](#)
- uploading licenses [75](#)
- assigning licenses [76](#)
- implications of expiration [72](#)
- using evaluation [74](#)

file filtering profile objects [144](#)

- reference [144](#)

file transfers [51](#)

- controlling [51](#)

filters [188, 189, 190](#)

- configuring event [188, 190](#)
- event rules [189](#)

Hheader-injection profile objects [149](#)

- reference [149](#)

health and performance monitoring [174](#)help, getting [28](#)high availability [44, 307, 308](#)

- about [307](#)
- configuring [44, 308](#)
 - devices [308](#)
- managing [308](#)

HTTP proxy [376](#)HTTPS [83, 283, 285, 286, 287, 288, 289, 291, 293, 294, 295, 297, 300, 302, 373, 374](#)

- decryption (ASA CX) [283, 285, 286, 287, 288, 289, 291, 293, 294, 295, 297, 300, 302](#)
 - bypassing [300](#)
 - configuration overview [288](#)
 - configuring decryption certificate [291](#)
 - configuring policies [295](#)
 - configuring settings [289](#)
 - configuring supplemental trusted certificates [294](#)
 - converting certificate formats [293](#)
 - decrypted traffic flow [286](#)
 - decryption policy properties [297](#)
 - do not decrypt traffic flow [287](#)
 - downloading, installing the CA certificate [293](#)
 - managing traffic flows [283](#)
 - overview [283](#)
 - purpose [285](#)
 - tips, limitations [288](#)
 - troubleshooting [302](#)
- installing server certificate [373](#)
- obtaining server certificate [374](#)
- preparing ASA devices for management [83](#)

icons, policy and alert [26](#)Identity NAT [344](#)identity objects [56, 132, 151](#)

- ASA reference [151](#)
- controlling access by user group [56](#)
- CX, reference [132](#)

identity policies [235, 236, 240, 241, 242](#)

- configuring [235](#)
- enabling active authentication [240](#)
- enabling transparent authentication [241](#)
- properties [236](#)
- transparent authentication requirements [242](#)

identity services (ASA CX) [53, 56](#)

- configuring passive authentication [53](#)
- controlling access by user group [56](#)

identity services (CX) [225, 226, 227, 228, 230, 231, 233, 234, 235, 236, 240, 241, 242, 243, 246](#)

- configuring [227](#)
- configuring authentication settings [246](#)
- configuring directory realms [230](#)
- configuring identity policies [235](#)
- deleting directories [234](#)
- deleting directory realms [234](#)
- directory properties [231](#)
- directory realm overview [228](#)
- directory search base [233](#)
- enabling active authentication [240](#)
- enabling transparent authentication [241](#)
- enabling transparent authentication (Firefox) [243](#)
- enabling transparent authentication (Internet Explorer) [243](#)
- identity policy properties [236](#)
- identity types [226](#)
- managing [225](#)
- overview [225](#)
- supported servers and methods [226](#)
- transparent authentication requirements [242](#)
- what to tell users [227](#)

integrated Windows authentication [241](#)interface [314, 315, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 335, 339](#)

- add/edit [318](#)
- bridge group [332](#)
 - properties [332](#)
- enable [319, 323, 326, 330](#)
- EtherChannel [314, 315, 325](#)
 - about [314](#)
 - load balancing [315](#)
 - properties [325](#)
- EUI-64 [331, 339](#)
- ID [320](#)
- link-local address [331, 339](#)

interface (*continued*)

- MAC address [321, 324, 328, 331](#)
 - active [321, 324, 328, 331](#)
 - standby [321, 324, 328, 331](#)
 - management [320](#)
 - MTU [320, 324, 327, 330](#)
 - name [319, 322, 325, 329](#)
 - physical [318](#)
 - properties [318](#)
 - properties [335, 339](#)
 - IPv4 [335](#)
 - IPv6 [339](#)
 - redundant interface [328](#)
 - properties [328](#)
 - security level [320, 323, 326, 330](#)
 - subinterface [322](#)
 - properties [322](#)
- interface role objects [150](#)
- reference [150](#)
- interfaces [313, 317](#)
- configuring [317](#)
 - managing [317](#)
 - understanding [313](#)
- inventory [36, 81, 84, 87, 89, 91, 93, 94, 95, 97, 98, 99](#)
- actions requiring delete, re-import [87](#)
 - adding devices [89, 91, 93](#)
 - adding HA devices [94](#)
 - converting device to full management [97](#)
 - deleting from inventory [99](#)
 - device restrictions [89](#)
 - managing CX [81](#)
 - object name conflicts [91](#)
 - out-of-band changes [36](#)
 - refreshing device certificate [98](#)
 - troubleshooting discovery [99](#)
 - troubleshooting import and discovery [95](#)
 - understanding discovery [84](#)
 - updating device credentials [97](#)
 - viewing [89](#)
 - viewing licenses [97](#)
- IPS [66, 180, 276, 277, 278](#)
- configuring filtering [276](#)
 - configuring settings [277](#)
 - filtering [276](#)
 - NG Intrusion Prevention dashboard [180](#)
 - scanning for threats [66](#)
 - viewing threats [278](#)
- IPS, Next Generation [279, 281](#)
- configuring updates [279](#)
 - troubleshooting updates [281](#)
- IPv4 [335](#)
- interface properties [335](#)
- IPv6 [339](#)
- interface properties [339](#)

K

- Kerberos authentication [241](#)
- Known Users CX identity object [132](#)

L

- language, changing web interface [21](#)
- LDAP server [231, 233](#)
 - properties (CX) [231](#)
 - search base [233](#)
- licenses [71, 72, 73, 74, 75, 76, 77, 78, 97](#)
 - 3DES/AES K9 [77](#)
 - applying [76](#)
 - CX feature [71, 72](#)
 - implications of expiration [72](#)
 - licenses page [73](#)
 - managing CX and PRSM [71](#)
 - PRSM [72](#)
 - overview [72](#)
 - revoking [78](#)
 - uploading [75](#)
 - using evaluation [74](#)
 - viewing assignments [97](#)
 - assigning [76](#)
 - CX feature [71, 72](#)
 - overview [71](#)
 - deleting [78](#)
 - renewing [76](#)
- link-local address [331, 339](#)
- local policies [104, 108, 109, 110, 111, 112, 113](#)
 - analyzing assignments [113](#)
 - changing sharing status [110](#)
 - configuring device [104](#)
 - configuring policy sets [108](#)
 - configuring rule-based [109](#)
 - deleting policy sets [113](#)
 - editing rule-based [112](#)
 - enabling, disabling [112](#)
 - making exceptions in shared policies [111](#)
 - moving rule-based [109](#)
- logging [193](#)
 - configuring for ASA [193](#)
- logging configuration (ASA) [194](#)
 - device settings [194](#)
- logging configuration (CX, PRSM) [383, 384](#)
 - downloading diagnostics file [383](#)
 - properties [384](#)
 - setting log levels [383](#)

M

MAC address [321, 324, 328, 331](#)
 interface [321, 324, 328, 331](#)
 active [321, 324, 328, 331](#)
 standby [321, 324, 328, 331](#)
 malware protection [274, 275](#)
 configuring settings [275](#)
 configuring web reputation filtering [274](#)
 management interface [320](#)
 menus, web interface [24](#)
 monitor-only mode, configuring [16](#)
 MTU [320, 324, 327, 330](#)

N

Name [319, 322, 325, 329](#)
 interface [319, 322, 325, 329](#)
 NAT [343, 344, 347, 348, 351](#)
 Bidirectional [344](#)
 Dynamic [344, 348](#)
 Identity [344](#)
 Object [344, 347, 351](#)
 properties [351](#)
 overview [343](#)
 Policy Dynamic [344](#)
 rules [347](#)
 managing [347](#)
 Static [344, 348](#)
 Twice [344, 347, 348](#)
 properties [348](#)
 network [173, 176](#)
 overview dashboard [173](#)
 responding to alerts [176](#)
 Network Address Translation [343](#)
 see NAT [343](#)
 network group objects [123, 125, 126](#)
 CX groups reference [123](#)
 groups reference [125](#)
 object reference [126](#)
 overview [123](#)
 network participation [375](#)
 Next Generation IPS [71, 279, 281](#)
 configuring updates [279](#)
 license [71](#)
 troubleshooting updates [281](#)
 NG IPS profile objects [66, 148](#)
 reference [148](#)
 scanning for threats [66](#)
 NTLM authentication [241](#)

O

Object NAT [344, 347, 351](#)
 properties [351](#)
 Object PAT [344](#)
 objects (policy) [91, 115, 116, 118, 119, 120, 121, 122, 123, 125, 126, 127, 129, 132, 134, 137, 138, 139, 140, 142, 143, 144, 146, 148, 149, 150, 151, 152](#)
 configuring [118](#)
 customizing per device [119](#)
 deleting [121](#)
 descriptions [116](#)
 importing [120](#)
 managing [115](#)
 name conflicts [91](#)
 overview [115](#)
 reference [121, 122, 123, 125, 126, 127, 129, 132, 134, 137, 138, 139, 140, 142, 143, 144, 146, 148, 149, 150, 151, 152](#)
 application objects [138](#)
 application service objects [140](#)
 ASA identity objects [151](#)
 common properties [122](#)
 CX identity objects [132](#)
 CX network groups [123](#)
 destination object groups [142](#)
 file filtering profile objects [144](#)
 header-injection profile objects [149](#)
 interface roles [150](#)
 network [126](#)
 network groups [125](#)
 network overview [123](#)
 NG IPS profile objects [148](#)
 Secure Mobility objects [139](#)
 service groups [127](#)
 source object groups [143](#)
 TCP/UDP port keywords [129](#)
 time range [152](#)
 URL objects [134](#)
 user agent objects [137](#)
 web reputation profile objects [146](#)
 out-of-band changes [36](#)
 dealing with [36](#)

P

packets [378](#)
 capturing [378](#)
 PAT [343, 344, 348, 351](#)
 Dynamic [344, 348](#)
 Object [351](#)
 properties [351](#)
 overview [343](#)
 Static [344, 348](#)

- physical interface [318](#)
 - properties [318](#)
- policies [26](#), [30](#), [72](#), [103](#), [104](#), [106](#), [109](#), [110](#), [111](#), [112](#), [113](#)
 - abandoning changes [30](#)
 - analyzing assignments [113](#)
 - committing changes [30](#)
 - concepts [103](#)
 - configuring device [104](#)
 - configuring rule-based [109](#)
 - deleting [113](#)
 - descriptions [106](#)
 - editing rule-based [112](#)
 - enabling, disabling [112](#)
 - icons [26](#)
 - license implications [72](#)
 - making exceptions in shared policies [111](#)
 - moving rule-based [109](#)
 - sharing [110](#)
- policing traffic [258](#)
- Policy NAT [344](#)
- policy objects [91](#), [115](#), [116](#), [118](#), [119](#), [120](#), [121](#), [122](#), [123](#), [125](#), [126](#), [127](#), [129](#), [132](#), [134](#), [137](#), [138](#), [139](#), [140](#), [142](#), [143](#), [144](#), [146](#), [148](#), [149](#), [150](#), [151](#), [152](#)
 - configuring [118](#)
 - customizing per device [119](#)
 - deleting [121](#)
 - descriptions [116](#)
 - importing [120](#)
 - managing [115](#)
 - name conflicts [91](#)
 - overview [115](#)
 - reference [121](#), [122](#), [123](#), [125](#), [126](#), [127](#), [129](#), [132](#), [134](#), [137](#), [138](#), [139](#), [140](#), [142](#), [143](#), [144](#), [146](#), [148](#), [149](#), [150](#), [151](#), [152](#)
 - application objects [138](#)
 - application service objects [140](#)
 - ASA identity objects [151](#)
 - common properties [122](#)
 - CX identity objects [132](#)
 - CX network groups [123](#)
 - destination object groups [142](#)
 - file filtering profile objects [144](#)
 - header-injection profile objects [149](#)
 - interface roles [150](#)
 - network [126](#)
 - network groups [125](#)
 - network overview [123](#)
 - NG IPS profile objects [148](#)
 - Secure Mobility objects [139](#)
 - service groups [127](#)
 - source object groups [143](#)
 - TCP/UDP port keywords [129](#)
 - time range [152](#)
 - URL objects [134](#)
 - user agent objects [137](#)
- policy objects (*continued*)
 - reference (*continued*)
 - web reputation profile objects [146](#)
- policy sets [72](#), [104](#), [108](#), [113](#)
 - configuring [108](#)
 - copying [108](#)
 - deleting [113](#)
 - license implications [72](#)
 - universal [104](#)
- Port Address Translation [343](#)
 - see PAT [343](#)
- ports [414](#)
 - open management [414](#)
- processes (system) [381](#)
 - managing [381](#)
- PRSM [1](#), [3](#), [5](#), [21](#), [22](#), [23](#), [30](#), [71](#), [72](#), [74](#), [75](#), [76](#), [78](#), [98](#), [363](#), [377](#), [385](#), [387](#), [388](#), [389](#), [390](#), [391](#), [393](#), [394](#), [395](#), [400](#), [402](#), [405](#), [406](#), [414](#)
 - backing up database [385](#)
 - backing up VM [388](#)
 - changing management IP [98](#)
 - checking connectivity [377](#)
 - committing changes [30](#)
 - discarding changes [30](#)
 - features [5](#)
 - getting started [21](#)
 - installation [393](#), [394](#), [395](#)
 - overview [394](#)
 - overview of packages [393](#)
 - preparing server [394](#)
 - virtual machine [395](#)
 - installing upgrades [402](#), [405](#), [406](#)
 - CLI [402](#)
 - overview [402](#)
 - troubleshooting [406](#)
 - uploading packages [405](#)
 - web interface [405](#)
- introduction [1](#)
- licenses [72](#), [74](#), [75](#), [76](#), [78](#)
 - applying [76](#)
 - revoking [78](#)
 - uploading [75](#)
 - assigning [76](#)
 - overview [72](#)
 - renewing [76](#)
 - using evaluation [74](#)
- logging in [22](#), [23](#)
 - CLI console [23](#)
 - overview [22](#)
 - web interface [22](#)
- maintaining [363](#)
- managing disk space [400](#)
- managing licenses [71](#)
- open management ports [414](#)
- overview [1](#), [3](#)

PRSM (*continued*)

- pruning database [389](#)
- resetting admin password [390](#)
- resetting to factory defaults [391](#)
- restoring database [385](#)
- restoring VM [388](#)
- scheduling database backups [387](#)
- troubleshooting [363](#)

R

- rate limits, applying [258](#)
- recovery user account [390](#)
- redundant interface [328](#)
 - properties [328](#)
- remote access VPN [67](#)
 - monitoring and controlling clients [67](#)
- reports [157, 162, 169, 171, 172, 400](#)
 - columns [169](#)
 - creating [171](#)
 - data collection and quality [162](#)
 - generating [171](#)
 - managing PRSM storage space [400](#)
 - overview [157](#)
 - properties [171](#)
 - types [172](#)
 - viewing [157](#)
- reputation [179, 272](#)
 - dashboard, malware traffic [179](#)
 - looking up [272](#)
- reputation (web) profile objects [146](#)
 - reference [146](#)
- restarting system processes [381](#)
- restore [385, 388](#)
 - database [385](#)
 - PRSM virtual machine [388](#)
- route tracking [317](#)
- routing [316, 317](#)
 - static routes [316](#)
 - tracking with SLAs [317](#)

S

- Safe Search [259](#)
 - enforcing [259](#)
- Secure Mobility objects [67, 139](#)
 - monitoring and controlling VPN clients [67](#)
 - reference [139](#)
- security level [320, 323, 326, 330](#)
 - interface [320, 323, 326, 330](#)

- server requirements [394](#)
 - PRSM installation [394](#)
- service group objects [127, 129](#)
 - reference [127](#)
 - TCP/UDP port keywords [129](#)
- shared policies [104, 108, 109, 110, 111, 112, 113](#)
 - analyzing assignments [113](#)
 - changing sharing status [110](#)
 - configuring device [104](#)
 - configuring policy sets [108](#)
 - configuring rule-based [109](#)
 - deleting policy sets [113](#)
 - editing rule-based [112](#)
 - enabling, disabling [112](#)
 - making exceptions [111](#)
 - moving rule-based [109](#)
- single sign-on [370, 371](#)
 - Cisco Security Manager [370](#)
 - generic [371](#)
- SLA [317](#)
 - route tracking [317](#)
- snapshots [388](#)
 - PRSM virtual machine [388](#)
- software installation [393, 402, 405, 406](#)
 - overview of packages [393](#)
 - upgrades [402, 405, 406](#)
 - CLI [402](#)
 - overview [402](#)
 - troubleshooting [406](#)
 - uploading packages [405](#)
 - web interface [405](#)
- source object groups [143](#)
 - reference [143](#)
- SSL [83, 98, 283, 285, 286, 287, 288, 289, 291, 293, 294, 295, 297, 300, 302, 373, 374](#)
 - decryption (ASA CX) [283, 285, 286, 287, 288, 289, 291, 293, 294, 295, 297, 300, 302](#)
 - bypassing [300](#)
 - configuration overview [288](#)
 - configuring decryption certificate [291](#)
 - configuring policies [295](#)
 - configuring settings [289](#)
 - configuring supplemental trusted certificates [294](#)
 - converting certificate formats [293](#)
 - decrypted traffic flow [286](#)
 - decryption policy properties [297](#)
 - do not decrypt traffic flow [287](#)
 - downloading, installing the CA certificate [293](#)
 - managing traffic flows [283](#)
 - overview [283](#)
 - purpose [285](#)
 - tips, limitations [288](#)
 - troubleshooting [302](#)
 - installing server certificate [373](#)

SSL (*continued*)

- obtaining server certificate [374](#)
- preparing ASA devices for management [83](#)
- refreshing device certificates [98](#)
- standby MAC address [321, 324, 328, 331](#)
- Static NAT [344, 348](#)
- static route [316](#)
 - about [316](#)
- status [37](#)
 - deployment jobs and devices [37](#)
- storage space [400](#)
 - managing PRSM [400](#)
- subinterface [322](#)
 - properties [322](#)
- support, technical [383](#)
 - creating diagnostic file [383](#)
- syslog [192, 193, 195](#)
 - configuring [192](#)
 - configuring for ASA [193](#)
 - configuring for CX [192](#)
 - properties for ASA [195](#)
 - settings (CX) [193](#)
- system events (CX, PRSM) [201](#)

T

- telemetry, sending to Cisco [375](#)
- threats [66, 179](#)
 - malware traffic dashboard [179](#)
 - scanning [66](#)
- time range [166](#)
 - changing dashboard [166](#)
- time range objects [152](#)
 - reference [152](#)
- TLS [283, 285, 286, 287, 288, 289, 291, 293, 294, 295, 297, 300, 302, 373, 374](#)
 - decryption (ASA CX) [283, 285, 286, 287, 288, 289, 291, 293, 294, 295, 297, 300, 302](#)
 - bypassing [300](#)
 - configuration overview [288](#)
 - configuring decryption certificate [291](#)
 - configuring policies [295](#)
 - configuring settings [289](#)
 - configuring supplemental trusted certificates [294](#)
 - converting certificate formats [293](#)
 - decrypted traffic flow [286](#)
 - decryption policy properties [297](#)
 - do not decrypt traffic flow [287](#)
 - downloading, installing the CA certificate [293](#)
 - managing traffic flows [283](#)
 - overview [283](#)
 - purpose [285](#)

TLS (*continued*)

- decryption (ASA CX) (*continued*)
 - tips, limitations [288](#)
 - troubleshooting [302](#)
- installing server certificate [373](#)
- obtaining server certificate [374](#)
- traffic events (CX) [196](#)
- transparent authentication [241, 242, 243](#)
 - enabling [241](#)
 - enabling in Firefox [243](#)
 - enabling in Internet Explorer [243](#)
 - requirements [242](#)
- transparent mode [41](#)
 - configuring for ASA CX [41](#)
- troubleshooting [18, 30, 37, 95, 99, 176, 281, 300, 302, 377, 381, 383, 384, 391](#)
 - checking system [377](#)
 - configuring logging properties [384](#)
 - creating diagnostics file [383](#)
 - deployment status [37](#)
 - discovery [99](#)
 - import and discovery [95](#)
 - managing system processes [381](#)
 - PRSM traffic redirection [18](#)
 - resetting system to factory defaults [391](#)
 - responding to alerts [176](#)
 - signature and engine updates [281](#)
 - TLS/SSL decryption [302](#)
 - unknown CA or bad certificate errors [300](#)
 - web interface problems [30](#)
 - when configuration changes become active [37](#)
- trusted certificates [294, 373, 374](#)
 - configuring supplemental [294](#)
 - installing server [373](#)
 - obtaining server [374](#)
- Twice NAT [344, 347, 348](#)
 - properties [348](#)

U

- undoing changes [30](#)
- Unknown Users CX identity object [132](#)
- Updater Connection events [281](#)
- updates [279, 281](#)
 - configuring signature and engine [279](#)
 - troubleshooting signature and engine [281](#)
- Upgrade Manager [393, 402, 404, 405, 406](#)
 - installing upgrades [405](#)
 - overview [404](#)
 - overview of packages [393](#)
 - system upgrades [402](#)
 - troubleshooting [406](#)

Upgrade Manager *(continued)*

uploading packages 405

upgrade packages 393, 402, 405, 406

installation overview 402

installing from CLI 402

installing from web interface 405

overview 393

troubleshooting 406

uploading 405

URL filtering 59, 63, 134, 266, 267, 271, 272, 273, 274, 279, 281

acceptable use policies 59

category descriptions 272

configuring URL objects 134

configuring web reputation filtering 274

controlling URL access 271

determining URL Category 272

filtering by web reputation 63, 273

overview 266

compared to application filtering 267

configuring updates 279

troubleshooting updates 281

URL objects 59, 134

acceptable use policies 59

reference 134

use cases 41, 44, 46, 51, 53, 56, 59, 63, 66, 67

acceptable use policies (URL filtering) 59

configuring passive authentication 53

controlling access by user group 56

controlling application use 51

controlling Secure Mobility devices 67

filtering by web reputation 63

gaining insight into traffic 46

overview 41

scanning for IPS threats 66

transparent mode 41

configuring high availability 44

user account 24

effect on web interface 24

user agent objects 137

reference 137

user groups 56

controlling access by user group 56

user identity 246

configuring authentication settings 246

users 29, 363, 364, 367, 368, 369, 370, 371, 372, 373

admin 367

changing password 372

configuring 368

configuring global directory realm 368

configuring SSO 371

configuring SSO for CSM 370

conflicts when editing policies 29

users *(continued)*

deleting 373

managing 363

page reference 363

properties 369

roles and privileges 364

V

views 187, 188, 189, 190, 191

configuring custom 187

deleting custom 187

filter rules 189

filtering events 188, 190

switching between real time and historical 188

using event 187

working with individual 191

virtual machine (VM) 395, 400

installing PRSM 395

managing disk space 400

W

web interface 21, 24, 25, 26, 27, 28, 29, 30

about PRSM 29

basics 24

changing languages 21

getting help 28

icons 26

lists and tables 25

menus 24

mousing over items 26

selecting items 27

troubleshooting 30

user conflicts 29

user role affect on 24

web reputation 63, 179, 272, 273, 274, 275

configuring filtering 274

configuring malware protection settings 275

dashboard, malware traffic 179

filtering by 63, 273

looking up 272

scores 273

web reputation profile objects 63, 146

filtering by web reputation 63

reference 146

Web Security Essentials 71

license 71