User Guide for ASA CX and Cisco Prime Security Manager 9.1

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-28138-02
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 ACOMPANYING 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)

© 2011-2013 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface xiii

Audience xiii
Related Documentation xiii
Conventions xiii
Obtaining Documentation and Submitting a Service Request xv

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 19

CHAPTER 3 Getting Started 21

Browser Requirements 21
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Into the System</td>
<td>22</td>
</tr>
<tr>
<td>Logging Into the Web Interface</td>
<td>22</td>
</tr>
<tr>
<td>Logging Into the ASA CX CLI</td>
<td>23</td>
</tr>
<tr>
<td>Logging Into the PRSM CLI</td>
<td>23</td>
</tr>
<tr>
<td>Web Interface Basics</td>
<td>24</td>
</tr>
<tr>
<td>Your User Role Controls What You Can See and Do</td>
<td>24</td>
</tr>
<tr>
<td>Menus</td>
<td>24</td>
</tr>
<tr>
<td>Lists and Tables</td>
<td>26</td>
</tr>
<tr>
<td>Policy, List, and Alert Icons</td>
<td>26</td>
</tr>
<tr>
<td>Select or Mouse Over List Items to See Commands</td>
<td>27</td>
</tr>
<tr>
<td>Selecting Items</td>
<td>27</td>
</tr>
<tr>
<td>Getting Help</td>
<td>30</td>
</tr>
<tr>
<td>Viewing Basic System Information</td>
<td>30</td>
</tr>
<tr>
<td>Troubleshooting Web Interface Problems</td>
<td>30</td>
</tr>
<tr>
<td>Committing or Discarding Changes</td>
<td>31</td>
</tr>
<tr>
<td>The Commit and Deploy Changes Page</td>
<td>33</td>
</tr>
<tr>
<td>Managing Deployment Jobs</td>
<td>34</td>
</tr>
<tr>
<td>Viewing Change History</td>
<td>35</td>
</tr>
<tr>
<td>When Do Configuration Changes Become Active?</td>
<td>36</td>
</tr>
<tr>
<td>Deployment Job and Device Status</td>
<td>37</td>
</tr>
<tr>
<td>Use Cases for ASA CX</td>
<td>39</td>
</tr>
<tr>
<td>How to Set Up ASA CX in Transparent Mode</td>
<td>39</td>
</tr>
<tr>
<td>Managing High Availability</td>
<td>42</td>
</tr>
<tr>
<td>How to Gain Insight Into Your Network Traffic</td>
<td>43</td>
</tr>
<tr>
<td>How to Control Application Usage</td>
<td>50</td>
</tr>
<tr>
<td>How to Use Passive Authentication</td>
<td>51</td>
</tr>
<tr>
<td>How to Create Access Policies that Apply to AD/LDAP User Groups</td>
<td>54</td>
</tr>
<tr>
<td>How to Implement an Acceptable Use Policy (URL Filtering)</td>
<td>58</td>
</tr>
<tr>
<td>How to Block Malware Using Web Reputation</td>
<td>60</td>
</tr>
<tr>
<td>How to Monitor and Control AnyConnect Secure Mobility Devices</td>
<td>62</td>
</tr>
<tr>
<td>Managing System Licenses</td>
<td>65</td>
</tr>
<tr>
<td>CX Feature and PRSM Licenses</td>
<td>65</td>
</tr>
<tr>
<td>Feature Licenses</td>
<td>65</td>
</tr>
</tbody>
</table>
Controlling the Data Displayed in Dashboards 149
Dashboard Columns 151
Creating Reports 153
  Generating Reports 153
  Report Properties 153
  Report Types 153
Dashboard Reference 154
  Network Overview 155
  Malicious Traffic Dashboard 157
    Malware Types Dashboard 158
    Users with Malicious Transactions Dashboard 159
    Web Categories with Malicious Transactions Dashboard 159
    Web Destinations with Malicious Transactions Dashboard 160
    Applications With Malicious Transactions Dashboard 161
  Users Dashboard 162
  Web Destinations Dashboard 164
  Web Categories Dashboard 165
  Policy Hits Dashboard 166
  User Devices Dashboard 168
  Applications Dashboard 169
  Application Types Dashboard 170
  Devices Dashboard 172
  Interface Dashboard 174

CHAPTER 10

Viewing Events 177
Overview of Event Viewer 177
Using Event Views 181
  Configuring Custom Views 181
  Switching Between Real Time and Historical Views 182
Filtering Events 182
  Event Filter Rules 183
Working with Individual Events 184
Event Messages 185
  Context-Aware Security Traffic Events 186
  CX Device and PRSM System Events 190
PART III

Configuring Context-Aware Security 207

CHAPTER 11

Managing Authentication and Identity Services 209

Overview of Authentication and Identity Services 209

Supported AAA Servers and Authentication Methods 210
Types of User Identity 210
What to Tell Users About Authentication 211
Configuring Authentication and Identity Services 211

Overview of Directory Realms 212
Configuring Directory Realms 213
Directory Properties 215
Deleting Directory Realms or Directories 217
Configuring Identity Policies 218
Identity Policy Properties 220
Enabling Active Authentication 222
Enabling Transparent User Authentication 224

Requirements for Transparent Authentication 225
Configuring Internet Explorer for Transparent Authentication 225
Configuring Firefox for Transparent Authentication 226
Identifying the Active Directory Agent 227
Configuring Authentication Settings 228

CHAPTER 12

Controlling Network Access with Context-Aware Access Policies 231

Overview of Context-Aware Access Policies 231
Default Context-Aware Access Policy Behavior 232
Configuring Context-Aware Access Policies 232
Context-Aware Access Policy Properties 234
Notifying Users of Blocking Policies 237
When Are Notifications Sent? 238
End User Notifications Page 239
Editing End User Notifications 240
End User Notification Variables 241
URL and Application Filtering 242
APPENDIX A

System Maintenance and Troubleshooting 295

Managing Users 295
  Overview of the Users Page 295
  User Roles and Privileges 296
Using the Pre-Defined Admin User 298
Configuring the Directory Realm for Remote Users 299
Configuring Users 299
  User Properties 300
  Configuring SSO Directories and Users 301
Changing Your Password 302
Deleting Users 303
Installing a Server Certificate 303
  Obtaining a Server Certificate 304
Basic Troubleshooting 306
  Checking System Connectivity 306
  Capturing Packets 307
  Managing System Processes 310
Creating a Diagnostics File for the Cisco Technical Assistance Center 312
  Logging Configuration Properties (CX, PRSM) 313

Maintaining the System 314
  Backing Up and Restoring the Database 314
  Scheduling Database Backups 316
  Backing Up and Restoring the PRSM VM 317
  Resetting the Admin Password 318
  Resetting to Factory Defaults 319

APPENDIX B

Installing Software 321

Image and Software Packages 321
Cisco Prime Security Manager Installation 322
  Preparing the Server for PRSM Installation 322
  Installing the PRSM Virtual Machine 323
Managing PRSM Disk Space 327
Upgrading the System 329
  Installing System Upgrades from the CLI 330
Preface

The preface contains the following topics.

- Audience, page xiii
- Related Documentation, page xiii
- Conventions, page xiii
- Obtaining Documentation and Submitting a Service Request, page xv

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
- Navigating the Cisco ASA 5500 Series Documentation

Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Commands, keywords, buttons, field names, and user-entered text appear in <strong>bold</strong> font. For menu-based commands, the full path to the command is shown.</td>
</tr>
<tr>
<td>Menu &gt; Menu Item</td>
<td></td>
</tr>
</tbody>
</table>
## Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>variable</code></td>
<td>Variables, for which you supply values, are in <em>italic</em> font. Italic font is also used for document titles and for general emphasis.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>`{x</td>
<td>y</td>
</tr>
<tr>
<td>`[x</td>
<td>y</td>
</tr>
<tr>
<td><code>courier font</code></td>
<td>Terminal sessions and information that the system displays appear in <em>courier font</em>.</td>
</tr>
<tr>
<td><code>&lt; &gt;</code></td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td><code>!, #</code></td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

### 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.
Obtaining Documentation and Submitting a Service Request


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.
CHAPTER 1

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 websites 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.
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.

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:

- 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.
• 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, and web reputation. 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 templates of shared policies (called device groups) 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:
  • 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:

Initial ASA CX Setup


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 337.

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.

- Multiple security context configurations.

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.
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
```

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...
Done.
Generating self-signed certificate, the web server will be restarted after that
```

Preparing CX Devices

Setting Up the ASA CX Software
Done.
Press ENTER to continue...

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.
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 43.

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.

```bash
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 Device > 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.

Before You Begin

If you already have device groups with the policy configured, and you intend to add the device to one of these groups, simply assign the device to the group. When you commit changes, the traffic redirection policy defined for the group will be applied to the device. You can assign the device to a group from the Device Groups page.

This procedure assumes that you need to enable and configure redirection in the device group that contains the device you are configuring.

Procedure

Step 1

Do one of the following to open the device group that contains the device whose traffic redirection policy you want to configure:

- When you add the device to the inventory, if the device does not have an active redirection policy, you are notified of the fact and you can click the link to go to the device group that was created for the device during discovery.
- If the device is already in the inventory, select Policies > Device Groups, then select the device group that contains the device.

If the traffic redirection settings section contains a message stating that the settings are not managed by PRSM, it means that one or more device in this group has a traffic redirection policy that was configured outside of PRSM using features that PRSM does not support. The device with the unmanaged redirection policy might have been removed from the group, but the group's redirection policy is permanently disabled. You must use the ASA CLI or ASDM to configure or change the redirection policy.

Step 2

Configure the following properties in the Traffic Redirection Settings group:

- Select Traffic Redirection: Enable.
- In 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.
- In Interfaces, leave the field blank if you want traffic that passes through any interface on the device to be redirected. If you select a specific interface, an interface from each device in the group must be represented in the list of interfaces.

For example, consider the following three devices and their interfaces:

- ASA-1: inside, outside, DMZ
In this case, selecting “inside, DMZ” would not be allowed, because no interface on ASA-3 is included in the list. The fact that ASA-1 has two selected interfaces whereas ASA-2 has one is not material; it means that redirection would occur on two interfaces on ASA-1. To save the group, you would need to select at least one of the GE1, GE2, and GE3 interfaces, so that ASA-3 is represented.

**Step 3** Click **Save Device Group** to save your changes.

---

**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. Additionally, PRSM is not aware of changes that you make to the ASA configuration done through the CLI or 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 configuration. Instead, the traffic redirection policy for that device will be considered unmanaged. You will not be able to configure the traffic redirection policy for any device group that contains an ASA with an unmanaged traffic redirection 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.
Device group membership

A device group either has a managed or an unmanaged traffic redirection policy. If you add a device to the group that has an unmanaged redirection policy, the policy becomes unmanaged in the device group. Once the device group's redirection policy becomes unmanaged, it is always unmanaged, even if you remove all devices that have unmanaged policies. You are warned whenever you try to add a device with an unmanaged policy to a group with a managed policy.

Note
If you do decide to add a device with an unmanaged policy to a group that has a managed policy and there are other devices in the group, the policies on those devices also become unmanaged. You will have to use ASDM or the ASA CLI to make changes to the redirection settings on those devices. PRSM will not be aware of changes to the redirection policies on those devices.

Interface changes

When you add the device to the PRSM inventory, PRSM discovers the interfaces configured at that moment in time. If you add, remove, or rename interfaces, PRSM is not aware of them. Thus, if you explicitly specify interfaces in the redirection policy, PRSM will configure the policy only on those interfaces that existed at the time of discovery.

For example, assume that an interface named DMZ was not defined on ASA-5 when you added the device to PRSM. You then assigned ASA-5 to a device group whose redirection policy included DMZ as one of the interfaces. Later, you use ASDM to name an interface DMZ on ASA-5. At this point, it would appear that PRSM should configure redirection for the DMZ interface on ASA-5. However, because DMZ was not defined on the device at the time of discovery, PRSM is not aware that it exists on ASA-5.

To work around this problem, you must delete ASA-5 from the PRSM inventory, then add it again. This action will rediscover the ASA configuration and PRSM will now be aware of the DMZ interface. You can then add ASA-5 back to the device group and get the configuration you expect.

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 device's device group.
Getting Started

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

- Browser Requirements, page 21
- Logging Into the System, page 22
- Web Interface Basics, page 24
- Committing or Discarding Changes, page 31

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 Windows 7. In many cases, 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.

- Mozilla Firefox 11
  
  Note
  To use an IPv6 address, Firefox 11 is the minimum release you can use.

- Windows Internet Explorer 8 with Google Chrome Frame
  
  Note
  If you try to log into the web interface using Internet Explorer 8 without Google Chrome Frame, you are prompted to install the add-on. This is an easy way to get to the required application.

- Google Chrome 17
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 296.

**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.

- **Policies**—The Policies menu includes the core features for defining security policies. From this menu, you can create policies, policy objects, and device groups. You can also view the applications that the Application Visibility and Control engine can identify.

- **Device**—The Device menu includes features related to the device configuration. In Multiple Device mode, this is also where you will find the device inventory, where you add devices and configure other device-specific features.

- **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:
  
  - **Welcome**—To open the 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.
- Event Viewer has unique filtering features, which are described in Filtering Events, on page 182.
- 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. Mousing over the icon opens a tool tip that provides details about the icon; these details can change depending on the context.

The following illustration shows the basic icons that you should become familiar with.

Figure 4: Policy (and Alert) Icons

The icons are:

- 1, 2, 3—Which licensed features are available for the policy set. Normally, the icons are black. A red background indicates a problem with the license that is required for the feature; mouse over the icon to see a description of the problem. The icons represent the following features:
  - 1—Application filtering is enabled for the policy set.
• 2—**URL filtering** is enabled for the policy set.

• 3—**Web reputation filtering** is enabled for the policy set.

• 4—**Alert**. The red-! triangle is a general alert icon, which indicates that there is some type of problem. In policy lists, it indicates a licensing problem. In dashboards or the PRSM device inventory, it indicates device problems, such as device unreachable, and the specific alert also appears as text next to the icon. In policy lists, mouse over the icon to determine the reason for the alert.

• 5—**Pending Changes**. The Pending Changes icon should be the most frequent one you see. It indicates that this item has been modified. You must commit changes before the edited version of the policy, object, or other setting becomes effective.

• 6—**Packet Capture**. The icon indicates that packet capture is turned on for this policy.

**Select or Mouse Over List Items to See Commands**

Commands that operate on items in a list are revealed only when you mouse over the item. 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 mousing-over items to see if commands appear on the item.

In the following example, mousing over the first access policy shows several commands related to the policy, such as **Delete Policy** and **Edit Policy**. In this image, the commands related to policy 2 are hidden; there are also hidden commands for the policy set that you would see if you moused over the "Access" header row.

**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 5: Item Picker with Object and Object Type Lists**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Object list.</td>
</tr>
<tr>
<td>2</td>
<td>Object type filter.</td>
</tr>
</tbody>
</table>

If you select an item type, the item list is filtered to show objects of that type only. For example, if you select Identity Object from the filter list for the Source field, you see identity 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.

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). Select the item from the list and press Enter to add it to the item picker box.

**Figure 6: Filter as you type**

Tip

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. The details open to the right of the entry form.

If you select multiple items in an item picker, the items are separated by spaces, as shown in the following illustration. You can mouse over the item to show a details pane to the right. From the details pane, you can
click **Edit Object** to edit the object contents from this form (the button is **View Object** for predefined system objects).

*Figure 7: Mouse over selected items to view details*

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.

If you make an invalid entry, the problem entry is highlighted and an **Errors** link appears beside the field. Click the link to see more information about the error; click **Hide Errors** to close the message.

*Figure 8: Item Selection Errors*

If the item you want is not in the list, and you are allowed to create items, click the **Create New Object** or **Create New Profile** link beneath the field. The required form opens to the right of the list. Fill in the object properties and click **Save Object**.
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

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.

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.

You cannot find a command mentioned in the documentation.

The role assigned to your user account controls what you can see and do in the web interface. However, if your role should allow a command that does not appear in the web interface, the problem might be your display resolution or zoom level in the browser. For menus, the web interface does not allow horizontal scrolling, and if a command does not fit in the display, it is truncated with no indication that anything is missing. Try using your browser’s “zoom out” command one or more times to see if that resolves the 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 Device > 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 Device > 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.

![Changes Pending](image)

### Note  
The link includes the number of pending changes. 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.

**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.

<table>
<thead>
<tr>
<th>Commit and Deploy Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Commit and Deploy Changes" /></td>
</tr>
</tbody>
</table>

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, for this job or for previous jobs, a section lists the devices that require your attention. You can try redeploying changes to these devices by selecting which devices to include in the redeployment job (using the Redeploy/Do Not Redeploy toggle) and clicking the Redeploy button.

---

**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 (number)**—This link name indicates that you have outstanding changes that need to be committed. The number of uncommitted changes is shown.

- **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.

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, first change the Redeploy/Do Not Redeploy toggle for each device to indicate which devices should be included in the redeployment job, then click the Redeploy button.

Before doing a redeployment, you might check the Change History page to see if there is a persistent problem with a device, for example, several failed deployment jobs. If the status for the device in the change history log indicates the device was unavailable, check the network connection between the PRSM server and the device.

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 (number)**—This link name indicates that you have outstanding changes that need to be committed. The number of uncommitted changes is shown.
- **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. You can try redeploying changes to these devices by selecting which devices to include in the redeployment job (using the **Redeploy/Do Not Redeploy** toggle) and clicking the **Redeploy** button.

---

**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. For each device, select whether to redeploy or not redeploy, then click the **Redeploy** button to start another attempt to deploy the same version.

---

**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. Changing the password is not allowed after importing the device. To resolve the problem, either change the password back to the original password, or delete the device from the inventory and add it back.

  • 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.

• **NotAllowed**—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 39
- Managing High Availability, page 42
- How to Gain Insight Into Your Network Traffic, page 43
- How to Control Application Usage, page 50
- How to Use Passive Authentication, page 51
- How to Create Access Policies that Apply to AD/LDAP User Groups, page 54
- How to Implement an Acceptable Use Policy (URL Filtering), page 58
- How to Block Malware Using Web Reputation, page 60
- How to Monitor and Control AnyConnect Secure Mobility Devices, page 62

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 9: Transparent Firewall Network**

![Diagram of a transparent firewall network](image)

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/en/US/docs/security/asa/asa84/configuration/guide/mode_fw.html](http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/mode_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
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# bridge-group 1

ciscoasa(config-if)# int g0/1
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 BVII

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 g0/1
!
interface GigabitEthernet0/1
nameif outside
bridge-group 1
security-level 0

ciscoasa(config-if)# sh run BVII
!
interface BVII
ip address 10.1.1.2 255.255.255.0
```

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.

### Managing 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 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.

Please note the following ASA CX failover caveats:

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

You can use Cisco Prime Security Manager (PRSM) to manage and monitor pairs of ASA CX devices operating in Active/Standby failover mode. Follow these steps to ensure a device pair is configured correctly for failover, and available for monitoring in PRSM:

**Procedure**

#### Step 1
Use the Adaptive Security Device Manager (ASDM) or the command-line interface (CLI) to configure the pair of ASA CX devices for Active/Standby failover, ensuring HTTP Replication is enabled.


**Important**
During failover configuration be sure to enable HTTP Replication. 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.

To enable HTTP Replication on the active device using ASDM, navigate to the **Configuration > Device Management > Failover > Setup** tab, check the **Enable HTTP Replication** box, and then click **Apply**.

To enable HTTP Replication on the active device using the CLI, enter the `failover replication http` command in global configuration mode.

#### Step 2
One at a time, discover the pair with PRSM:

Start with the primary device. When you add the primary unit to the inventory, it will fail because the CX services are restarted. Wait for the services to come back up, and then use ASDM or the CLI to manually make the unit active again.

Add the secondary device to the PRSM inventory.

For information about discovering devices in PRSM, see **Understanding Device Discovery and Managing the Device Inventory**.

#### Step 3
To ensure configuration and policy synchronization, make both devices members of the same PRSM device group.

You can either create a new device group and assign the Active/Standby pair to it, or you can simply assign the secondary device to the primary device group. See **Assigning Devices to Device Groups** for more information.

---

**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 additional policies to provide more data:

- You need an identity policy to get user-based information in the dashboards.
- You need a decryption policy to gain insight into TLS/SSL (for example, HTTPS) traffic.

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 **Policies > Policies**.
b) Mouse over the access policy set and click **Add New Policy**.
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.

![Policy Configuration Example]

**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.

- **a)** Select **Device > Directory Realm**.
- **b)** Select **I Want To > Add Realm**.
- **c)** 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 213. 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.
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**.

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 215. 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.
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.

![Completed Realm](image)

h) Select **Policies > Policies**.

i) Do one of the following to configure the identity policy:

   - If an identity policy was automatically created when you added the realm, mouse over the policy and click **Edit Policy**.
   - Otherwise, mouse over the identity policy set and click **Add New Policy**.

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 220.

The following illustration shows the action settings when configuring active authentication with a negotiated authentication method.
k) Click Save Policy.

Step 4  (Optional) To gain insight into HTTPS and other TLS/SSL traffic, you might want to enable decryption and define a decryption policy.

By decrypting HTTPS traffic, you can gain insight into web destination, web category, and web reputation. If your decryption policy decision is to decrypt the traffic flow (after the initial analysis of the flow), you also gain insight into application and application type.

Note  Proceed with caution when configuring decryption. Many sites, including most Financial sites, will not work with decryption. Thus, you might want to initially create a policy that decrypts low reputation traffic only, and gradually add more decryption policies as you gain experience with the product.

a) Select Device > Decryption.

b) Select Enable Decryption Policies: On.

c) For Certificate Initialization Method, select whether to generate a new CA certificate or to import one you already have.

This step is more complex than it looks, because you need to have a good understanding of decryption and certificate requirements. Before configuring the certificate, read Configuring the Decryption Certificate, on page 274.

d) Click Save.

e) Select Policies > Policies.

f) Mouse over the decryption policy set and select Add New Policy.

g) Ensure that the policy has a meaningful name, adjust the source and destination if you do not want the policy to apply to all sources and destinations.

If you want to ensure no traffic is actually decrypted, you can configure a URL object that specifies example.com as the destination. Because example.com is a reserved name, it should never apply to an actual destination server. Because traffic must be initially decrypted to determine whether the destination is matched, you will still collect valuable data from HTTPS traffic flows.

h) Initially, you might want to select Decrypt Potentially Malicious Traffic to limit decryption to low-reputation traffic.

Thus, even if a destination does not work with decryption, you are isolating access problems to low reputation sites that you probably do not want users accessing anyway. When you select this option, you also need to select a web reputation profile, which defines which reputation values are considered low.

Initially, select the predefined Default Reputation Profile object, as shown in the following illustration.
i) Click **Save Policy**.

**Step 5**
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 6**
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 lets 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 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 or types.

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 Policies > Policies.

Step 2 Mouse over the access policy set and click Add New Policy. Alternatively, mouse over the policy above which you want to place the policy and click Add Above.

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 or application type, 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**

<table>
<thead>
<tr>
<th>Passive Authentication</th>
<th>Active Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 AD Agent, which sends the mapping to the ASA CX. Supports AD only.</td>
<td>Supports basic authentication for LDAP and AD, and also NTLM and Kerberos for AD. Authentication occurs when the user attempts an HTTP connection only.</td>
</tr>
<tr>
<td>Best-effort user identification, not real authentication.</td>
<td>Real authentication.</td>
</tr>
<tr>
<td>Useful for applications and clients that do not support active authentication.</td>
<td>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.</td>
</tr>
<tr>
<td>Completely transparent to the user</td>
<td>NTLM and Kerberos are usually transparent, while basic authentication shows a popup to the user to obtain username and password.</td>
</tr>
<tr>
<td>The AD agent is required. AD 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.</td>
<td>No agent is required.</td>
</tr>
</tbody>
</table>

ASA CX uses the Cisco 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 AD 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**

- The AD agent software is separate from ASA CX. Download the AD agent application using this URL, or search for it on Cisco.com:
  
  http://www.cisco.com/cisco/software/release.html?
  
  mdfid=281191384&flowid=4378&softwareid=280775065
  
  &release=AD_Agent&rellifecycle=&relind=AVAILABLE&reltype=all


- Configuring an 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 according to the procedures explained in http://www.cisco.com/en/US/docs/security/ibf/setup_guide/ibf10_install.html.
When you come to the client configuration, configure the ASA CX as the client (first, cd to IDF/CLI):

```bash
adacfg client create-n ASA-CX-nickname-ip ASA-CX_mgmt_IP-secret RADIUS_secret
```

where

• *ASA-CX-nickname* is a name used by the AD agent to refer to the ASA CX client.

• *ASA-CX_mgmt_IP* is either the IP address of the ASA CX management interface, or the subnet that contains the address, for example, 10.100.10.1 or 10.100.10.0/24.

• *RADIUS_secret* is a RADIUS shared secret that you will also configure in ASA CX. This secret encrypts and protects communications between ASA CX and the AD agent.

Tips:
You might find the following AD agent commands useful for verifying or troubleshooting the configuration:

• *adacfg dc list*, to verify the connection between the AD agent and AD server.

• *adacfg cache list*, to verify that the agent is getting user-to-IP mappings.

• *adacfg client list*, to list the clients currently served by the AD agent.

Step 2
In PRSM (Single Device mode or Multiple Device mode), identify the AD agent:

a) Select *Device > AD Agent*.
b) Enter the DNS host name or IP address of the AD agent.
c) For *Password*, enter the RADIUS shared secret.
d) Click *Save*.

Step 3
If you have not created an AD realm, create a directory realm to identify the AD servers from which the AD agent is collecting login information:

a) Select *Device > 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 213

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 215.

**Step 4** Select Policies > Policies and create or edit the identity policy for the realm to provide the desired service.

To use the passive mappings obtained from 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 220.

**Step 5** 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 6** Click the Changes Pending link in the menu bar to open the Uncommitted Changes page.

**Step 7** 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 **Policies > Policies**.

**Step 2** Create a policy that blocks all access to the partner site.

a) Mouse over the access policy set and click **Add New Policy**.

Alternatively, mouse over the policy above which you want to place the policy and click **Add Above**.

b) Enter a name for the policy.

c) Select **Policy Action: Deny**.

d) Keep **Any** as the traffic source.

e) Click the **Create New Object** link beneath the **Destination** field to create a URL object that identifies the partner site.

The Create Object form opens to the right of the policy properties.

f) Enter a name for the object, for example, Partner A Site.

g) Select **URL Object** for **Object Type**.

h) 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.

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

a) Mouse over the deny policy you just created and click Add Above.
b) Enter a name for the policy.
c) Keep Policy Action: Allow.
d) Click the Create New Object link beneath the Source field to create an identity object that identifies the user group.
e) Enter a name for the object, for example, Partner A Contract Team.
f) Select Identity 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.
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select Policies &gt; Policies.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Mouse over the access policy set and click Add New Policy. Alternatively, mouse over the policy above which you want to place the policy and click Add Above.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter a name for the policy, for example, Block Bad Sites.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Policy Action: Deny.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Keep Any as the traffic source.</td>
</tr>
</tbody>
</table>
| Step 6 | Create the URL object that will define the destinations that users are not allowed to access:  
   a) Click the Create New Object link beneath the Destination field to create a URL object that identifies the objectionable categories and sites.  
      The Create Object form opens to the right of the policy properties.  
   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. |
h) Click **Save Object** to save the object and add it to the destination field.

**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.

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

To look up the reputation of a site, you can use the tool at http://www.senderbase.org/home.

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.

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** Select Policies > Policies.
**Step 2** Add the web reputation profile to the desired access policies.
   a) Mouse over the “Allow” access policy that you want to modify and click Edit Policy.
   b) In the Profile section, select Default Reputation Profile in the Web Reputation field.

   If you want to define a different low reputation range, click the Create New Profile link and create your own web reputation 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.

**Step 3**
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) Mouse over the decryption policy that you want to modify and click **Edit Policy**.
b) In the Action section, change the action to **Decrypt Potentially Malicious Traffic**.
c) Select **Default Reputation Profile** or another profile of your choosing in the **Web Reputation** field.

d) Click **Save Policy**.

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

**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.
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—
- AnyConnect Secure Mobility user guides for various client types—

**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:


**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 Policies > Policies.

b) Mouse over the access policy set and select Add New Policy.

Alternatively, find the policy above which you want to insert the new policy, mouse over it and click Add Above.

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, 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.
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.
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 65
- What Happens When a Feature License Expires, page 66
- Overview of the Licenses Page, page 67
- Configuring System Licenses, page 68

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.

- 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.

Note
If you allow a subscription-based license to expire, and you have policies that specify objects that require the license, your policies will continue to function, but you will not be able to edit the policies that use the objects until you upload a new license.

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.

What Happens When a Feature License Expires
The subscription licenses used by CX devices have expiration dates. You must ensure that you have the valid unexpired licenses required by the features that you are using. 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.

The following points provide more detail about subscription license expiration:

- Policy sets include icons for each feature enabled for the set. Mouse over the icons to see the feature names and the days left on the license, or whether the license is expired and past the expiration date.

In PRSM Multiple Device mode, the license expiration dates are derived from the devices in the device groups that use the policy set. If more than one device group uses a policy set, the expiration date is the nearest one of the licenses assigned devices in the various groups. Thus, expiration processing is controlled by the device with the shortest-life license, not your longest-life license.

- If the license has expired and is beyond the grace period, you cannot edit any policy that uses a feature controlled by the license, or create a new policy that uses the feature. For example, if the Application Visibility and Control license expires, you cannot edit any access policy that specifies an application, application type, application object, or application-service object. You can, however, delete these policies. Policies that require an expired license are indicated with warning icons.
Policies that use an expired license continue to work. 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.

- If the license has expired but it is still within the grace period, you can edit existing policies that use the license, but you cannot create new policies that require the license.

- When operating in PRSM Multiple Device mode, if you find yourself in a situation where policies are locked because a policy set is assigned to a device group that contains at least one device with an expired license, the easiest resolution is to apply a new license. If that is not possible, consider the following temporary options:

  - If the problem is an entire device group, that is, all devices in the group have expired licenses, make a copy of the policy set and assign the copy to the device group with the expired licenses. This will allow you to edit the policies in the original policy set. Then, when you apply a valid license to the device group, you can reassign it the original policy set, and the devices in the device group will pick up changes to the policies.

  - If the problem is a single device within a device group, remove the device from the group until you can apply a valid license. When you edit the device group containing a device with an expired license, you are asked if you want to make a copy of the group that will contain devices with unexpired licenses only. The policy sets are moved to the new group with the devices that have active licenses, and the devices with expired license are isolated in the old group. To edit device groups, select Policies > Device Groups.

  - If you do not have any license for a feature, or if you disable the feature globally in Single Device mode or for every device group in Multiple Device mode, signature updates for that feature do not occur. For example, if you do not have an Application Visibility and Control license, the system does not update application signatures. If you do not have a Web Security Essentials license, web categories are not updated, and category-based filtering uses the last-downloaded categorizations.

  - There is no need to delete licenses. When a license expires, it is automatically removed from the system. In Multiple Device mode, all devices assigned to the license must first be assigned to other licenses before the expired license is removed.

### 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:

- **Apply Licenses**—(Multiple Device mode only.) To apply unused licenses to devices that need licenses.
- **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.
- **Manage Licensed Features**—(Single Device mode only.) To selectively enable or disable licensed features. If you decide you do not want to use a particular feature that requires a subscription license, you can disable the feature so that you cannot inadvertently define policies that require the license.

In Multiple Device mode, you manage licensed features for each device group. Select **Policies > Device Groups** to edit the groups.

List of Licenses

Shows each license available on the system. Each license also contains a list of devices that are using the license.

(Multiple Device mode only.) To see the commands related to a license or device, mouse over the license header or the device row. The following are the available commands:

- **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.
- **Revoke License**—(Device command.) To remove the license from this device. Before you can revoke a license, you must move the device to a device group that does not use the license. That is, the device group that contains the device cannot use policy sets that contain policies that use the feature 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.

### Selectively Enabling Licensed Features

By default, all features that require subscription licenses are enabled globally. You can selectively disable a feature if you want to prevent its use, even if you have a current license that would allow you to use the feature.

**Tip**

You cannot disable a feature if you are already using that feature in a policy. For example, if you have configured an access policy to use an application object (even if the policy is disabled), you cannot disable the Application Services feature. Policy objects can exist, and you can create new ones, but the objects cannot be used in a policy.

You can control the use of the following features:

- **Application Services**—Requires an Application Visibility and Control license. The feature controls the use of applications, application types, application objects, or application service objects and the Applications field in access policies.

- **URL Filtering**—Requires the Web Security Essentials license. The feature controls the use of URL objects.

- **Web Reputation**—Requires the Web Security Essentials license. The feature controls the use of web reputation profile objects.

**Caution**

If you disable a feature for a device group in Multiple Device mode, the feature is disabled in each policy set used by the device group. If another device group is using the same policy set, you are effectively disabling the feature for the other device group. Thus, changing the enable status of a feature can affect more than just the device group you are editing. Before disabling a feature, carefully examine whether other device groups will be affected.

How you enable or disable features differs based on the operational mode:
• Single Device mode—You manage features from the Licensing page.
  1. Select Administration > Licenses.
  2. Select I want to > Manage Licensed Features.
  3. Select the desired setting, Enable or Disable, for each feature.
  4. Click Save Settings.

• Multiple Device mode—You manage features for each device group.
  1. Select Policies > Device Groups.
  2. Select the device group.
  3. In the Manage Licensed Features section, select the desired setting, Enable or Disable, for each feature.
  4. Click Save Device Group. If you enable a feature, and devices in the group do not have the license required for the feature, you are prompted to apply licenses. If necessary, you can upload new licenses.
  5. You should also revoke licenses for disabled features for all devices in the group. Make a note of the effected devices and commit your changes. Then select Administration > Licenses, mouse over each device within the assigned feature license and click Revoke License.

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.

There are two places to upload licenses:

• From the Administration > Licenses page. This is the preferred method and is the procedure described below.

• (Multiple Device mode only.) While assigning or renewing licenses. You can apply licenses from the Licenses page or while editing a device group.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Administration &gt; Licenses.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select I want to &gt; Upload License File.</td>
</tr>
<tr>
<td>Step 3</td>
<td>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:</td>
</tr>
</tbody>
</table>

• Single Device mode—The license is applied and activated immediately. You do not need to 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.
Managing System Licenses

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. In PRSM Multiple Device mode, you need to explicitly assign licenses to devices.

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.

There are two main methods for applying or renewing licenses:

- From the Administration > Licenses page. In Single Device mode, the act of uploading a license applies it, replacing the old license. In Multiple Device mode, after uploading licenses, you either apply licenses to devices that do not have them, or renew currently assigned licenses.

- From the Policies > Device Groups page in Multiple Device mode. If you edit a device group, you are prompted to apply or renew licenses in the following cases:
  - You added a device to the group and it needs a license for the features enabled in the group.
  - You edited a group that already had devices with no license or an expired license for enabled features.
  - You enable a previously disabled feature on the group and the devices in the group do not already have a license for the feature.

The following topics explain how to manage feature licenses in PRSM Multiple Device mode from the License page. The same license window is also used when prompting for licenses during device group edit.

Applying Licenses

(Multiple Device mode only.) The following procedure explains how to apply an unused feature license to devices that currently have no license or whose license has expired.

Repeat this procedure for each device group that contains unlicensed devices.
### Procedure

**Step 1** Select Administration > Licenses.

**Step 2** Select I want to > Apply Licenses.

The Apply Licenses window opens. For more information on the Apply Licenses window, see Apply or Renew License Window, on page 73.

**Step 3** Select the type of license you want to apply and the device group that contains the unlicensed or license-expired devices.

The list of device groups includes only those groups that have devices that need the selected type of license.

If there are not enough licenses, you are notified of the problem, and you see a list that shows the number of licenses required by device model. The number includes devices that do not have a license and devices whose license has expired.

You must upload a sufficient number of licenses to meet these requirements. You can drag files from your system into the **Upload License Files** box or click the box to open a file selector.

**Step 4** Click **Apply**.

The system automatically applies the licenses with the nearest expiration date to the devices that need them and you are shown a list of the licenses applied. Other devices in the group are not affected.

**Step 5** Click **OK** to complete the assignment.

### Renewing Licenses

(Multiple Device mode only.) The following procedure explains how to renew an expiring license by replacing it with new unused feature licenses. When you renew a license, you replace it on all devices in the selected device group that use the license.

You must repeat this procedure for each device group that contains devices that use the license.

**Procedure**

**Step 1** Select Administration > Licenses.

**Step 2** Mouse over the license you want to replace and select Renew License.

This opens the Renew License window, which shows the license type and device model. The Select a Device Group list includes all device groups that have devices using this license. The Select Available License Files list shows all unused licenses that are available to replace the license; if there are no available licenses, the list does not appear.

For more information on the Renew Licenses window, see Apply or Renew License Window, on page 73.

**Step 3** Select a device group.

**Step 4** Click each license you want to apply until you have selected a sufficient number of licenses.

Clicking a selected license deselects it.

The required number of licenses is all devices in the group that are using the license. If there are not enough licenses of the appropriate type and device model, you can drag files from your system into the box or click the box to open a file selector. You cannot continue until you have selected the required number of licenses.
Step 5  Click Renew.
The selected licenses replace the license you are "renewing" on the devices that used the license; devices in
the group that use different licenses are unchanged.

Apply or Renew License Window

Use the Apply or Renew Licenses popup window to assign feature licenses to devices that need them. If there
are enough licenses of the appropriate type, including device model, the system can automatically apply them.
However, when renewing licenses from the Licenses page, you need to select which licenses you want to use
to replace the selected license.

If you need to select or upload licenses, the window indicates the number of licenses that are required. You
must select a sufficient number of licenses to equal the number of required licenses or you cannot save your
changes.

• When applying a license, the required number lists devices that do not yet have a license and devices
whose license has expired. Licenses are not applied to other devices in the group.

• When renewing (replacing) a license, the required number is all devices in the group that are using the
license. The selected licenses replace the license you are "renewing" on the devices that used the license;
devices in the group that use different licenses are unchanged.

The Apply License and Renew Licenses windows are similar and include the following fields:

(Select a) License Type
When you apply licenses from the Administration > Licenses page, you must select the type of license
you are applying.
When renewing licenses, this field shows the license type and device model for the license you are
replacing.

(Select a) Device Group
When applying or renewing licenses from the Administration > Licenses page, select the device group
that contains the unlicensed or expired-license devices.
When applying or renewing licenses while editing a device group, this field simply displays the name
of the device group.

Select Available Licenses
When renewing a license from the Administration > Licenses page, select the licenses you want to
replace the license. The list shows unassigned licenses of the appropriate type and device model. Click
a license to select or deselect it; click multiple rows to select more than one license. You must select
enough licenses to equal the required number of licenses or you cannot save your changes.

License Files Needed
If there are not enough available license files of the appropriate type and device model, this list appears
and shows how many licenses are required. When applying licenses while editing a device group, there
can be separate lists for each type of license.
Upload License Files

If there are not enough licenses of the appropriate type and device model, you can drag files from your system into the box or click the box to open a file selector. You can cancel the upload while it is in progress but not after it is complete.

You must upload a sufficient number of licenses to equal the required number of licenses or you cannot save your changes.

Tip

You can upload any type of license and it is added to the system and available for use. However, the upload affects the required license count only if it is for the required license type and device model.

Apply or Renew button

Click this button to assign licenses to the devices that need them.

When applying licenses, or renewing licenses when editing a device group, the system assigns the licenses with the nearest expiration date first if there are more available licenses than needed.

When renewing licenses from the Licenses page, the licenses you selected are applied.

You are shown a confirmation page with the license assignments. Click OK to continue.

Navigation

These windows open when you do any of the following:

- Select Administration > Licenses, and then select I want to > Apply Licenses.
- Select Administration > Licenses, mouse over a license and click Renew License.
- When editing a device group on the Policies > Device Groups page, enable a feature, add a device, or have the group contain devices with expired licenses, and click Save Group.

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.

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.
PART I

The Basics

- Managing Devices, page 79
- Managing Policies, page 93
- Managing Policy Objects, page 107
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 79
- Preparing ASA Devices for Management, page 81
- Understanding Device Discovery, page 82
- Managing the Device Inventory, page 84
- Troubleshooting Device Communications, page 89

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 an ASA CX into managed mode, you add the ASA that contains the ASA CX SSP to the device inventory.

Upon successful device configuration discovery, the CX device is placed in managed mode.
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).

**Tip**

**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.
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. 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.

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. Each discovered device is initially assigned to its unique device group, which is created during the discovery process.

During discovery, if there are naming conflicts between a discovered object and one that already exists in the PRSM database, you are prompted to supply a suffix for the discovered objects. 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.

ASA Devices

Only those policies and settings that PRSM supports are discovered. 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 syslog server settings with both PRSM and Cisco Security Manager.

Discovered policies and settings are handled differently based on whether they are managed:

- Managed—If you change managed policies or settings and commit changes, the changes are deployed to the ASA. Managed policies and settings include the traffic redirection policy, syslog servers, and logging settings.

- Unmanaged—Unmanaged policies or settings are discovered but are not deployed back to the ASA. In other words, discovery is one-way: you bring in the configuration once, but from that point forward, PRSM is unaware of changes to the policies or settings. Discovered but unmanaged settings include the interface list, and network, network group, service, and service group objects. Although you cannot edit interfaces, you can edit the objects after discovery. However, if you need your edits to be reflected in the ASA configuration, you must use the ASA CLI or ASDM to repeat your changes.

CX Devices

All policies and policy objects are discovered, but discovery of other settings is either limited or not supported. The following list provides details on each non-policy setting:
• Directory realms—An Active Directory (AD) realm is imported only if no AD realm is defined yet in PRSM Multiple Device mode. 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. You must either remove the AD realm from the server or the device, or make their definitions the same. If you truly need different AD realms, then you cannot manage the device using this PRSM server; you will need a separate PRSM server.

  **Note** LDAP directory realms are imported; you are prompted to supply a suffix if there are any naming conflicts with realms already defined in the PRSM database.

• Decryption settings—Decryption policies must be enabled to define decryption policies. What happens during import differs based on whether decryption policies are enabled on the device and on PRSM Multiple Device mode:
  - If decryption is not enabled on the device, then the device import is allowed, and when you commit changes, the settings defined in PRSM Multiple Device mode, including the certificate, are deployed to the device.
  - If decryption is enabled on the device, but disabled in PRSM Multiple Device mode, then it will be enabled in PRSM Multiple Device mode and the device’s decryption policies and certificate will be imported.
  - If decryption is enabled on both the device and the server, then the certificate and certificate settings must be identical or you will be prevented from adding the device. You must log into the device and make the settings identical to those on PRSM Multiple Device mode, then try import again.

• 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 import. For example, if the imported 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 import the device until you add the licenses to the PRSM server.

• PRSM log settings—These are discovered and included in the device configuration. The PRSM Multiple Device mode log settings are not changed; the log settings are considered distinct.

• 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.

  **Note** If you are using PRSM Multiple Device mode to manage a CX device, do not change the password of the admin user on the CX device. Changing the password will prevent PRSM from communicating with the device. You will have to remove the device from the PRSM inventory and add it back to update PRSM with the new admin password.

• 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 you already customized a page in PRSM, the corresponding page is not imported. However, if PRSM has the default page, and the device you are discovering has a customized page, the customized page is imported and used for all managed devices.

• 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 importing the device, ensure that you are comfortable with how these settings will change.

  • AD agent
  • Authentication settings
  • Signature update settings (frequency and proxy settings)
  • Packet capture settings

Managing the Device Inventory

The device inventory is simply the list of devices that you are managing. You must ensure that the credentials for logging into each device are accurate, or PRSM cannot manage them.

Overview of the Device Inventory

You can view a list of the currently managed devices. From this list, you can add devices and perform other basic inventory management tasks.

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), description, the operational mode (routed or transparent), the management IP address, the device type and software version, the device serial number, the configuration commit version, and the device group to which the device belongs.

Tip

If there is a warning icon on the far right, 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. For more information on alerts, see Resolving DeviceAlerts, on page 145.

To view the device inventory, select Device > Devices.

The device inventory includes the following items:

• I want to—Contains the following commands:
  • Add New Device—To add a device to the inventory and to discover its configuration. To add an ASA CX SSP, you add the ASA device that contains it. See Adding ASA and ASA CX Devices, on page 85.

• List of devices—The devices that are currently in the inventory. An ASA CX SSP is considered a child of the ASA that contains it.

  To see the commands related to a device, mouse over the device row, including rows for component modules. The following are the available commands:
• **Delete Device**—To delete the device and the modules it contains. See [Deleting Devices](#) on page 89.

• **Refresh Certificate**—To update the SSL certificate associated with the device. The certificate is used for communication with the device. See [Refreshing Device Certificates](#) on page 87.

• **Device Configuration**—To view or change device configuration settings. See [Working with the Device Configuration](#) on page 88.

---

**Adding ASA and ASA CX Devices**

Before you can manage an ASA device or ASA CX SSP, you must add it to the device inventory.

When you add an ASA to the inventory, the configuration of the device is discovered as is the configuration of any ASA CX SSP contained in the device. You do not add an ASA CX SSP directly.

Devices must meet the following general requirements; for additional details, such as the required software versions, see [Cisco CX and Cisco Prime Security Manager Compatibility](http://www.cisco.com/en/US/docs/security/asacx/compatibility/cx_prsm_comp.html).

- **ASA device**—Single-context mode, routed or transparent mode. You must enable the HTTP server on the device (it is enabled by default).

- **ASA CX**—The device cannot be running in monitor-only mode.

**Before You Begin**

In PRSM Multiple Device mode, you must commit or discard any pending changes. If there is a Changes Pending link in the menu bar, click it and determine how to handle the changes listed.

**Procedure**

**Step 1** Select Device > Devices to open the inventory list.

**Step 2** Select I want to > Add New Device.

**Step 3** Fill in the following information to define the communication properties for the ASA device.

- **Hardware Type**—Displays the device type. You must add the ASA, you cannot directly add the ASA CX.

- **Device Name**—The name by which the device will appear in selectors in PRSM, typically the same as the device host name.

- **Description**—An optional description of the device.

- **IP Address**—The IP address of the management interface or another interface that allows access to the internal HTTP server.

- **Port**—The port number used for HTTPS access to the internal HTTP server. The default 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.
Note If you are not importing an ASA device, click the I do not have an ASA link. See the release notes on Cisco.com for information on devices you can import without importing the ASA.

Step 4 Click Discover to initiate device configuration discovery. The device is contacted using the supplied credentials. If contact is successful, you are presented with the certificate retrieved from the device.

Step 5 After viewing and verifying the certificate, click Accept. The device is analyzed for modules.

Step 6 If the ASA contains an ASA CX SSP, you are prompted for its communication properties. The properties are explained above. Keep the following in mind when filling in the properties for ASA CX:

- The admin username and password are required. The admin username is the only one allowed for device discovery.

  **Tip** Do not change the admin password on the device after adding it to the inventory, or communication with the device will fail. You will have to delete the device from the inventory and add it again to use the new password.

- Keep the port number 443.

- You cannot change the device name, but you can change the default description.

- 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.

- 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 7 Click Discover to initiate device configuration discovery. The device is contacted using the supplied credentials. If contact is successful, you are presented with the certificate retrieved from the device.

Step 8 After viewing and verifying the certificate, click Accept. The device running configurations are analyzed and brought into the application.

  **Tip** Be patient. Device discovery can take time, and the time required to complete the discovery increases with the size of the device’s configuration. When discovery completes, if there are naming conflicts between discovered items and equivalent items already defined in the database, you are asked how to handle them.

Step 9 If there are naming conflicts, decide how to handle them.

If an item in the discovered configuration has the same name as an item already in the database, if the content of the items is identical, the item in the database is used and replaces the discovered item. 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 items differ; for example, two network objects with the same name that include different addresses. All conflicts of this type are listed in the table of naming conflicts.

To resolve the conflicts and complete the device import, you must 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. If you change the suffix, click Preview to see the updated proposed names.
When you are satisfied with the suffix you select, click Rename. If you do not want to rename objects in this manner, click Cancel to abort the device import. You will have to rename the objects in the database or the device before you can import it without going through the rename step.

**Step 10**  
Click Commit to complete the import.  
You must commit changes to complete the import and put the ASA CX in managed mode.  
After commit, ASA CX SSP are added to the inventory and placed in managed mode.  
For ASA devices, any supported device configuration commands or policies are added to the database and are available for you to alter using PRSM Multiple Device mode. You should no longer make changes to the discovered parts of the configuration using any other tools or techniques.  
A unique device group is created for the ASA. You can move the device to another device group if you want to replace the imported policies with policies shared with other devices. You can also add other devices to the new device group.

**Step 11**  
If traffic redirection from the ASA to the ASA CX SSP is not currently turned on, you are notified of the situation. Click Go to Device Group to get to the redirection policy so that you can enable redirection.  
Click Close if you do not want to edit the redirection setting immediately. Clicking Close does not cancel the import; you are not required to change the redirection policy during device import.

---

### Refreshing Device Certificates

You might need to refresh the SSL certificate associated with a device when you generate a new certificate on the device 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 Device > Devices to open the inventory list.

**Step 2**  
Mouse over the device and click Refresh Certificate.

**Step 3**  
The certificate is retrieved from the device and presented to you. If the certificate looks right, click Accept to save it.

---

### 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.

**Working with the Device Configuration**

Device configuration settings are those settings not directly related to firewall policy, such as logging configuration and syslog server settings on ASA devices. You edit the device configuration through the device inventory page.

**Procedure**

1. **Step 1** Select Device > Devices to open the inventory list.
2. **Step 2** Mouse over the device and click Device Configuration. A panel opens that lists the various configuration settings. Related settings are grouped together in panels that you can open and close.

   To change any setting, click the setting name to open the page where you can make your changes. Click the Help link on the settings page for detailed information for a particular group of settings.

**Dealing with Out-of-Band Changes**

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.

Out-of-band changes are never recognized. The configuration of your device at the time you added it to the inventory is the baseline for the device’s configuration in PRSM. Thus:

- If you make a change to a managed setting, such as syslog servers, the change is not recognized and might be overwritten the next time you make changes to the settings in PRSM and then deploy changes.

- Changes to interfaces, including the addition, removal, or renaming of them, are not recognized. Thus, settings that include an interface name, such as traffic redirection or syslog servers, will not reflect your changes. For example, you cannot select an interface that was added after the device became managed. Even if you type in the interface name, PRSM does not know that it exists on the device, and will not deploy the configuration.

- Changes to network and service objects and groups are not recognized, nor are the addition or deletion of those objects. If you use an ASA object in an ASA CX policy, the content of the object at ASA discovery remains static. However, even if you delete the object from the ASA, the ASA CX policy is
unaffected and will function normally, because the ASA CX configuration is not tied to the currently running ASA configuration.

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 policies, policy sets, policy objects, directory realms, and licenses 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. However, the device group created when you added the device to the inventory is deleted unless you changed its name or added other devices to the group.

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.

Before You Begin

You must commit any pending changes before you can delete a device.

Procedure

| Step 1 | Select **Device > Devices** to open the inventory list. |
| Step 2 | Mouse over the device and click **Delete Device**. You are asked to confirm 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. Changing the password (or username) is not allowed. You must delete the device from the inventory and add it back to update the username or password.

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 94
- Overview of Policies, page 95
- Policy Basics, page 97
Policy Concepts

The following illustration and subsequent list explains the terminology used in PRSM policy management. You need to understand these concepts to effectively design firewall policies. Although these concepts apply in both Single Device mode and Multiple Device mode, some items are transparent in Single Device mode.

**Policy**—A single rule that defines some aspect of your firewall security policy. For example, deny access to gambling websites, or require users to authenticate. There are different types of policy that provide specific types of services, such as access policies, identity policies, and decryption policies on the CX device.

**Note** Not every setting in the device configuration is considered a policy. The word “policy” applies to firewall rules. Other settings, such as interface configuration, logging settings, and so forth, are considered device configuration settings. Although you can share policies among a group of devices when using PRSM Multiple Device mode, all device configuration settings are unique to each device and must be configured separately.

**Policy set**—An ordered list of policies. All policies are members of a policy set. In Single Device mode, there is a single policy set for each type of policy. In Multiple Device mode, you can create multiple policy sets to define different security policies, and use device groups to assign the policy sets to 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.

**Device group**—A container that maps policy sets to devices when using PRSM Multiple Device mode. In Single Device mode, there is a single device group that is transparent to you. In Multiple Device mode, device groups are the method you use to share the same security policies among a group of devices that fulfill the same role within your network. The policy sets, and the policy objects used in the policies within the set, are configured on all devices assigned to the group.
• Shared or local policy—When considered as a whole, the combination of policy sets, policies, and policy objects defines your security policy, which is either shared among devices through a device group in Multiple Device mode, or local to a single device when configuring a CX device in Single Device mode. Structurally, there is no difference between shared and local policies. In simple terms, any security policy you define in Multiple Device mode is a shared policy, even if you assign a single device only to the device group, and any policy you create when directly configuring a CX device is a local policy.

Overview of 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.

Policies are grouped into policy sets. A policy set governs a particular type of behavior, such as network access or user authentication requirements. Each policy set is a single unit that defines the policy for the selected behavior for all devices to which the set is applied. Policy sets 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.

Tip

All traffic flows are matched against every policy set applied to a device. However, if you deny access to a traffic flow, policies in other policy sets might not be applied. For example, if your identity policy set requires authentication, but your access policy denies a traffic flow, the user is not prompted to authenticate prior to being denied access.

To open the Policies page, where you can create, edit, delete, and manage policies and policy sets, select Policies > Policies.

The Policies page includes the following items:

• Filter—You can filter the view to help you locate policies. Type in one or more strings and click Filter to show only those policies that include one of the strings. The strings you enter can appear in the policy name or type for the policy to be considered a match. That is, a string does not have to match the start of the policy name.

To remove a filter, delete it from the box and click Filter.

• I want to—(Multiple Device mode only.) Contains the following commands:
  • Add CX Policy Set—To add a new policy set for CX policies. You are prompted for the policy set name, description, and policy type.

Note

When configuring a CX device in Single Device mode, the policy sets are pre-defined. You cannot add or remove them.

• List of policy sets and their policies—All policy sets and policies are presented in a single list, organized by policy set. Every policy is contained within a policy set.
Each policy set shows the policy set name, the device groups that use the policy set, the type of policy set, and the number of policies within the policy set.

The **Features Enabled** icons indicate which licensed features are enabled for the policy set for those types that use these features. Mouse over an icon to see the feature type. If the icon is red, it means that the license for the feature is reaching its expiration date or it has expired; you should look into renewing the license. Look for warning icons on individual policies within the set to see where the features are used. Mousing over a warning icon shows the state of the license, including days remaining before expiration and whether you are in the grace period.

You can have policy sets for the following types of policy:

- **Access (CX)**—Controls access to the network.
  
  Each access policy within the set shows the numbered order of the policy within the set, a summary of the source, destination, services, and applications that define the traffic matching criteria, and the action that will be applied (allow, conditional allow, or deny).

- **Identity (CX)**—Determines 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.
  
  Each identity policy within the set shows the numbered order of the policy within the set, a summary of the source, destination, and services that define the traffic matching criteria, and the action that will be applied (Do Not Require Authentication, Using AD Agent, Using AD Agent or Active Authentication, Active Authentication, or Conditional Active Authentication, which means you are requiring authentication but excluding certain user agents). The realm and authentication type is also shown.

- **Decryption (CX)**—Determines how to handle SSL/TLS decrypted traffic flows. Decrypting HTTPS traffic flows makes it possible to apply access policies based on the inspected content of the traffic flow, such as application, URL category, web reputation, and so forth.
  
  Each decryption policy within the set shows the numbered order of the policy within the set, a summary of the source, destination, and services that define the traffic matching criteria, and the action that will be applied (Decrypt Malicious, Always Decrypt for Inspection, or Do Not Decrypt).

---

**Note**

If a Pending Commit icon appears on the right, the policy has not yet been committed to the configuration database.

To see the commands related to a policy set or policy, mouse over the policy set header or the policy row. The following are the available commands:

- **Policy Set commands:**
  
  - **Add New Policy**—To add a new policy to the policy set. The policy is added to the top of the set as the first entry. After creating the policy, move it to the desired position before committing your changes. Alternatively, find the policy above which you want to insert the new policy, mouse over it and click Add Above.

  - **Edit Policy Set**—(Multiple Device mode only.) To edit the properties of the policy set. You cannot change the type of policies included in the set.

  - **Duplicate Policy Set**—(Multiple Device mode only.) To create a copy of the policy set.
• **Delete Policy Set**—(Multiple Device mode only.) To delete the policy set. To delete a policy set, it cannot be referenced by a device group.

• **Policy commands:**
  
  • **Object Name**—If the policy uses a policy object, you can click the name of the object to view the object contents. When viewing a user-defined object, you can click **Edit Object** to make changes.

  • **Hits**—If there is a hit count, click the link to see the detailed policy hits dashboard for the policy. The hit count is based on the time range currently selected in the dashboards. Mouse over the hit count to see the time range.

  • **Delete Policy**—To delete the policy. The policy remains in force on devices to which it has been applied until you commit changes.

  • **Edit Policy**—To edit the policy.

  • **Duplicate Policy**—To create a copy of the policy. You must change the policy name and also some attributes so that the policy content is no longer identical to any existing policy. The policy is added as the first policy in the same policy set; you cannot copy policies between policy sets.

  • **Add Above**—To create a new policy immediately above this policy.

  • **Move Up, Move Down**—To move the policy until it is in the desired position. The up and down commands move the policy a single row. You can also click and drag a policy to the desired location.

---

**Policy Basics**

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

**Configuring Policy Sets**

| Note | You can create policy sets in PRSM Multiple Device mode only. When configuring a CX device in Single Device mode, the policy sets are pre-defined and you cannot add, edit, or delete them. |

Use policy sets to define collections of policies that are to be applied to one or more device. The policy set itself contains no indication of whether it applies to a single device (a local security policy) or to many devices (a common, shared security policy).

**Procedure**

| Step 1 | Select Policies > Policies. The policies are organized in policy sets, and each policy set is a separate ordered list of policies. To see the commands related to a policy set, you must mouse-over the name of the policy set. To see the commands |
related to an individual policy, you must mouse-over the name of the policy. You can then select the desired command.

If you need to work with an existing policy, use the filter controls to help you locate the policy you want to change.

**Step 2** Do one of the following:

- To create a new policy set for CX devices, select **I want to > Add CX Policy Set**.
- To edit an existing policy set, mouse over the policy set name and click **Edit Policy Set**.
- To create a copy of a policy set, mouse over the policy set name and click **Duplicate Policy Set**.

**Step 3** Fill in the policy set properties:

- **Policy Set Name**—The name of the policy set. If you change this name, all device groups that reference the policy set are updated.
- **Policy Set Type**—The type of policies that will be included in this policy set. You cannot change this property after you create the policy set.
- **Description**—A description of the policy set.
- **Device Groups**—The device groups to which this policy set is assigned. Select all device groups that should use the policy set. Click in the field to open a drop down list that contains all of the currently selectable groups; you cannot select a group if it has already been assigned a policy set of this type. To change the policy set assigned to a group, you must edit the device group or remove the device group from the policy set it is currently using.
- **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** to save your changes.

---

**What to Do Next**

For new policy sets, add policies to the set. Assign the policy set to a device group (an existing one or create a new one), then commit changes to deploy the policies to the devices assigned to the group. You can assign device groups either through the policy set properties or through the device group properties.

**Configuring 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.

Policies are grouped into policy sets. A policy set governs a particular type of behavior, such as network access or user authentication requirements. Each policy set is a single unit that defines the policy for the selected behavior for all devices to which the set is applied. Policy sets 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.

**Procedure**

**Step 1** Select **Policies > Policies**.
The policies are organized in policy sets, and each policy set is a separate ordered list of policies. To see the commands related to a policy set, you must mouse-over the name of the policy set. To see the commands related to an individual policy, you must mouse-over the name of the policy. You can then select the desired command.

If you need to work with an existing policy, use the filter controls to help you locate the policy you want to change.

**Step 2** Do one of the following:

- To create a new policy at the top of the list, mouse over the policy set name and click **Add New Policy**.
- To insert a new policy into the list, mouse over the policy immediate below the desired location and click **Add Above**.
- To edit an existing policy, mouse over the policy name and click **Edit Policy**.
- To base a new policy on a similar existing policy, mouse over the policy name and click **Duplicate Policy**.

A form opens with the policy properties for the type of policy you are creating or editing. For detailed information about these properties, see the appropriate topic:

- **Context-Aware Access Policy Properties, on page 234**
- **Identity Policy Properties, on page 220**
- **Decryption Policy Properties, on page 280**

**Step 3** Click **Save Policy** to save your changes.
The name and content of the policy must be unique within the policy set to save it.

**Step 4** On the Policies page, if necessary, move the policy so that it is in priority order within the policy set.

Policies within a policy set 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.

You can drag and drop policies, or use the **Move Up, Move Down** links that appear when you mouse over a policy.
Deleting Policies or Policy Sets

**Note**
You can delete policy sets in PRSM Multiple Device mode only. When configuring a CX device in Single Device mode, the policy sets are pre-defined and you cannot delete them. However, you can delete policies.

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 editing it and selecting *Enable Policy: Off*. 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 group that references it. When you commit changes, the entire policy set is removed from the device.

**Before You Begin**
Before you can delete a policy set, you must remove it from any device group that references it.

**Procedure**

**Step 1**
Select Policies > Policies.

**Step 2**
Do any of the following:

- To delete a policy, mouse over the policy and select *Delete Policy*.
- To delete a policy set, mouse over the policy set name and select *Delete Policy Set*.

---

Managing Device Groups

**Note**
You can create device groups in PRSM Multiple Device mode only. When configuring a CX device in Single Device mode, device groups are not needed because you are configuring a single device only.

A **device group** is a template that applies selected policy sets to one or more devices. Typically, you would define a device group based on the purpose a device serves. For example, **Internet Edge** devices, which control the flow between the Internet and your internal networks.

In a device group, you select one policy set per policy type, and the devices to which you will apply these policies. The device group is the mechanism used for assigning shared policies to devices. Thus, you will need just enough device groups to create all of the combinations of policy sets that you need for your network.
You can assign a device to one, and only one, device group. Initially when you add a device to the inventory, a unique device group is created for the device. You can leave the device in this group, move it to another group, or even add other devices to the group.

To open the Device Groups page, where you can create, edit, delete, and view device groups, select Policies > Device Groups.

The Device Groups page includes the following items:

- **Device Group Carousel**—Existing device groups are shown in a carousel that you scroll left or right. Each device group bubble shows the group name and the number of devices assigned to the group. Click a device group to see its properties, which are loaded into the property fields below the carousel.

- **I want to**—Contains the following commands:
  - **Add New Device Group**—To add a new device group. The device group property fields are cleared if you were viewing an existing group.

### Device Group Properties

When you select a device group from the carousel, its properties are shown below the carousel. The device group properties are:

- **Device Group Name**
  The name of the device group.

- **Description**
  A description of the device group.

- **Devices**
  The devices that are assigned to the device group, if any.

  When entering multiple items, press Enter to accept each item and to allow you to select additional items; selecting an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press Enter. To remove an item already in the box, mouse over it and click the X to the right of the name, or click it, then press Delete to remove it, and click away to complete the removal. If your entry is not valid, it is colored yellow; click the Errors link next to the field for information on the problem that you must correct.

  If you hover over an item in the list, a View Device link appears that allows you to see the device properties, which can help you select the right device.

### Tip

If you select a device with a traffic redirection setting whose managed state differs from that of the device group, you will see a message explaining the consequences of adding that device to the group. Read the message carefully before you add the device.
Manage Licensed Features

These settings determine whether a feature that requires a special license is available for the group. If you disable a feature, you cannot assign policy sets that contain policies that use the feature. For example, if you disable application filtering, you cannot include application objects in any access policy. You cannot disable a feature if you have already assigned a policy set that uses the feature; remove the reference to the policy set first.

You can control the use of the following features:

• **Application Services**—Requires an Application Visibility and Control license. The feature controls the use of applications, application types, application objects, or application service objects and the Applications field in access policies.

• **URL Filtering**—(ASA CX only.) Requires the Web Security Essentials license. The feature controls the use of URL objects.

• **Web Reputation**—(ASA CX only.) Requires the Web Security Essentials license. The feature controls the use of web reputation profile objects.
Traffic Redirection Settings

These settings determine the type of traffic that is redirected from the ASA to the ASA CX SSP. If the traffic redirection settings section contains a message stating that the settings are not managed by PRSM, it means that one or more device in this group has a traffic redirection policy that was configured outside of PRSM using features that PRSM does not support. The device with the unmanaged redirection policy might have been removed from the group, but the group’s redirection policy is permanently disabled. You must use the ASA CLI or ASDM to configure or change the redirection policy.

For device groups that support traffic redirection configuration, you can configure the following settings:

- **Traffic Redirection: Enable/Disable**—Whether to configure traffic redirection on the devices in the group. If you select **Disable**, any existing traffic redirection policy is removed and no traffic will go through the ASA CX SSP.

- **TCP/UDP Ports**—The TCP or UDP ports whose traffic should be redirected. The default is Any, which applies not only to TCP/UDP ports, but will include traffic for all other protocols. If you enter an explicit port number, only the TCP/UDP traffic that goes through the port will be redirected. Enter the ports in protocol/port format, such as tcp/80 or udp/80. You can enter a range of ports using a hyphen, such as tcp/1-100, udp/1-100. Port numbers can be 1-65535.

- **Interfaces**—The interfaces whose traffic should be redirected. The default is All Interfaces, which will redirect traffic that goes through any active interface on the ASA. If there is more than one device in the group, the interfaces available in the drop-down list includes all interfaces on all devices. You can select any combination of interfaces, but you must select at least one interface for each device included in the group.

For example, consider the following three devices and their interfaces:

- ASA-1: inside, outside, DMZ
- ASA-2: inside, outside
- ASA-3: GE1, GE2, GE3

In this case, selecting "inside, DMZ" would not be allowed, because no interface on ASA-3 is included in the list. The fact that ASA-1 has two selected interfaces whereas ASA-2 has one is not material; it means that redirection would occur on two interfaces on ASA-1. To save the group, you would need to select at least one of the GE1, GE2, and GE3 interfaces, so that ASA-3 is represented.

Policy Sets

Each type of policy has a field that allows you to select a policy set. You can select a single policy set per policy type. If you do not want to implement a certain type of policy, you can leave the field for that policy type blank. In some cases, default behaviors for a particular policy set will apply if you do not assign a specific policy set.

Best practice is to select a policy set for each policy type, even if the policy set includes a simple policy that effectively applies no special services for that type of firewall behavior. This ensures that you know exactly what the device should be doing.

When you select a policy set, the number of policies contained in that policy set is shown.
**Save Device Group button**

Saves your changes to the device group properties.

**Delete Device Group button**

Deletes the device group whose properties you are currently viewing. When you delete a device group, any devices assigned to the group are unassigned. Make sure you reassign the devices to different groups.

**Configuring Device Groups**

You can create device groups so that you can assign a group of policy sets to devices that perform the same role in your network. For example, you can create a device group for Internet Edge firewalls, and apply the same group of policies to all devices that protect your internal networks from Internet traffic.

This procedure explains how to create new groups or edit existing groups.

**Procedure**

**Step 1** Select Policies > Device Groups.

**Step 2** Do one of the following:

- To create a new device group, select I want to > Add New Device Group. Selecting this option clears the device group properties if you were viewing an existing device group.

- To edit an existing device group, select it in the carousel so that the group’s properties appear in the property fields.

**Step 3** Edit the name and description. A name is required.

**Step 4** Select the devices to assign to the group in the Devices field.

A device must already be in the inventory to select it.

You also cannot select a device if it is already assigned to another device group. If you want to assign a device to a new group, you must first delete it from the Devices field of the old group and save your changes. The device will then be available for assigning to the new group.

**Note** If the managed state of the traffic redirection settings differs between the device group and the device, you will see a message explaining the ramifications of adding the device to the group. Read the message carefully before continuing. Mixing devices with managed and unmanaged traffic redirection settings in the same group will prevent you from using PRSM to configure these settings for all devices in the group.

**Step 5** If you want to control the use of licensed features, select Enable or Disable as appropriate for each feature in the Manage License Features group.

The features require the use of the Application Visibility and Control or Web Services Essentials licenses. If you do not want to purchase a type of license, you can disable the feature that requires it. Your settings control the types of policy set you can assign to the group. You cannot disable a feature if it is already being used by an assigned policy set. You must first unassign the policy set, or assign a different one, before you can save your changes.

**Step 6** If the traffic redirection settings are available, configure the settings to define which traffic should be redirected to the ASA CX SSP.
Read the following topics to get a better understanding of traffic redirection and its implications.

- Redirecting Traffic to ASA CX Using PRSM, on page 17
- Troubleshooting PRSM Traffic Redirection Policies, on page 19

**Step 7** Select the policy sets to assign to the device group.
You can select a single policy set per policy type. If you do not want to assign a particular policy type, you can leave that property empty.

**Step 8** Click **Save Device Group** to save your changes.
If any of the selected devices does not have the licenses required to support the features used in the group, you are prompted to apply the appropriate license to those devices. You are also prompted to renew licenses for any devices that have expired licenses. If necessary, you can upload new license files at this time.

---

**What to Do Next**
If you disabled a feature with the intention of permanently disabling it, but devices in the group were already configured with the license to support the feature, you should revoke the license from devices in the group to free the license for other devices. Make note of which devices are in the group, then select **Administration > Licenses**, mouse over each device and click **Revoke License**.

**Assigning Devices to Device Groups**

---

<table>
<thead>
<tr>
<th><strong>Note</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>You assign ASA devices to a device group; you do not assign ASA CX devices separately.</td>
</tr>
</tbody>
</table>

When you add a device to the inventory, a unique device group is created for the device. You can keep the device in this group, move the device to another group, or even add devices to the group.

---

<table>
<thead>
<tr>
<th><strong>Tip</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>If the managed state of the traffic redirection settings differs between the device group and the device, you will see a message explaining the ramifications of adding the device to the group. Read the message carefully before continuing. Mixing devices with managed and unmanaged traffic redirection settings in the same group will prevent you from using PRSM to configure these settings for all devices in the group.</td>
</tr>
</tbody>
</table>

---

**Procedure**

**Step 1** Select **Policies > Device Groups**.

**Step 2** If the device is already assigned to a group, first select that group from the carousel (to show the group properties on the page), then mouse over the device name in the **Devices** field in the group properties and click the X to remove the device. Click **Save Device Group** to save your changes.

**Step 3** Select the new group in the carousel, then click in the **Devices** field and select the device.

**Step 4** Click **Save Device Group** to save your changes.
If the selected device does not have all licenses required to support the features used in the group, you are prompted to apply the appropriate license to the device.
Deleting Device Groups

If you no longer need a device group, you can delete it.

When you delete a device group, any devices assigned to the group are unassigned. However, the policies configured on the device are not removed or changed until you assign the device to a new group. Ensure that all devices are assigned to device groups.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Policies &gt; Device Groups.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select the device group you want to delete in the device group carousel.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Ensure that the properties for the group you want to delete are displayed in the property fields, then click Delete Device Group.</td>
</tr>
</tbody>
</table>
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.

- Overview of Policy Objects, page 107
- Policy Object Reference, page 110

Overview of 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 action 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 action 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 Policies > Objects.

The Policy Objects page includes the following items:

- **Filter**—You can filter the view to help you locate policy objects using the following controls:
  - Use the drop-down arrow to filter the list based on object type; you can select multiple types. To remove a type, click the X in the object type name in the filter box. If you select one or more object types, any string you enter is matched against the selected types only.
  - Type in one or more string and click Filter. The strings you enter can appear anywhere within the object for the object to be considered a match. That is, a string does not have to match the start of the object name.

- **I want to**—This list includes the Add command for each type of object. The following is a brief description of each object type:
* CX Network Group—IP addresses to identify hosts and networks. You can use these objects on CX devices only.

* Service Group—Protocol and port definitions, such as TCP/80 for TCP traffic on port 80.

* 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, 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 names, application types, 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.

* Interface Role—A group of name patterns that identify interfaces on the device.

• 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).  

User Guide for ASA CX and Cisco Prime Security Manager 9.1
• **Edit Object**—To edit the object.

• **View Object**—(Pre-defined system objects only.) To view the object contents.

### 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. Any changes that you make are not deployed to the ASA; they affect the use of the objects for CX policies only.

---

### Procedure

**Step 1**

To open the form for creating or editing an object, do one of the following:

- To create an object directly, select **Policies > Objects**, then select **I want to > Add Object Type**.
- To edit an object directly, select **Policies > Objects**, then mouse over the object and click **Edit Object**.
- To create an object while editing a policy, select **Policies > Policies**, create or edit a policy, then click the **Create New Object** link beneath the field to which you are adding the object. 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, select **Policies > Policies**, then create or edit a policy. You then 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, mouse over the object.
  
  - 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.

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 Policies > 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 2: Common Policy Object Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the object.</td>
</tr>
<tr>
<td></td>
<td>If you change the name while editing the object, the name is automatically</td>
</tr>
<tr>
<td></td>
<td>changed in any policy or object that refers to the object.</td>
</tr>
<tr>
<td>Object Type</td>
<td>The type of object.</td>
</tr>
<tr>
<td></td>
<td>If you create the object while editing a policy, you can select the desired</td>
</tr>
<tr>
<td></td>
<td>object type from among the types supported in the associated field.</td>
</tr>
<tr>
<td></td>
<td>Otherwise, this information is read-only.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the object.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ticket ID</td>
<td>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.)</td>
</tr>
<tr>
<td>Tags</td>
<td>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.</td>
</tr>
<tr>
<td>Object Information</td>
<td>Information about the object usually appears on the right side of the object window and can include the following information:</td>
</tr>
<tr>
<td></td>
<td>• Status—The current status of the object:</td>
</tr>
<tr>
<td></td>
<td>• Pending (New)—The object is new and has never before been committed.</td>
</tr>
<tr>
<td></td>
<td>• Pending (Modified)—The object has been changed since the last commit.</td>
</tr>
<tr>
<td></td>
<td>• Committed—The object has been committed to the device configuration and no changes have been made since the last commit.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Object Type Objects</td>
<td>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. When entering multiple items, press Enter to accept each item and to allow you to select additional items; selecting an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press Enter. To remove an item already in the box, mouse over it and click the X to the right of the name, or click it, then press Delete to remove it, and click away to complete the removal. If your entry is not valid, it is colored yellow; click the Errors link next to the field for information on the problem that you must correct.</td>
</tr>
<tr>
<td>Usage</td>
<td>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.</td>
</tr>
</tbody>
</table>
Network Group and Network Objects

Use network group and network objects (collectively referred to as network objects) to define the IP 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 ASA or CX policies or objects. You can discover these objects from existing ASA configurations and edit or delete them. Any changes that you make are not deployed to the ASA; they affect the use of the objects for CX policies only.

Network objects include the following primary properties. For information on properties common to most policy objects, see Common Policy Object Properties, on page 110.

Include, Exclude lists (CX network group only.)

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.

When entering multiple items, press Enter to accept each item and to allow you to select additional items; selecting an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press Enter. To remove an item already in the box, mouse over it and click the X to the right of the name, or click it, then press Delete to remove it, and click away to complete the removal. If your entry is not valid, it is colored yellow; click the Errors link next to the field for information on the problem that you must correct.

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 ::, 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.
  - IPv6 representation of an IPv4 address, for example, ::10.1.68.3 or 2001:DB8::10.1.68.3.

- 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::CD30::/60.

- (CX network group and ASA network object only.) 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 object only.) IPv6 address ranges, with the first and last address in the range separated by a hyphen, for example, 2001:DB8::0:CD30::1-2001:DB8::CD30::FFFF. The first address must a lower number than the second. You cannot enter an IPv6 address range in a network group object (ASA or ASA CX).

Hostname (network object only.)

A DNS hostname, such as server.example.com.

Network Objects (network group objects, CX and ASA, only.)

The network objects to include in the group object, if any, with the following limitations:

- CX network groups can include these types of objects: CX network group, network group, and network object.

- Network objects (those that can be shared between an ASA and a CX device) can include these types of objects: network group and network object.
Navigation Path

- To create a CX network group object, select Policies > Objects, then select I want to > Add CX Network Group.
- To edit a network group object, select Policies > Objects, then mouse over the object and click Edit Object.

Tip

You can also create and edit objects when you are creating or editing policies. To create a new object, click Create New Object beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click View Object next to the object name in the drop-down list for a field to open the object, then click Edit Object in the object display area. Fill in the object properties, and click Save Object.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

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. In Multiple Device mode, you can discover these objects from existing ASA configurations and edit or delete them.
- Service object—(Multiple Device mode only.) You can use these objects in ASA or CX policies or objects. You can discover these objects from existing ASA configurations and edit or delete them. Any changes that you make are not deployed to the ASA; they affect the use of the objects for CX policies only.

Service objects include the following primary properties. For information on properties common to most policy objects, see Common Policy Object Properties, on page 110.

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.

When entering multiple items, press Enter to accept each item and to allow you to select additional items; selecting an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press Enter. To remove an item already in the box, mouse over it and click the X to the right of the name, or click it, then press Delete to remove it, and click away to complete the removal. If your entry is not valid, it is colored yellow; click the Errors link next to the field for information on the problem that you must correct.
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.

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 Policies > Objects, then select I want to > Add Service Group.
- To edit a service object, select Policies > Objects, then mouse over the object and click Edit Object.

Tip

You can also create and edit objects when you are creating or editing policies. To create a new object, click Create New Object beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click View Object next to the object name in the drop-down list for a field to open the object, then click Edit Object in the object display area. Fill in the object properties, and click Save Object.

Supported Device Types

You can use these objects in policies for the following device types:

- ASA CX

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 110.

Tip

When entering multiple items, press Enter to accept each item and to allow you to select additional items; selecting an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press Enter. To remove an item already in the box, mouse over it and click the X to the right of the name, or click it, then press Delete to remove it, and click away to complete the removal. If your entry is not valid, it is colored yellow; click the Errors link next to the field for information on the problem that you must correct.
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:

• 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 an identity object, select Policies > Objects, then select I want to > Add Identity Object.

• To edit an identity object, select Policies > Objects, then mouse over the object and click Edit Object.
You can also create and edit objects when you are creating or editing policies. To create a new object, click Create New Object beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click View Object next to the object name in the drop-down list for a field to open the object, then click Edit Object in the object display area. Fill in the object properties, and click Save Object.

### 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 110.

#### 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.

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 websites 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.

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.

**Navigation Path**

• To create a URL object, select Policies > Objects, then select I want to > Add URL Object.

• To edit a URL object, select Policies > Objects, then mouse over the object and click Edit Object.

**Tip**

You can also create and edit objects when you are creating or editing policies. To create a new object, click Create New Object beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click View Object next to the object name in the drop-down list for a field to open the object, then click Edit Object in the object display area. Fill in the object properties, and click Save Object.

**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 110.

Tip

When entering multiple items, press Enter to accept each item and to allow you to select additional items; selecting an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press Enter. To remove an item already in the box, mouse over it and click the X to the right of the name, or click it, then press Delete to remove it, and click away to complete the removal. If your entry is not valid, it is colored yellow; click the Errors link next to the field for information on the problem that you must correct.

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 **Policies > Objects**, then select **I want to > Add User Agent Object**.
- To edit a user agent object, select **Policies > Objects**, then mouse over the object and click **Edit Object**.

---

**Tip**
You can also create and edit objects when you are creating or editing policies. To create a new object, click **Create New Object** beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click **View Object** next to the object name in the drop-down list for a field to open the object, then click **Edit Object** in the object display area. Fill in the object properties, and click **Save Object**.

---

**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 110.

---

**Tip**
When entering multiple items, press Enter to accept each item and to allow you to select additional items; selecting an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press Enter. To remove an item already in the box, mouse over it and click the X to the right of the name, or click it, then press Delete to remove it, and click away to complete the removal. If your entry is not valid, it is colored yellow; click the **Errors** link next to the field for information on the problem that you must correct.
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.

Application Type

A list of application types. 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.

Navigation Path

- To create an application object, select Policies > Objects, then select I want to > Add Application Object.
- To edit an application object, select Policies > Objects, then mouse over the object and click Edit Object.

Tip

You can also create and edit objects when you are creating or editing policies. To create a new object, click Create New Object beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click View Object next to the object name in the drop-down list for a field to open the object, then click Edit Object in the object display area. Fill in the object properties, and click Save Object.

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 110.

Tip

When entering multiple items, press Enter to accept each item and to allow you to select additional items; selecting an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press Enter. To remove an item already in the box, mouse over it and click the X to the right of the name, or click it, then press Delete to remove it, and click away to complete the removal. If your entry is not valid, it is colored yellow; click the Errors link next to the field for information on the problem that you must correct.

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 Policies > Objects, then select I want to > Add Secure Mobility Object.
- To edit a Secure Mobility object, select Policies > Objects, then mouse over the object and click Edit Object.

Tip
You can also create and edit objects when you are creating or editing policies. To create a new object, click Create New Object beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click View Object next to the object name in the drop-down list for a field to open the object, then click Edit Object in the object display area. Fill in the object properties, and click Save Object.

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 110.

Tip
When entering multiple items, press Enter to accept each item and to allow you to select additional items; selecting an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press Enter. To remove an item already in the box, mouse over it and click the X to the right of the name, or click it, then press Delete to remove it, and click away to complete the removal. If your entry is not valid, it is colored yellow; click the Errors link next to the field for information on the problem that you must correct.
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 Policies > Objects, then select I want to > Add Application Service Object.

- To edit an application service object, select Policies > Objects, then mouse over the object and click Edit Object.

Tip

You can also create and edit objects when you are creating or editing policies. To create a new object, click Create New Object beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click View Object next to the object name in the drop-down list for a field to open the object, then click Edit Object in the object display area. Fill in the object properties, and click Save Object.
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 110.

Tip
When entering multiple items, press Enter to accept each item and to allow you to select additional items; selecting an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press Enter. To remove an item already in the box, mouse over it and click the X to the right of the name, or click it, then press Delete to remove it, and click away to complete the removal. If your entry is not valid, it is colored yellow; click the Errors link next to the field for information on the problem that you must correct.

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 Policies > Objects, then select I want to > Add Destination Object Group.
• To edit a destination object group, select Policies > Objects, then mouse over the object and click Edit Object.

Tip
You can also create and edit objects when you are creating or editing policies. To create a new object, click Create New Object beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click View Object next to the object name in the drop-down list for a field to open the object, then click Edit Object in the object display area. Fill in the object properties, and click Save Object.

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 110.

Tip
When entering multiple items, press Enter to accept each item and to allow you to select additional items; selecting an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press Enter. To remove an item already in the box, mouse over it and click the X to the right of the name, or click it, then press Delete to remove it, and click away to complete the removal. If your entry is not valid, it is colored yellow; click the Errors link next to the field for information on the problem that you must correct.

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.

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 Policies > Objects, then select I want to > Add Source Object Group.
- To edit a source object, select Policies > Objects, then mouse over the object and click Edit Object.

Tip

You can also create and edit objects when you are creating or editing policies. To create a new object, click Create New Object beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click View Object next to the object name in the drop-down list for a field to open the object, then click Edit Object in the object display area. Fill in the object properties, and click Save Object.

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 110.

Tip

When entering multiple items, press Enter to accept each item and to allow you to select additional items; selecting an item from a drop-down list automatically enters it into the box. To edit an existing item, click it, make your edits, and press Enter. To remove an item already in the box, mouse over it and click the X to the right of the name, or click it, then press Delete to remove it, and click away to complete the removal. If your entry is not valid, it is colored yellow; click the Errors link next to the field for information on the problem that you must correct.
Block file downloads

The MIME type (Multipurpose Internet Mail Extensions, or in general, Internet Media Type) of files that users should be prevented from downloading from destination sites. Use * (asterisk) as a wildcard to indicate zero or more characters; */* to indicate all files. The main types are available in the drop-down list, but you can also specify sub-types, such as application/javascript. The default is to allow all file downloads.

Block file uploads

The MIME type of files that users should be prevented from uploading to destination sites. Use * (asterisk) as a wildcard to indicate zero or more characters; */* to indicate all files. The main types are available in the drop-down list, but you can also specify sub-types, such as application/javascript. The default is to allow all file uploads.

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 Policies > Objects, then select I want to > Add File Filtering Profile.

• To edit a file filtering profile object, select Policies > Objects, then mouse over the object and click Edit Object.
You can also create and edit objects when you are creating or editing policies. To create a new object, click Create New Object beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click View Object next to the object name in the drop-down list for a field to open the object, then click Edit Object in the object display area. Fill in the object properties, and click Save Object.

**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.

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, you can use the tool at http://www.senderbase.org/home.

For information on properties common to most policy objects, see Common Policy Object Properties, on page 110.

Pre-Defined Web Reputation Objects
The Default Reputation Profile pre-defined object implements the recommended low reputation zone.

Navigation Path
• To create a web reputation profile object, select Policies > Objects, then select I want to > Add Web Reputation Profile.
• To edit a web reputation profile object, select Policies > Objects, then mouse over the object and click Edit Object.

Tip
You can also create and edit objects when you are creating or editing policies. To create a new object, click Create New Object beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click View Object next to the object name in the drop-down list for a field to open the object, then click Edit Object in the object display area. Fill in the object properties, and click Save Object.

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
**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.

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 110.

**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.

**Navigation Path**

- To create an interface role object, select **Policies > Objects**, then select **I want to > Add Interface Role**.

- To edit an interface role object, select **Policies > Objects**, then mouse over the object and click **Edit Object**.

You can also create and edit objects when you are creating or editing policies. To create a new object, click **Create New Object** beneath the field to which you are adding the object, and if necessary, select the desired object type in the object display area. To edit the object, mouse over the object name in the field or click **View Object** next to the object name in the drop-down list for a field to open the object, then click **Edit Object** in the object display area. Fill in the object properties, and click **Save Object**.
Supported Device Types

You can use these objects in policies for the following device types:

- No device types are supported. See the release notes on Cisco.com for the latest support information.

Note

For CX devices, the interface names are those that exist on the host, or parent, device.
PART II

Monitoring Devices

- Viewing Dashboards and Reports, page 139
- Viewing Events, page 177
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 139
- Dashboard Basics, page 142
- Dashboard Reference, page 154

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 ASACX.

**Figure 11: Network Overview Dashboard, Single Device mode**

1. Device summary dashboard.
2. Time selector to determine the range of data in the dashboard.
3. Toggle between viewing data based on transaction count or throughput (bits per second).
4. Health and Performance dashboard. The overview dashboard includes dashboards for several items.
5. Mouse over graphs to see pop up details about individual data points.
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 ASACX, as shown in the following illustration.

**Figure 12: Device Summary Dashboard, Multiple Device mode**
### Overview of Dashboards

| 1 | Dashboard title. | 4 | View More link. Click this link to go to the summary dashboard for that reportable item. |
| 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 13: Top Destinations Dashboard**

![Top Destinations Dashboard](image)
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.

- Data is aggregated into 5 minute buckets, and 30 minute and one hour graphs show data points in 5 minute increments. Real time data is added to the current 5 minute bucket, which will always be less than a full 5 minutes. For older time ranges, these buckets are further aggregated into one hour buckets (for the past day) and one day buckets (for up to a week) and one week buckets (for older periods). The farther back you look, the more aggregated the data.

  **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.

- 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.

- 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.
Some dashboards are inherently more accurate than other dashboards. The following dashboards have exact data: Network Summary, Applications, Application Types, Policy Hits, Web Categories, User Devices, Malicious Traffic. All other summary and detail dashboards provide approximate data.

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 14: Going from top five dashboard to full summary dashboard**

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 15: 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.

*Figure 16: Going from summary dashboard to Event Viewer through transactions link*

### 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 **Device > Devices**. If there are any alerts, they are shown on the right side of the device row.

*Figure 17: 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_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. You cannot update the password in PRSM, so you should never change the password after adding the device to the inventory. If this is the cause of the problem, you must delete the device from the inventory and add it back using the new password. You will have to reassign the device to the desired device group.

**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.
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.

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.

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 3: Time Ranges for Dashboards

<table>
<thead>
<tr>
<th>Time Range</th>
<th>Data Returned In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last 30 minutes</td>
<td>Thirty (30) complete minutes in 5 minute intervals, plus up to 5 additional minutes.</td>
</tr>
<tr>
<td>Last Hour</td>
<td>Sixty (60) complete minutes in 5 minute intervals, plus up to 5 additional minutes.</td>
</tr>
<tr>
<td>Time Range</td>
<td>Data Returned In</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last 24 Hours</td>
<td>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.</td>
</tr>
<tr>
<td>Last 7 Days</td>
<td>One hour intervals for the last 7 days rounded to the previous hour boundary.</td>
</tr>
<tr>
<td>Last 30 Days</td>
<td>One day intervals for the last 30 days starting from the previous midnight.</td>
</tr>
<tr>
<td>Yesterday</td>
<td>The last 24 hours (00:00 to 23:59) using the time zone defined on the device. Data is in one hour intervals.</td>
</tr>
</tbody>
</table>
| 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. The intervals presented depend on the length of time in the range:  
  • Ten (10) hours or less uses 5 minute intervals.  
  • Ten hours to ten days uses one hour intervals.  
  • Longer ranges use one day intervals. |

**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, Data Usage

Click these links to view charts based on the number of transactions or the amount of data in the transactions.

*Figure 18: Toggling between transactions and data usage*
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.

Figure 19: Toggling between all transactions and denied transactions (denied site names have been blanked out)

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 4: Dashboard Columns**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard Columns</strong></td>
<td></td>
</tr>
<tr>
<td>Transactions</td>
<td>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.</td>
</tr>
<tr>
<td>Transactions allowed</td>
<td>The number of transactions that were allowed for the reported item.</td>
</tr>
<tr>
<td>Transactions denied</td>
<td>The number of transactions that were blocked (based on policy) for the reported item.</td>
</tr>
<tr>
<td>Data Usage</td>
<td>The sum of bytes sent and received for the reported item.</td>
</tr>
<tr>
<td>Bytes sent</td>
<td>The number of bytes sent for the reported item.</td>
</tr>
<tr>
<td>Bytes received</td>
<td>The number of bytes received for the reported item.</td>
</tr>
<tr>
<td><strong>Variable Columns</strong></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>The name of the application in the transaction as determined by the AVC engine.</td>
</tr>
<tr>
<td>Application type</td>
<td>The name of the application type for the application used in the transaction as determined by the AVC engine.</td>
</tr>
<tr>
<td>Device Name</td>
<td>(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 &quot;- DELETED.&quot;</td>
</tr>
<tr>
<td>Domain name</td>
<td>The DNS name or IP address of the web site involved in the transaction.</td>
</tr>
<tr>
<td>Policy name</td>
<td>The name of the context-aware access policy that matched the transaction. If you deleted the policy, the name is appended with &quot;- DELETED.&quot;</td>
</tr>
<tr>
<td>User device</td>
<td>The name of the operating system or device used by the remote access VPN client making the transaction.</td>
</tr>
<tr>
<td>User name</td>
<td>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 Realm\ANONYMOUS. Users who simply do not have a mapping because they were not required to authenticate are shown as their IP address.</td>
</tr>
<tr>
<td>Web category</td>
<td>The name of the web (URL) category. Information for a category is the summary for all URLs that fall within the category.</td>
</tr>
</tbody>
</table>
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 153.

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 153.

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.

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.

Dashboard Reference

The topics in this reference explain the content of the various dashboards.
Network Overview

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.

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.

To view the network overview, select Dashboard > Network Overview.

The following table explains the elements of the network overview dashboard.

<table>
<thead>
<tr>
<th>Table 5: Network Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Element</strong></td>
</tr>
<tr>
<td>Time Range</td>
</tr>
</tbody>
</table>
| On-box device summary (Single Device mode only.) | Summary information about the CX device you are logged into, including any alerts that need to be addressed. (For more information on alerts, see Resolving Device Alerts, on page 145.) 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 (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 data display between the ASA and the ASA 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 145.  
    - 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. |
### Element | Description
--- | ---
Malicious Traffic | 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
- EventType=HTTP Complete
- EventType=TLS Complete

Click **View All** to see the Malicious Traffic dashboard, which provides more details about low reputation traffic.

Health and Performance | 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.

Top policies | The access policies that matched the most traffic flows, by transactions or data usage. Click **View More** to see a complete list.

Top sources | The users, and their remote-access-VPN user devices, who generated the most traffic, by transactions or data usage. Usernames are in the format Realm\username.. Click **View More** to see a complete list for each option.

Top CX (Multiple Device mode only.) | The CX devices that processed the most traffic by transactions or data usage. Click **View More** to see a complete list.
### 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
The web categories, web destinations, applications, and application types users visited or used most, in transactions or data usage. Click View More to see a complete list for each option.

---

**Malicious Traffic Dashboard**

The malicious traffic 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. For more information on web reputation, see Web Reputation Profile Objects, on page 132.

**Tip**
To look up the reputation of a site, you can use the tool at [http://www.senderbase.org/home](http://www.senderbase.org/home).

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.

To view the malicious traffic dashboard, select Dashboard > Malicious Traffic. You can also view the dashboard by clicking View All in the Malicious Traffic dashboard on the network overview.

The following table explains the elements of the malicious traffic dashboard.

**Table 6: Malicious Traffic Dashboard**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Range</strong></td>
<td>The time range for data to include in the dashboard. For more information, see Changing the Dashboard Time Range, on page 148.</td>
</tr>
<tr>
<td>Malware Types</td>
<td>A pie chart that shows the malware types identified in the low reputation traffic, by transactions or data usage. Click View More to see detailed information in the Malware Types dashboard.</td>
</tr>
<tr>
<td>Top Malicious Transactions</td>
<td>The users, web categories, web destinations, and applications involved most often in low reputation traffic, in transactions or data usage. Click View More to see the malicious transactions dashboard for each option.</td>
</tr>
</tbody>
</table>
Malicious Traffic

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.

Malware Types Dashboard

The malware types dashboard shows the types of malware associated with the low-reputation malicious traffic in the network. A transaction is considered to be malicious if the web reputation of the site is -6 or lower. For more information on web reputation, see Web Reputation Profile Objects, on page 132.

To open the malware types dashboard, select Dashboard > Malicious Traffic to open the malicious traffic dashboard, then click View More in the Malware Types dashboard.

Potential malware types include the following:

- Adware
- Conficker
- Not Malicious
- Related to Phishing
- Related to Spam
- Spyware
- Suspected Malware
- Trojan

The following table explains the elements of the malware types dashboard.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Range</td>
<td>The time range for data to include in the dashboard. For more information, see Changing the Dashboard Time Range, on page 148.</td>
</tr>
<tr>
<td>Items Shown</td>
<td>How many items to show in the list: 10, 100, or 1000.</td>
</tr>
<tr>
<td>Values, Percentages</td>
<td>Whether to view statistics based on the raw numbers (Values) or the percentage of overall usage (Percentages).</td>
</tr>
</tbody>
</table>
The users with malicious transactions dashboard shows the users who had transactions with low reputation web servers. A transaction is considered to be malicious if the web reputation of the site is -6 or lower. For more information on web reputation, see Web Reputation Profile Objects, on page 132.

To open the users with malicious transactions dashboard, select Dashboard > Malicious Traffic to open the malicious traffic dashboard, then click View More in the Users section of the Top Malicious Transactions dashboard.

The following table explains the elements of the users with malicious transactions dashboard.

### Table 8: Users with Malicious Transactions Dashboard

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Range</strong></td>
<td>The time range for data to include in the dashboard. For more information, see Changing the Dashboard Time Range, on page 148.</td>
</tr>
<tr>
<td><strong>Items Shown</strong></td>
<td>How many items to show in the list: 10, 100, or 1000.</td>
</tr>
<tr>
<td><strong>Values, Percentages</strong></td>
<td>Whether to view statistics based on the raw numbers (Values) or the percentage of overall usage (Percentages).</td>
</tr>
<tr>
<td>Users with malicious transactions table</td>
<td>Summary information about the transactions and bytes associated with each user with malicious transactions.</td>
</tr>
<tr>
<td></td>
<td>• Click the number in the transactions cell to open the Event Viewer with the events table filtered based on the user name, web reputation, and time range.</td>
</tr>
</tbody>
</table>

The web categories with malicious transactions dashboard shows the categories of web sites that included servers with low reputation with which users had transactions. A transaction is considered to be malicious if the web reputation of the site is -6 or lower. For more information on web reputation, see Web Reputation Profile Objects, on page 132.

To open the web categories with malicious transactions dashboard, select Dashboard > Malicious Traffic to open the malicious traffic dashboard, then click View More in the Web Categories section of the Top Malicious Transactions dashboard.
The following table explains the elements of the web categories with malicious transactions dashboard.

**Table 9: Web Categories with Malicious Transactions Dashboard**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Range</strong></td>
<td>The time range for data to include in the dashboard. For more information, see <a href="#">Changing the Dashboard Time Range</a>, on page 148.</td>
</tr>
<tr>
<td><strong>Items Shown</strong></td>
<td>How many items to show in the list: 10, 100, or 1000.</td>
</tr>
<tr>
<td><strong>Values, Percentages</strong></td>
<td>Whether to view statistics based on the raw numbers (Values) or the percentage of overall usage (Percentages).</td>
</tr>
<tr>
<td><strong>Web Categories with malicious transactions table</strong></td>
<td>Summary information about the transactions and bytes associated with each web category with malicious transactions.</td>
</tr>
<tr>
<td></td>
<td>• Click the number in the transactions cell to open the Event Viewer with the events table filtered based on the category name, web reputation, and time range.</td>
</tr>
</tbody>
</table>

**Web Destinations with Malicious Transactions Dashboard**

The web destinations with malicious transactions dashboard shows the low-reputation web sites with which users are having transactions. A transaction is considered to be malicious if the web reputation of the site is -6 or lower. For more information on web reputation, see [Web Reputation Profile Objects](#), on page 132.

To open the web destinations with malicious transactions dashboard, select **Dashboard > Malicious Traffic** to open the malicious traffic dashboard, then click **View More** in the Web Destinations section of the Top Malicious Transactions dashboard.

The following table explains the elements of the web destinations with malicious transactions dashboard.

**Table 10: Web Destinations with Malicious Transactions Dashboard**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Range</strong></td>
<td>The time range for data to include in the dashboard. For more information, see <a href="#">Changing the Dashboard Time Range</a>, on page 148.</td>
</tr>
<tr>
<td><strong>Items Shown</strong></td>
<td>How many items to show in the list: 10, 100, or 1000.</td>
</tr>
<tr>
<td><strong>Values, Percentages</strong></td>
<td>Whether to view statistics based on the raw numbers (Values) or the percentage of overall usage (Percentages).</td>
</tr>
<tr>
<td><strong>Web destinations with malicious transactions table</strong></td>
<td>Summary information about the transactions and bytes associated with each web destination with malicious transactions.</td>
</tr>
<tr>
<td></td>
<td>• Click the number in the transactions cell to open the Event Viewer with the events table filtered based on the domain name, web reputation, and time range.</td>
</tr>
</tbody>
</table>
**Applications With Malicious Transactions Dashboard**

The applications with malicious transactions 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. For more information on web reputation, see [Web Reputation Profile Objects](#) on page 132.

There are two types of applications with malicious transactions dashboard, summary and detail:

- **Applications with Malicious Transactions Summary Dashboard**—Simply named Applications with Malicious Transactions, this dashboard provides summary information about all of the applications that had low-reputation traffic. To view the applications with malicious transactions dashboard, click View All in the applications list of the Top Malicious Transactions dashboard in the Malicious Traffic dashboard (Dashboard > Malicious Traffic).

- **Applications with Malicious Transactions Detail Dashboard**—The name of this dashboard indicates the application being viewed in the format Applications with Malicious Transactions > Application Name. You can view this dashboard by clicking an application link in the applications with malicious transactions dashboard or the applications with malicious transactions dashboard. You can also click an application in the Top Malicious Transactions dashboard in the Malicious Traffic dashboard.

The following table explains the elements of the applications with malicious transactions dashboard.

<table>
<thead>
<tr>
<th>Table 11: Applications with Malicious Transactions Dashboard</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Element</strong></td>
</tr>
<tr>
<td>Time Range</td>
</tr>
<tr>
<td>Items Shown</td>
</tr>
<tr>
<td>Values, Percentages</td>
</tr>
</tbody>
</table>

Applications with malicious transactions table

Summary information about the transactions and bytes associated with each application with malicious transactions.

- Click an application name to see a detailed dashboard for that application.
- Click the number in the transactions cell to open the Event Viewer with the events table filtered based on the application name, web reputation, and time range.

Applications Detail Dashboard

Application summary

Summary information about the low-reputation transactions and bytes associated with the application.
### Users Dashboard

The users dashboard 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`. 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.

There are two types of users dashboard, summary and detail:

- **Users Summary Dashboard**—Simply named Users, this dashboard provides summary information about all of the users identified. To view the users dashboard, select **Dashboard > Users**.

- **Users Detail Dashboard**—The name of this dashboard indicates the user being viewed in the format **Users > User Name**. You can view this dashboard by clicking a user link in the users dashboard or the users chart in the top sources dashboard.

**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 an Active Directory (AD) agent to supply passive authentication and optionally use active authentication as a backup method.

The following table explains the elements of the users dashboard.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top policies</td>
<td>The access policies that matched the low-reputation connection attempts for the application most often, by transactions or data usage. Click <strong>View More</strong> to see a complete list.</td>
</tr>
<tr>
<td>Top sources</td>
<td>The users, and their remote-access-VPN user devices, who generated the most low-reputation traffic for the application, by transactions or data usage. Usernames are in the format Realm\username.. Click <strong>View More</strong> to see a complete list for each option.</td>
</tr>
<tr>
<td>Top CX (Multiple Device mode only.)</td>
<td>The CX devices that processed the most low-reputation traffic by transactions or data usage for this application. Click <strong>View More</strong> to see a complete list.</td>
</tr>
<tr>
<td>Top destinations</td>
<td>The web categories and destinations used with or associated with the low-reputation traffic for this application most often, in transactions or data usage. Click <strong>View More</strong> to see a complete list for each option.</td>
</tr>
</tbody>
</table>
### Table 12: Users Summary and Detail Dashboard

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Users Summary Dashboard</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Time Range</strong></td>
<td>The time range for data to include in the dashboard. For more information, see <a href="#">Changing the Dashboard Time Range, on page 148</a>.</td>
</tr>
<tr>
<td><strong>Items Shown</strong></td>
<td>How many items to show in the list: 10, 100, or 1000.</td>
</tr>
<tr>
<td><strong>Values, Percentages</strong></td>
<td>Whether to view statistics based on the raw numbers (Values) or the percentage of overall usage (Percentages).</td>
</tr>
<tr>
<td><strong>Users table</strong></td>
<td>Summary information about the transactions and bytes associated with each user.</td>
</tr>
<tr>
<td></td>
<td>• Click a user name to see a detailed dashboard for that user.</td>
</tr>
<tr>
<td></td>
<td>• Click the number in the transactions cell to open the Event Viewer with the events table filtered based on the user name and time range.</td>
</tr>
<tr>
<td><strong>Users Detail Dashboard</strong></td>
<td></td>
</tr>
<tr>
<td><strong>User summary</strong></td>
<td>Summary information about the transactions and bytes associated with the user.</td>
</tr>
<tr>
<td><strong>Applications with malicious transactions</strong></td>
<td>The transactions made with sites of low web reputation, if any, by transactions or data usage. The user might have made direct attempts to connect to the site, or the transactions might have been made through other web pages the user visited. Click <strong>View More</strong> to see a complete list.</td>
</tr>
<tr>
<td><strong>Top user devices</strong></td>
<td>The devices the user used to connect to the network through remote access VPN most often, by transactions or data usage. This chart is empty if the user made no remote access VPN connections during the selected time range. Click <strong>View More</strong> to see a complete list.</td>
</tr>
<tr>
<td><strong>Top policies</strong></td>
<td>The access policies that matched the user’s connection attempts most often, by transactions or data usage. Click <strong>View More</strong> to see a complete list.</td>
</tr>
<tr>
<td><strong>Top destinations</strong></td>
<td>The web categories, web destinations, applications, and application types the user visited or used most, in transactions or data usage. Click <strong>View More</strong> to see a complete list for each option.</td>
</tr>
<tr>
<td><strong>Top CX (Multiple Device mode only.)</strong></td>
<td>The CX devices that processed the most traffic by transactions or data usage for this user. Click <strong>View More</strong> to see a complete list.</td>
</tr>
</tbody>
</table>
**Web Destinations Dashboard**

The web destinations dashboard shows which servers, such as www.google.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.

There are two types of destinations dashboard, summary and detail:

- **Web Destinations Summary Dashboard**—Simply named Web destinations, this dashboard provides summary information about all of the websites identified. To view the web destinations dashboard, select **Dashboard > Web Destinations**.

- **Web Destinations Detail Dashboard**—The name of this dashboard indicates the destination being viewed in the format **Web destinations > Destination Name**. You can view this dashboard by clicking a domain name link in the web destinations dashboard or the web destinations chart in the top destinations dashboard.

The following table explains the elements of the web destinations dashboard.

### Table 13: Web Destinations Summary and Detail Dashboard

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web Destinations Summary Dashboard</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Time Range</strong></td>
<td>The time range for data to include in the dashboard. For more information, see <strong>Changing the Dashboard Time Range</strong>, on page 148.</td>
</tr>
<tr>
<td><strong>Items Shown</strong></td>
<td>How many items to show in the list: 10, 100, or 1000.</td>
</tr>
<tr>
<td><strong>Values, Percentages</strong></td>
<td>Whether to view statistics based on the raw numbers (Values) or the percentage of overall usage (Percentages).</td>
</tr>
</tbody>
</table>
| Destinations table | Summary information about the transactions and bytes associated with each website.  
  - Click a domain name to see a detailed dashboard for that site.  
  - Click the number in the transactions cell to open the Event Viewer with the events table filtered based on the domain name and time range. |
| **Web Destinations Detail Dashboard** | |
| Web destination summary | Summary information about the transactions and bytes associated with the website. |
| Applications with malicious transactions | The transactions made through this site with sites of low web reputation, if any, by transactions or data usage. Click **View More** to see a complete list. |
| Top sources | The users, and their remote-access-VPN user devices, who generated the most traffic for the site, by transactions or data usage. Usernames are in the format Realm\username. Click **View More** to see a complete list for each option. |
Web Categories Dashboard

The web, or URL, categories dashboard shows which categories of websites, such as Gambling, Advertisements, or Search Engines and Portals, are being used in the network based on the categorization of websites 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.

There are two types of web categories dashboard, summary and detail:

- **Web Categories Summary Dashboard**—Simply named Web Categories, this dashboard provides summary information about all of the categories identified. To view the web categories dashboard, select Dashboard > Web Categories.

- **Web Categories Detail Dashboard**—The name of this dashboard indicates the category being viewed in the format Web Categories > Category Name. You can view this dashboard by clicking a category name link in the web categories dashboard or the web categories chart in the top destinations dashboard.

The following table explains the elements of the web categories dashboard.

### Table 14: Web Categories Summary and Detail Dashboard

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web Categories Summary Dashboard</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Time Range</strong></td>
<td>The time range for data to include in the dashboard. For more information, see Changing the Dashboard Time Range, on page 148.</td>
</tr>
<tr>
<td><strong>Items Shown</strong></td>
<td>How many items to show in the list: 10, 100, or 1000.</td>
</tr>
<tr>
<td><strong>Values, Percentages</strong></td>
<td>Whether to view statistics based on the raw numbers (Values) or the percentage of overall usage (Percentages).</td>
</tr>
</tbody>
</table>
### Element | Description
--- | ---
Web category table | Summary information about the transactions and bytes associated with each web category.
- Click a category name to see a detailed dashboard for that category.
- Click the number in the transactions cell to open the Event Viewer with the events table filtered based on the category name and time range.

#### Web Categories Detail Dashboard

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web category summary</td>
<td>Summary information about the transactions and bytes associated with the web category. Click the open/close arrow next to the category name to see specific information for all sites within the category that had traffic during the selected time period.</td>
</tr>
<tr>
<td>Applications with malicious transactions</td>
<td>The transactions made through the sites in this category with sites of low web reputation, if any, by transactions or data usage. Click View More to see a complete list.</td>
</tr>
<tr>
<td>Top sources</td>
<td>The users, and their remote-access-VPN user devices, who generated the most traffic for sites in the category, by transactions or data usage. Usernames are in the format Realm\username. Click View More to see a complete list for each option.</td>
</tr>
<tr>
<td>Top policies</td>
<td>The access policies that matched the connection attempts to sites in the category most often, by transactions or data usage. Click View More to see a complete list.</td>
</tr>
<tr>
<td>Top destinations</td>
<td>The applications and application types used with or associated with sites in this web category most often, in transactions or data usage. Click View More to see a complete list for each option.</td>
</tr>
<tr>
<td>Top CX (Multiple Device mode only.)</td>
<td>The CX devices that processed the most traffic by transactions or data usage for web sites in this category. Click View More to see a complete list.</td>
</tr>
</tbody>
</table>

### Policy Hits Dashboard

The policy hits dashboard shows how the access policies have been applied to traffic in the network. Use this information to help evaluate policy efficacy.

There are two types of policy hits dashboard, summary and detail:

- Policy Hits Summary Dashboard—Simply named Policy Hits, this dashboard provides summary information about all of the access policies. To view the policy hits dashboard, select Dashboard > Policies.
• Policy Hits Detail Dashboard—The name of this dashboard indicates the policy being viewed in the format **Policy Hits > Policy Name**. You can view this dashboard by clicking a policy link in the policies dashboard or the policy hits chart in the top policies dashboard.

The following table explains the elements of the policy hits dashboard.

### Table 15: Policy Hits Summary and Detail Dashboard

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy Hits Summary Dashboard</strong></td>
<td></td>
</tr>
<tr>
<td>Time Range</td>
<td>The time range for data to include in the dashboard. For more information, see Changing the Dashboard Time Range, on page 148.</td>
</tr>
<tr>
<td>Items Shown</td>
<td>How many items to show in the list: 10, 100, or 1000.</td>
</tr>
<tr>
<td>Values, Percentages</td>
<td>Whether to view statistics based on the raw numbers (Values) or the percentage of overall usage (Percentages).</td>
</tr>
</tbody>
</table>
| Policy hits table                    | Summary information about the transactions and bytes associated with each access policy.  
  - Click a policy name to see a detailed dashboard for that policy. If you deleted the policy, the name is appended with "- DELETED."  
  - Click the number in the transactions cell to open the Event Viewer with the events table filtered based on the policy name and time range. |

| **Policy Hits Detail Dashboard**     |                                                                             |
| Policy summary                       | Summary information about the transactions and bytes associated with the policy. |
| Applications with malicious transactions | The transactions made by flows matching this policy with sites of low web reputation, if any, by transactions or data usage. Click View More to see a complete list. |
| Top sources                          | The users, and their remote-access-VPN user devices, who generated the most traffic that matched this policy, by transactions or data usage. Usernames are in the format Realm\username.. Click View More to see a complete list for each option. |
| Top CX (Multiple Device mode only.)  | The CX devices that processed the most traffic by transactions or data usage that matched this policy. Click View More to see a complete list. |
| Top destinations                     | The web categories, web destinations, applications, and application types used most often in traffic flows that matched this policy. Click View More to see a complete list for each option. |
User Devices Dashboard

The user devices 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.

There are two types of user devices dashboard, summary and detail:

- **User Devices Summary Dashboard**—Simply named User Devices, this dashboard provides summary information about all of the operating systems used on remote access VPN devices. To view the remote access VPN user devices dashboard, select **Dashboard > User Devices**.

- **User Devices Detail Dashboard**—The name of this dashboard indicates the operating system being viewed in the format **User Devices > Operating System**. You can view this dashboard by clicking a user device link in the user devices dashboard or the user devices chart in the top sources dashboard.

The following table explains the elements of the user devices dashboard.

<table>
<thead>
<tr>
<th><strong>Table 16: User Devices Dashboard</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Element</strong></td>
</tr>
<tr>
<td>User Devices Summary Dashboard</td>
</tr>
<tr>
<td><strong>Time Range</strong></td>
</tr>
<tr>
<td><strong>Items Shown</strong></td>
</tr>
<tr>
<td><strong>Values, Percentages</strong></td>
</tr>
<tr>
<td>User devices table</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>User Device Detail Dashboard</td>
</tr>
<tr>
<td>User device summary</td>
</tr>
<tr>
<td>Top users</td>
</tr>
</tbody>
</table>
Applications Dashboard

The applications 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.

There are two types of applications dashboard, summary and detail:

- Applications Summary Dashboard—Simply named Applications, this dashboard provides summary information about all of the applications identified. To view the applications dashboard, select Dashboard > Applications.

- Applications Detail Dashboard—The name of this dashboard indicates the application being viewed in the format Applications > Application Name. You can view this dashboard by clicking an application link in the applications dashboard or the applications chart in the top destinations dashboard.

The following table explains the elements of the applications dashboard.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Applications Summary Dashboard</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Time Range</strong></td>
<td>The time range for data to include in the dashboard. For more information, see Changing the Dashboard Time Range, on page 148.</td>
</tr>
<tr>
<td><strong>Items Shown</strong></td>
<td>How many items to show in the list: 10, 100, or 1000.</td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Values, Percentages</td>
<td>Whether to view statistics based on the raw numbers (Values) or the percentage of overall usage (Percentages).</td>
</tr>
</tbody>
</table>
| Applications table   | Summary information about the transactions and bytes associated with each application.  
                        - Click an application name to see a detailed dashboard for that application.  
                        - Click the number in the transactions cell to open the Event Viewer with the events table filtered based on the application name and time range. |

### Applications Detail Dashboard

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application summary</td>
<td>Summary information about the transactions and bytes associated with the application. The category to which the application belongs is identified.</td>
</tr>
<tr>
<td>Top policies</td>
<td>The access policies that matched the connection attempts for the application most often, by transactions or data usage. Click <strong>View More</strong> to see a complete list.</td>
</tr>
<tr>
<td>Top sources</td>
<td>The users, and their remote-access-VPN user devices, who generated the most traffic for the application, by transactions or data usage. Usernames are in the format Realm/username.. Click <strong>View More</strong> to see a complete list for each option.</td>
</tr>
<tr>
<td>Top CX (Multiple Device mode only.)</td>
<td>The CX devices that processed the most traffic by transactions or data usage for this application. Click <strong>View More</strong> to see a complete list.</td>
</tr>
<tr>
<td>Top destinations</td>
<td>The web categories and destinations used with or associated with this application most often, in transactions or data usage. Click <strong>View More</strong> to see a complete list for each option.</td>
</tr>
</tbody>
</table>

### Application Types Dashboard

The application types 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.

There are two types of application types dashboard, summary and detail:

- **Application Types Summary Dashboard**—Simply named Application Types, this dashboard provides summary information about all of the application types identified. To view the application types dashboard, select **Dashboard > Application Types**.

- **Application Types Detail Dashboard**—The name of this dashboard indicates the application type being viewed in the format Application Types > Application Type Name. You can view this dashboard by clicking an application type link in the applications dashboard or the application types chart in the top destinations dashboard.
The following table explains the elements of the application types dashboard.

Table 18: Application Types Summary and Detail Dashboard

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Types Summary Dashboard</strong></td>
<td><strong>Time Range</strong> The time range for data to include in the dashboard. For more information, see Changing the Dashboard Time Range, on page 148.</td>
</tr>
<tr>
<td><strong>Items Shown</strong></td>
<td>How many items to show in the list: 10, 100, or 1000.</td>
</tr>
<tr>
<td><strong>Values, Percentages</strong></td>
<td>Whether to view statistics based on the raw numbers (Values) or the percentage of overall usage (Percentages).</td>
</tr>
</tbody>
</table>
| **Application types table**                 | Summary information about the transactions and bytes associated with each application type.  
                                           |   • Click an application type name to see a detailed dashboard for that application type.  
                                           |   • Click the number in the transactions cell to open the Event Viewer with the events table filtered based on the application type name and time range. |

**Application Types Detail Dashboard**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Application type summary**                | Summary information about the transactions and bytes associated with the application type.  
                                           | Click the open/close arrow next to the application type name to see specific information for all applications of this type that had traffic during the selected time period. |
| **Applications with malicious transactions**| The transactions made using applications of this type with sites of low web reputation, if any, by transactions or data usage. Click View More to see a complete list. |
| **Top sources**                             | The users, and their remote-access-VPN user devices, who generated the most traffic for the applications of this type, by transactions or data usage. Usernames are in the format Realm\username.. Click View More to see a complete list for each option. |
| **Top policies**                            | The access policies that matched the connection attempts for the applications of this type most often, by transactions or data usage. Click View More to see a complete list. |
| **Top destinations**                        | The web categories and destinations used with or associated with the applications of this type most often, in transactions or data usage. Click View More to see a complete list for each option. |
The CX devices that processed the most traffic by transactions or data usage for this application type. Click View More to see a complete list.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top CX</td>
<td>The CX devices that processed the most traffic by transactions or data usage for this application type. Click View More to see a complete list.</td>
</tr>
</tbody>
</table>

### Devices Dashboard

The devices dashboard is available in PRSM Multiple Device mode only.

The devices dashboard shows summary information for each device that is managed by this PRSM server. 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.

There are two types of devices dashboard, summary and detail:

- Devices Summary Dashboard—Simply named Devices, this dashboard provides summary information about all of the devices being managed. To view the devices dashboard, select Dashboard > Devices.

- Devices Detail Dashboard—The name of this dashboard indicates the device being viewed in the format Devices > Device Name or IP Address. You can view this dashboard by clicking a device link in the devices dashboard or the device summary dashboard.

### Note

If you delete a device from the inventory, its data remains available for historical periods. The device name is appended with "DELETED."

The following table explains the elements of the devices dashboard.

**Table 19: Devices Summary and Detail Dashboard**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices Summary Dashboard</td>
<td></td>
</tr>
<tr>
<td>Time Range</td>
<td>The time range for data to include in the dashboard. For more information, see Changing the Dashboard Time Range, on page 148.</td>
</tr>
<tr>
<td>Items Shown</td>
<td>How many items to show in the list: 10, 100, or 1000.</td>
</tr>
<tr>
<td>Values, Percentages</td>
<td>Whether to view statistics based on the raw numbers (Values) or the percentage of overall usage (Percentages).</td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Devices table | Summary information about the transactions and bytes associated with each device.  
  - Click a device name to see a detailed dashboard for that device.  
  - Click the number in the transactions cell to open the Event Viewer with the events table filtered based on the device name and time range. |
| Devices Detail Dashboard | Summary information about the managed devices, including any alerts that need to be addressed. (For more information on alerts, see Resolving Device Alerts, on page 145.) The summary includes the following information:  
  - The list on the left shows the software version running on each device, the device model, the device group, 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.  
  - The chart and table on the right shows the amount of network activity passing through the system based on transactions (raw number of connections) and throughput (data rate). Use the links above the graph to toggle between the ASA and the ASA CX. Use the drop-down list to view denied, allowed, or all transactions when viewing the CX charts. Mouse over the graph to see the time and value of specific data points.  
    You can add or remove lines by clicking on Transactions or Throughput in the chart legend. |
| Devices summary | The transactions made with sites of low web reputation, if any, by transactions or data usage. Users might have made direct attempts to connect to the site, or the transactions might have been made through other web pages users visited. Click View More to see a complete list. |
| Applications with malicious transactions | The transactions made with sites of low web reputation, if any, by transactions or data usage. Users might have made direct attempts to connect to the site, or the transactions might have been made through other web pages users visited. Click View More to see a complete list. |
| Health and Performance | Separate charts for aggregate CPU and memory usage, which provide insight into the load on the device. There are separate lines for the ASA and the ASA 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. |
| Top policies | The access policies that matched the connection attempts through the device most often, by transactions or data usage. Click View More to see a complete list. |
The users, and their remote-access-VPN user devices, who generated the most traffic through the device, by transactions or data usage. Usernames are in the format Realm\username. Click View More to see a complete list for each option.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top sources</td>
<td>The users, and their remote-access-VPN user devices, who generated the most traffic through the device, by transactions or data usage. Usernames are in the format Realm\username. Click View More to see a complete list for each option.</td>
</tr>
<tr>
<td>Top destinations</td>
<td>The web categories, web destinations, applications, and application types that were visited or used most through this device, in transactions or data usage. Click View More to see a complete list for each option.</td>
</tr>
</tbody>
</table>

### Interface Dashboard

The interface dashboard is available in PRSM 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.

You can view a single interface at a time.

The time range used in the dashboard is the same range you selected in the device detail dashboard.

The following table explains the elements of the interface dashboard.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port name and status (Interfaces with problems only.)</td>
<td>The name of the hardware port, for example, GigabitEthernet0/0, and current status, for example, down because the administrator shut it down.</td>
</tr>
<tr>
<td>Interface name</td>
<td>The name of the interface, for example, inside.</td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Traffic Usage</td>
<td>A chart that shows traffic rates. Mouse over the lines to see the time and</td>
</tr>
<tr>
<td></td>
<td>value of specific data points. You can manipulate the chart using the</td>
</tr>
<tr>
<td></td>
<td>following controls:</td>
</tr>
<tr>
<td></td>
<td>• VLAN name—If VLANs are defined for the interface, select a VLAN name</td>
</tr>
<tr>
<td></td>
<td>to see data rates for the VLAN only.</td>
</tr>
<tr>
<td></td>
<td>• Packet rates—To view the chart in packets per second. There are separate</td>
</tr>
<tr>
<td></td>
<td>lines for incoming and outgoing traffic; you can add or remove these</td>
</tr>
<tr>
<td></td>
<td>lines by clicking the Input, Output labels in the legend.</td>
</tr>
<tr>
<td></td>
<td>• Throughput—To view the chart in bits per second.</td>
</tr>
<tr>
<td></td>
<td>• Avg packet size—To view the chart in average packet size in bytes.</td>
</tr>
<tr>
<td></td>
<td>• Dropped packet count—To view the chart in a raw count of dropped packets.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>A chart that shows various error rates. Mouse over the lines to see the</td>
</tr>
<tr>
<td></td>
<td>time and value of specific data points. In most charts, you can add or</td>
</tr>
<tr>
<td></td>
<td>remove lines by clicking the labels in the legend. Click Refresh to</td>
</tr>
<tr>
<td></td>
<td>update the charts with new data.</td>
</tr>
<tr>
<td></td>
<td>You can manipulate the chart using the following controls:</td>
</tr>
<tr>
<td></td>
<td>• Packet Errors—To view a count of CRC and frame packet errors.</td>
</tr>
<tr>
<td></td>
<td>• Buffer Resources—To view packet counts for buffer overrun and under-run.</td>
</tr>
<tr>
<td></td>
<td>• Collision Count—To view packet counts for collisions and late collisions.</td>
</tr>
<tr>
<td></td>
<td>• Other—To view a count of broadcast packets.</td>
</tr>
</tbody>
</table>
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 177
- Using Event Views, page 181
- Event Messages, page 185

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 20: Event Viewer**

1. **Add view (+) button.**
2. **View tabs.**
3. **Event filter.**
4. **Save Filter command.**
5. **Clear Filter (X) button.**
6. **Filter button.**
7. **Add/Change columns button.**
8. **View Details button (mouse-over).**
9. **Events table.**
10. **Time range (historical); Play/Pause and refresh rate (real-time).**
11. **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 181
- Configuring Custom Views, on page 181

Filter

Use this field to create filters based on event attributes. If you saved a filter, you can simply select it from the right half of the drop-down list.

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 182 and Event Filter Rules, on page 183.

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.

- **Save Filter**—Click this link to save the filter so that you can apply it again without rebuilding it. The filter is added to the right half of the drop-down list in the Filter field for all views. If you later want to delete the saved filter, click the X next to the filter in the right half of the drop-down list.

- **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.

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.

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.

**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.
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.

If you save a filter, it is available for all views. It is added to the Filter drop-down list, which is divided into two halves. The left half lists atomic filter elements, the right half lists saved filters.
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 183.

To use an existing saved filter, select it from the right half of the drop-down list.

**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.

- To save the filter for later use, click the *Save Filter* link. The filter is added to the drop-down list.

- To delete a saved filter, which removes it from the drop-down list, click the X icon button to the right of the filter in the drop-down list.

**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:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Equals. The event matches the specified value. You cannot use wildcards.</td>
</tr>
<tr>
<td>!=</td>
<td>Not equals. The event does not match the specified value. You must type in the ! (exclamation point) to build a not-equals expression.</td>
</tr>
<tr>
<td>&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;</td>
<td>Less than. The event contains a value that is less than the specified value. This operator is available for numeric values only.</td>
</tr>
</tbody>
</table>

**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.

**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 to 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.

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 186.

• 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 190.

• ASA syslog messages—These events are syslog messages generated by an ASA. For information on the possible messages, see the appropriate version of Cisco ASA 5500 Series System Log Messages available from http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html.

For information on the various columns, see Event Columns, on page 199.

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 Device > 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 traceroute commands to verify there is a path to the directory from the device.
Event Messages

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 website 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 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.

**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.

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.

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 off 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.

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%.

**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: A new Protocol Pack (Updated at %Protocol_Pack_Updated_Time%) is loaded. Pack info: %Info_String%
Explanation: An NBAR signature update was downloaded. The message indicates the update version and other information, for example:
Recommended Action: No action required.

Protocol Pack Update Failed

Message: Update of Protocol Pack Failed. Location of Protocol pack is %Protocol_Pack_Path%
Explanation: The protocol pack update failed. The location of the pack is shown in the message.
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.

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.

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.

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 %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 Update Version %App_Version%. Failed component details: %Bad_Versions%

**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 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 Device > 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 %App_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 %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 %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 %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 %App_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 %App_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 %App_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.

<table>
<thead>
<tr>
<th>Column</th>
<th>Device Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Group</td>
<td>ASA</td>
<td>The AAA group policy.</td>
</tr>
<tr>
<td>AAA Server</td>
<td>ASA</td>
<td>The AAA server that handled the user request for access and performed the authentication, authorization, or accounting.</td>
</tr>
<tr>
<td>AAA Type</td>
<td>ASA</td>
<td>The AAA type, authentication, authorization or accounting.</td>
</tr>
<tr>
<td>ACE Hash 1</td>
<td>ASA</td>
<td>The hashcode1 and hashcode2 of the access control list entry (ACE).</td>
</tr>
<tr>
<td>ACE Hash 2</td>
<td>ASA</td>
<td></td>
</tr>
<tr>
<td>ACL Name</td>
<td>ASA</td>
<td>The name or ID of the access control list (ACL).</td>
</tr>
<tr>
<td>Action</td>
<td>ASA</td>
<td>(ASA) The action performed on the flow. For example: Terminated or denied.</td>
</tr>
<tr>
<td>Application</td>
<td>CX</td>
<td>The name of the application used in the traffic flow, if any is available.</td>
</tr>
<tr>
<td>Application Type</td>
<td>CX</td>
<td>If the traffic flow matches an application, the application type to which the application belongs.</td>
</tr>
<tr>
<td>Auth Policy Name</td>
<td>CX</td>
<td>The name of the identity policy applied to the traffic flow, if any.</td>
</tr>
<tr>
<td>Auth Realm Name</td>
<td>CX</td>
<td>The name of the directory realm used in the identity policy applied to the flow.</td>
</tr>
<tr>
<td>Column</td>
<td>Device Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Auth Retry Count</td>
<td>CX</td>
<td>The number of times the user tried but failed to supply the correct username and password during active authentication.</td>
</tr>
<tr>
<td>Auth Server Name</td>
<td>CX</td>
<td>The name of the directory server used during authentication.</td>
</tr>
<tr>
<td>Auth Type</td>
<td>CX</td>
<td>The authentication mechanism used, such as basic authentication (clear text), NTLM, or Kerberos.</td>
</tr>
<tr>
<td>AVC App Behavior</td>
<td>CX</td>
<td>If an application is matched, the specific behavior of that application being used in the traffic flow, if the application has defined identifiable behaviors.</td>
</tr>
<tr>
<td>Backtrace</td>
<td>CX</td>
<td>The back trace generated from parser exception, shown in HTTP Inspection Aborted events.</td>
</tr>
<tr>
<td>Botnet Category</td>
<td>ASA</td>
<td>The category showing the reason a domain name is blacklisted, for example, botnet, Trojan, spyware, and so on.</td>
</tr>
<tr>
<td>Botnet Domain</td>
<td>ASA</td>
<td>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.</td>
</tr>
<tr>
<td>Botnet Domain</td>
<td>ASA</td>
<td>The threat level: none, very-low, low, moderate, high, and very-high.</td>
</tr>
<tr>
<td>Byte Count</td>
<td>CX</td>
<td>The number of bytes transmitted in the traffic flow.</td>
</tr>
<tr>
<td>Class Map</td>
<td>ASA</td>
<td>The class map name.</td>
</tr>
<tr>
<td>Client OS</td>
<td>CX</td>
<td>The name of the operating system running on the client for remote VPN connections.</td>
</tr>
<tr>
<td>Component</td>
<td>CX</td>
<td>In system events, the name of the component to which the event applies.</td>
</tr>
<tr>
<td>Component</td>
<td>PRSM</td>
<td></td>
</tr>
<tr>
<td>Config Version</td>
<td>CX</td>
<td>The configuration version for the policies matched by this event. The number relates directly to the version numbers shown in the change history page.</td>
</tr>
<tr>
<td>Connection Duration</td>
<td>ASA</td>
<td>The lifetime of the connection.</td>
</tr>
<tr>
<td>Connection ID</td>
<td>CX</td>
<td>An identifier for the traffic flow or connection.</td>
</tr>
<tr>
<td>Connection ID</td>
<td>ASA</td>
<td></td>
</tr>
<tr>
<td>Connection Limit</td>
<td>ASA</td>
<td>The maximum number of connections or sessions.</td>
</tr>
<tr>
<td><strong>Column</strong></td>
<td><strong>Device Type</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connection Termination Value</td>
<td>ASA</td>
<td>A factor for which the connection is terminated, for example, incorrect version or invalid payload-type.</td>
</tr>
<tr>
<td>Current Connection Count</td>
<td>ASA</td>
<td>The number of current connections.</td>
</tr>
<tr>
<td>Decryption Policy Name</td>
<td>CX</td>
<td>The name of the decryption policy that matched this flow, if any.</td>
</tr>
<tr>
<td>Deny Reason</td>
<td>CX</td>
<td>For Flow Deny or HTTP Deny events, the reason the flow was denied, such as “Flow is denied by access policy.” If the device could not establish a secure connection for TLS/SSL decryption, the reason will be “The server presented an untrusted or invalid certificate.” In these cases, you might be able to resolve the problem by uploading the certificate for the server on the <strong>Device &gt; Certificates</strong> page.</td>
</tr>
<tr>
<td>Description</td>
<td>CX, ASA</td>
<td>The event message.</td>
</tr>
<tr>
<td>Destination</td>
<td>CX, ASA</td>
<td>The IP address or host name of the destination of the traffic flow.</td>
</tr>
<tr>
<td>Destination Host</td>
<td>CX, ASA</td>
<td>The fully-qualified domain name (FQDN) of the destination if it is known.</td>
</tr>
<tr>
<td>Destination Interface</td>
<td>ASA</td>
<td>The destination interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>CX, ASA</td>
<td>The IP address of the destination of the traffic flow.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>CX, ASA</td>
<td>The port number of the destination for TCP/UDP traffic flows.</td>
</tr>
<tr>
<td>Destination Service</td>
<td>CX, ASA</td>
<td>The destination service for the flow, one of tcp/port, udp/port, icmp/message. For example, tcp/80 or icmp/echo.</td>
</tr>
<tr>
<td>Device</td>
<td>CX, ASA, PRSM</td>
<td>(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.</td>
</tr>
<tr>
<td>Direction</td>
<td>ASA</td>
<td>The direction of the traffic: inbound or outbound.</td>
</tr>
<tr>
<td>Column</td>
<td>Device Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dropped Event Count</td>
<td>CX</td>
<td>(Dropped Event messages.) The number of event messages dropped, usually due to an event rate higher than the device can handle.</td>
</tr>
<tr>
<td></td>
<td>PRSM</td>
<td></td>
</tr>
<tr>
<td>Dropped Event Type</td>
<td>CX</td>
<td>(Dropped Event messages.) The name of the type of events that were dropped.</td>
</tr>
<tr>
<td>Egress Interface</td>
<td>CX</td>
<td>The interface through which the traffic left the device.</td>
</tr>
<tr>
<td>Error Details</td>
<td>CX</td>
<td>If there are OpenSSL errors during decryption processing, the details about those errors. These messages are directly from the OpenSSL library.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, if ASA CX does not include the certificate for a site, and you have not added it to the <strong>Device &gt; Certificates</strong> page, you will see a decryption error like the following on a Flow Deny event:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>error: 14090086: SSL routines: SSL3_GET_SERVER_CERTIFICATE: certificate verify failed: Server Certificate Common Name: servername</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Event ID</td>
<td>ASA</td>
<td>A unique sequential number for each event, assigned internally.</td>
</tr>
<tr>
<td>Event Name</td>
<td>ASA</td>
<td>A user-friendly name given to the event.</td>
</tr>
<tr>
<td>Event Type</td>
<td>CX</td>
<td>The name of the event.</td>
</tr>
<tr>
<td></td>
<td>ASA</td>
<td>For ASA devices, the syslog message number. CX devices will also show an event type ID, but the number is not meaningful.</td>
</tr>
<tr>
<td>Event Type ID</td>
<td>ASA</td>
<td>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.</td>
</tr>
<tr>
<td>Hit Count</td>
<td>ASA</td>
<td>ACL Hit Count information, for example, First hit.</td>
</tr>
<tr>
<td>ICMP Code</td>
<td>ASA</td>
<td>The code of the ICMP type. For example, ICMP Type 3 and Code 0 is Net Unreachable or Code 1 is Host Unreachable.</td>
</tr>
<tr>
<td>Column</td>
<td>Device Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ICMP Type</td>
<td>ASA</td>
<td>The type of ICMP message. For example, 3 for Destination Unreachable, 8 for Echo.</td>
</tr>
<tr>
<td>Identity Source</td>
<td>CX</td>
<td>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.</td>
</tr>
<tr>
<td>Identity Type</td>
<td>CX</td>
<td>The type of identity, meaning how the user identity was acquired: active, passive, none, unknown, or guest.</td>
</tr>
<tr>
<td>Ingress Interface</td>
<td>CX</td>
<td>The interface through which the traffic entered the device.</td>
</tr>
<tr>
<td>K9 License Missing</td>
<td>CX</td>
<td>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 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.</td>
</tr>
<tr>
<td>License Limit</td>
<td>ASA</td>
<td>The maximum number of licenses.</td>
</tr>
<tr>
<td>List Name</td>
<td>ASA</td>
<td>The list that includes the domain name, administrator whitelist, blacklist, or IronPort list.</td>
</tr>
<tr>
<td>Malicious Host</td>
<td>ASA</td>
<td>The hostname of the malicious host.</td>
</tr>
<tr>
<td>Malicious IP</td>
<td>ASA</td>
<td>The IP address of malicious device.</td>
</tr>
<tr>
<td>Max Connection</td>
<td>ASA</td>
<td>The maximum number of NAT connections.</td>
</tr>
<tr>
<td>MaxEmbryonic Connection</td>
<td>ASA</td>
<td>The maximum number of embryonic connections.</td>
</tr>
<tr>
<td>NAT Destination</td>
<td>ASA</td>
<td>The translated (also called natted) destination IP address.</td>
</tr>
<tr>
<td>NAT Destination Service</td>
<td>ASA</td>
<td>The translated (or natted) destination port.</td>
</tr>
<tr>
<td>NAT Destination Host</td>
<td>ASA</td>
<td>Host name of the translated destination.</td>
</tr>
<tr>
<td>NAT Global IP</td>
<td>ASA</td>
<td>The global address. It can contain IPv4 or IPv6 addresses.</td>
</tr>
<tr>
<td>NAT Source</td>
<td>ASA</td>
<td>The translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.</td>
</tr>
<tr>
<td>Column</td>
<td>Device Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NAT Source Service</td>
<td>ASA</td>
<td>The translated (or natted) source port.</td>
</tr>
<tr>
<td>NAT Type</td>
<td>ASA</td>
<td>The type of network address translation, for example Static or Dynamic.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>CX</td>
<td>The name of the access policy that matched this traffic flow.</td>
</tr>
<tr>
<td>Policy Map</td>
<td>ASA</td>
<td>The policy map name.</td>
</tr>
<tr>
<td>Protocol</td>
<td>CX/ASA</td>
<td>The protocol of the traffic flow, such as tcp, udp, icmp, and so forth.</td>
</tr>
<tr>
<td>Protocol (Non L3)</td>
<td>ASA</td>
<td>Some non-Level-3 or -4 protocol seen in the event, for example, TACACS, RADIUS, FTP, or H245.</td>
</tr>
<tr>
<td>Reason</td>
<td>ASA</td>
<td>A rationale associated with certain events. For example, a connection tear down may have an associated reason.</td>
</tr>
<tr>
<td>Receive Time</td>
<td>CX/ASA</td>
<td>The date and time the event was received.</td>
</tr>
<tr>
<td>Reputation Score</td>
<td>CX/ASA</td>
<td>The numeric web reputation score of the destination web site.</td>
</tr>
<tr>
<td>Request Magic Type</td>
<td>CX</td>
<td>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.</td>
</tr>
<tr>
<td>Response Magic Type</td>
<td>CX</td>
<td>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.</td>
</tr>
<tr>
<td>Server Certificate Issuer</td>
<td>CX</td>
<td>An identifier of who issued the destination server certificate for TLS/SSL traffic. For example, /O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at <a href="https://www.verisign.com/rpa">https://www.verisign.com/rpa</a> (c)09/CN=VeriSign Class 3 Secure Server CA - G2.</td>
</tr>
<tr>
<td>Server Certificate Name</td>
<td>CX</td>
<td>The common name on the certificate used in TLS/SSL traffic, such as the host name of the destination server.</td>
</tr>
<tr>
<td>Severity</td>
<td>CX/ASA</td>
<td>The severity of the message, for example, Informational or Error.</td>
</tr>
<tr>
<td>Column</td>
<td>Device Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Source</td>
<td>CX ASCASA</td>
<td>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.</td>
</tr>
<tr>
<td>Source Host</td>
<td>ASCASA</td>
<td>The hostname of the source IP address.</td>
</tr>
<tr>
<td>Source Interface</td>
<td>ASCASA</td>
<td>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.</td>
</tr>
<tr>
<td>Source IP</td>
<td>CX ASCASA</td>
<td>The IP address of the source of the traffic flow.</td>
</tr>
<tr>
<td>Source Port</td>
<td>CX ASCASA</td>
<td>The port number of the source of TCP/UDP traffic flows.</td>
</tr>
<tr>
<td>SSO Server</td>
<td>ASCASA</td>
<td>The single sign-on (SSO) server name.</td>
</tr>
<tr>
<td>SSO Server Type</td>
<td>ASCASA</td>
<td>The single sign-on (SSO) server type, for example, SiteMinder.</td>
</tr>
<tr>
<td>Threat Detail</td>
<td>ASCASA</td>
<td>A detailed description of the type of threat.</td>
</tr>
<tr>
<td>Threat Type</td>
<td>CX ASCASA</td>
<td>A short description of the type of threat that caused the score to be low, or blank if there is no threat in particular.</td>
</tr>
<tr>
<td>TLS Ambiguous Destination</td>
<td>CX ASCASA</td>
<td>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.</td>
</tr>
<tr>
<td>TLS Server Cipher Suite</td>
<td>CX ASCASA</td>
<td>The cipher used in TLS/SSL traffic, for example, RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5.</td>
</tr>
<tr>
<td>TLS Flow Decrypted</td>
<td>CX ASCASA</td>
<td>Whether the traffic flow was decrypted by the TLS proxy, Yes or No.</td>
</tr>
<tr>
<td>TLS Flow Encrypted</td>
<td>CX ASCASA</td>
<td>Whether the traffic flow was TLS/SSL encrypted, Yes or No.</td>
</tr>
<tr>
<td>TLS Protocol Version</td>
<td>CX ASCASA</td>
<td>The version of TLS used in the TLS/SSL traffic flow, for example, TLSv1.</td>
</tr>
<tr>
<td>TLS Requested Domain</td>
<td>CX ASCASA</td>
<td>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.</td>
</tr>
<tr>
<td>Column</td>
<td>Device Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Tunnel Type</td>
<td>ASA</td>
<td>The VPN tunnel type.</td>
</tr>
<tr>
<td>URL</td>
<td>CX</td>
<td>For HTTP/HTTPS traffic, the URL of the destination web site.</td>
</tr>
<tr>
<td>User Realm</td>
<td>CX</td>
<td>The combination of the authentication realm and username in the format Realm\username.</td>
</tr>
<tr>
<td>Username</td>
<td>CX</td>
<td>If known, the username associated with the source of the traffic flow.</td>
</tr>
<tr>
<td></td>
<td>ASA</td>
<td>The VPN group policy.</td>
</tr>
<tr>
<td>VPN Group</td>
<td>ASA</td>
<td>The IPSec Security Parameter Index.</td>
</tr>
<tr>
<td>VPN User</td>
<td>ASA</td>
<td>The VPN username.</td>
</tr>
<tr>
<td>Web Category</td>
<td>CX</td>
<td>For traffic flows that have a destination URL, the web category to which the URL belongs.</td>
</tr>
</tbody>
</table>
PART III

Configuring Context-Aware Security

• Managing Authentication and Identity Services, page 209
• Controlling Network Access with Context-Aware Access Policies, page 231
• Managing SSL/TLS Traffic Flows, page 267
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 209
• Configuring Authentication and Identity Services, page 211

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:
  - 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 (No restrictions.)

- **OpenLDAP**—Version 2.4.21 or later. The Basic authentication method is the only available method.

### 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. Users who simply do not have a mapping because they were not required to authenticate are shown as their IP address.

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 213. 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, on page 227. 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 228.
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 218. 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 222.

**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 224. 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 232. 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 116.

**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 139. 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 177.

---

**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 **Device > 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.

There can be a single Active Directory realm. When binding to Active Directory, the first AD server in the realm is used. There can be any number of Standard LDAP 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**

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.
(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 **Device > 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**. You can create a single Active Directory realm, but you can create more than one standard LDAP realm.
     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 301.
   - **Primary Domain**—(AD only.) The fully qualified Active Directory domain name that the device should join. For example, example.com. Domains in a trust relationship with this domain are also supported.
   - **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 215. 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

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 21: Directory Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Hostname</td>
<td>The DNS name or IP address of the directory server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number used for communications with the server. The default is 389.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LDAP Login Name</td>
<td>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. If you do not specify a name, the system will attempt an anonymous bind to LDAP for querying user and group information.</td>
</tr>
</tbody>
</table>
| AD Login Name         | 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 Principal 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. |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Search Base</td>
<td>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.</td>
</tr>
<tr>
<td>Note</td>
<td>It is possible, but not necessary, that the user and group search base is the same string.</td>
</tr>
<tr>
<td>Group Attribute</td>
<td>The LDAP attribute that lists all users that belong to a group. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• member—The normal group attribute for Active Directory.</td>
</tr>
<tr>
<td></td>
<td>• uniqueMember—The normal group attribute for OpenLDAP.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Test Connection link</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Navigation Path**

- To add a directory to a realm, select Device > Directory Realm, mouse over the name of the realm to reveal related commands, and click Add New Directory.
- To edit a directory, select Device > Directory Realm, mouse over the name of the directory (within a realm) to reveal related commands, and click Edit Directory Configuration.

**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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Device &gt; Directory Realm.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Do any of the following:</td>
</tr>
</tbody>
</table>

- 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 **Policies > Policies**.
The policies are organized in policy sets, and each policy set is a separate ordered list of policies. To see the commands related to a policy set, you must mouse-over the name of the policy set. To see the commands related to an individual policy, you must mouse-over the name of the policy. You can then select the desired command.

If you need to work with an existing policy, use the filter controls to help you locate the policy you want to change.

**Step 2** Do one of the following:

- To create a new policy at the top of the list, mouse over the identity policy set name and click **Add New Policy**.
- To insert a new policy into the list, mouse over the identity policy immediate below the desired location and click **Add Above**.
- To edit an existing policy, mouse over the identity policy name and click **Edit Policy**.
- To base a new policy on a similar existing policy, mouse over the identity policy name and click **Duplicate Policy**.

A form opens with the identity policy properties. For detailed information about these properties, see **Identity Policy Properties**, on page 220.

**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 220. 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.
- For AD realms with active authentication, you can select the authentication method: basic, NTLM, Kerberos, or Advanced. Select the method supported by your server and clients; select Advanced if you support more than one method.

**Step 6** Click **Save Policy**.

**Step 7** On the Policies page, if necessary, move the policy so that it is in priority order within the policy set.
Policies within a policy set 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.

You can drag and drop policies, or use the **Move Up, Move Down** links that appear when you mouse over a policy.
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.

(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.
Authentication Type

(AD only.) If you select an option that requires or allows for active authentication, select the authentication method to use during active authentication. This setting applies for AD realms only; LDAP realms always use basic authentication. You can use the following authentication methods; select one for which your AD servers are configured:

- **NTLM** (NT LAN Manager). Supported by all Windows platforms.
- **Kerberos**. Supported for Windows XP only.
- **Basic**. This is the default. Supported on all platforms.
- **Advanced**. 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.

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 224. Otherwise, users are prompted for their directory username and password.

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.

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.)

Navigation Path

- To create an identity policy, select **Policies > Policies**, then mouse over the name of the identity policy set and click **Add New Policy**.
- To edit an identity policy, select **Policies > Policies**, then mouse over the policy and click **Edit Policy**.

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 224.

• 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
  namelf internet
  security-level 100
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.

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.
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 Active Directory 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 AD 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 AD agent setup to enable identity-aware firewall services.

**Tip**

Configuring an 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

The AD agent is separate software that you must install in your network. You must configure it to work with the Active Directory servers and with the network devices that are its clients. Before completing this task, install and configure the AD agent software.


You must add the CX device as a client, which you can do before or after you complete this procedure. Keep in mind that the RADIUS shared secret configured for the CX client on the AD agent and the one configure here must be the same. The command to create the client on the AD agent is:

```
adacfg client create -n client-nickname -ip mgmt_IP -secret RADIUS_secret
```

where
• `client_nickname` is a name used by the AD agent to refer to the CX client.
• `mgmt_IP` is either the IP address of the CX management interface, or the subnet that contains the address, for example, 10.100.10.1 or 10.100.10.0/24.
• `RADIUS_secret` is a RADIUS shared secret that you will also configure in the CX device. This secret encrypts and protects communications between the CX device and the AD agent.

You might find the following AD agent commands useful for verifying or troubleshooting the configuration:

• `adacfg dc list`, to verify the connection between the AD agent and AD server.
• `adacfg cache list`, to verify that the agent is getting user-to-IP mappings.
• `adacfg client list`, to list the clients currently served by the AD agent.

### Procedure

**Step 1** Select Device > AD Agent.

**Step 2** Enter the following information:

- **Hostname or IP**—The DNS name or IP address of the AD agent server.
- **Password**—The RADIUS shared secret that is configured on the AD agent for use with this client device.

**Step 3** Click Test to check whether the AD 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 AD agent.

(Multiple Device mode.) The connectivity is checked between all managed CX devices and the AD agent.

**Step 4** Click Save to save your changes.

### What to Do Next

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 AD 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.

### Configuring Authentication Settings

You can configure authentication settings related to how your identity policies function.

**Procedure**

**Step 1** Select Device > Authentication.

**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.

**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 231
- Notifying Users of Blocking Policies, page 237
- URL and Application Filtering, page 242
- Configuring Signature and Engine Updates, page 263

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.

• 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.

**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 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 Policies > Policies.
The policies are organized in policy sets, and each policy set is a separate ordered list of policies. To see the commands related to a policy set, you must mouse-over the name of the policy set. To see the commands related to an individual policy, you must mouse-over the name of the policy. You can then select the desired command.

If you need to work with an existing policy, use the filter controls to help you locate the policy you want to change.

Step 2  Do one of the following:

- To create a new policy at the top of the list, mouse over the access policy set name and click Add New Policy.
- To insert a new policy into the list, mouse over the access policy immediate below the desired location and click Add Above.
- To edit an existing policy, mouse over the access policy name and click Edit Policy.
- To base a new policy on a similar existing policy, mouse over the access policy name and click Duplicate Policy.

A form opens with the access policy properties. For detailed information about these properties, see Context-Aware Access Policy Properties, on page 234.

Step 3  Select the policy action to apply to matching traffic, Allow or Deny.
You can also modify the following properties, but the defaults are correct for most policies:

- Eventing: On/Off—Whether to generate events for this policy. You must enable eventing for traffic flows that match this policy to generate events in Event Viewer or data in dashboards. Eventing is enabled by default.
- Capture Packets: On/Off—Whether to capture packets that match this policy. All packets are captured, whether allowed or denied. This setting works only if all traffic match criteria are Any or are Layer 3/Layer 4 only (that is, network and service objects, no other object types).

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 entire application types (which apply the same policies to all specific applications that are of that type), or you can control specific applications, including application services that you define yourself. When you specify applications or types, you can control access without limiting the control to specific ports.
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.

**Note**

Step 5  (Optional) Unless the policy action is Deny, you can also configure the following profiles to selectively disallow actions:

- **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. The pre-defined system object Default Reputation Profile implements the recommended blocking of sites with reputation scores from -10 to -6.

Step 6  Click Save Policy.

Step 7  On the Policies page, if necessary, move the policy so that it is in priority order within the policy set. Policies within a policy set 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.

You can drag and drop policies, or use the Move Up, Move Down links that appear when you mouse over a policy.

**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: Allow/Deny**

Whether the policy allows or denies network access. Denied traffic is dropped.
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 307.

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 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.
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:

- **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. Use the pre-defined system object, **Default Reputation Profile**, to implement the recommended policy, which drops any traffic whose reputation is -6 or lower.

Note

You can create new profile objects by clicking **Create New Profile**. The process of creating, editing, and viewing profiles is the same as doing those actions with other policy objects, as described above.

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.)

Navigation Path

- To create a context-aware access policy, select **Policies > Policies**, then mouse over the name of the access policy set and click **Add New Policy**.
- To edit a context-aware access policy, select **Policies > Policies**, then mouse over the policy and click **Edit Policy**.

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 website. 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.
- If you deny access based on IP address, user name, or user group membership, no notifications are sent.
- 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 access to a URL. 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 21: 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:

- 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.
(2) Preview Draft
Click this button to see how the message you are editing will appear to users. Sample values are used for variables.

(3) 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.

(4) 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.

(5) 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.

(6) 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}}.
- Message body—Type in the message body box. Use the Tab/Reverse Tab key to add or remove indents.

Editing End User Notifications
You can edit the pages shown to users when you deny access to a site. There are different pages for each denial reason.
Notifying Users of Blocking Policies

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 239.

**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.

- 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.

**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.

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Example</th>
<th>Description</th>
<th>Notification Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>application_behavior</td>
<td>Tweet</td>
<td>The application behavior, which is not available for all applications.</td>
<td>Application</td>
</tr>
<tr>
<td>application_name</td>
<td>Twitter</td>
<td>The name of the application.</td>
<td>Application</td>
</tr>
<tr>
<td>application_type</td>
<td>Social Networking</td>
<td>The general type of application.</td>
<td>Application</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Example</th>
<th>Description</th>
<th>Notification Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>blocking_reason</td>
<td>Application</td>
<td>The reason access was blocked.</td>
<td>All</td>
</tr>
<tr>
<td>destination_ip</td>
<td>10.100.10.10</td>
<td>The IP address of the destination site.</td>
<td>All</td>
</tr>
<tr>
<td>destination_port</td>
<td>80</td>
<td>The TCP/UDP port on the destination site.</td>
<td>All</td>
</tr>
<tr>
<td>file_type</td>
<td>audio</td>
<td>The media, or MIME, type for the file.</td>
<td>File type</td>
</tr>
<tr>
<td>flow_id</td>
<td>384</td>
<td>The identifier given to the traffic flow by the firewall.</td>
<td>All</td>
</tr>
<tr>
<td>full_url</td>
<td><a href="http://www.example.com/index/">http://www.example.com/index/</a></td>
<td>The URL of the destination, including the full path.</td>
<td>All</td>
</tr>
<tr>
<td>source_ip</td>
<td>10.100.10.10</td>
<td>The IP address of the traffic source.</td>
<td>All</td>
</tr>
<tr>
<td>source_port</td>
<td>80</td>
<td>The TCP/UDP port of the traffic source.</td>
<td>All</td>
</tr>
<tr>
<td>time</td>
<td>02:50:55pm UTC</td>
<td>When the traffic flow occurred.</td>
<td>All</td>
</tr>
<tr>
<td>threat_type</td>
<td>Phishing</td>
<td>The threat type associated with the low reputation site. The reputation must be -6 or below to have a threat type.</td>
<td>Web reputation</td>
</tr>
<tr>
<td>uploads_or_downloads</td>
<td>upload</td>
<td>Whether the file transfer was an upload (source to destination) or download (destination to source).</td>
<td>File type</td>
</tr>
<tr>
<td>web_category</td>
<td>Social Networking</td>
<td>The general web category to which the destination URL belongs.</td>
<td>URL filtering</td>
</tr>
<tr>
<td>web_reputation</td>
<td>-6.7</td>
<td>The web reputation of the destination site, from -10 (worst) to 10 (best).</td>
<td>Web reputation</td>
</tr>
</tbody>
</table>

**User Guide for ASA CX and Cisco Prime Security Manager 9.1**

242
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.

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.
- 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.
Filtering Criteria

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.

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 Policies > 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 websites, or you can decrypt all HTTPS requests for web-based email websites.

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 website 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.

**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
  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.

**URL Category Descriptions**

The following list describes the URL categories available at the time of this release. URL category updates can add, remove, merge, or divide categories.

**Adult**

Directed at adults, but not necessarily pornographic. May include adult clubs (strip clubs, swingers clubs, escort services, strippers); general information about sex, non-pornographic in nature; genital piercing; adult products or greeting cards; information about sex not in the context of health or disease.

Examples:
- www.adultentertainmentexpo.com
- www.adultnetline.com

**Advertisements**

Banner and pop-up advertisements that often accompany a web page; other advertising websites that provide advertisement content. Advertising services and sales are classified as "Business and Industry."

Examples:
- www.adforce.com
- www.doubleclick.com

**Alcohol**

Alcohol as a pleasurable activity; beer and wine making, cocktail recipes; liquor sellers, wineries, vineyards, breweries, alcohol distributors. Alcohol addiction is classified as "Health and Nutrition." Bars and restaurants are classified as "Dining and Drinking."

Examples:
- www.samueladams.com
- www.whisky.com

**Arts**

Galleries and exhibitions; artists and art; photography; literature and books; performing arts and theater; musicals; ballet; museums; design; architecture. Cinema and television are classified as "Entertainment."

Examples:
- www.moma.org
- www.nga.gov
Astrology
Astrology; horoscope; fortune telling; numerology; psychic advice; tarot.
Examples:
• www.astro.com
• www.astrology.com

Auctions
Online and offline auctions, auction houses, and classified advertisements.
Examples:
• www.craigslist.org
• www.ebay.com

Business and Industry
Marketing, commerce, corporations, business practices, workforce, human resources, transportation, payroll, security and venture capital; office supplies; industrial equipment (process equipment), machines and mechanical systems; heating equipment, cooling equipment; materials handling equipment; packaging equipment; manufacturing: solids handling, metal fabrication, construction and building; passenger transportation; commerce; industrial design; construction, building materials; shipping and freight (freight services, trucking, freight forwarders, truckload carriers, freight and transportation brokers, expedited services, load and freight matching, track and trace, rail shipping, ocean shipping, road feeder services, moving and storage).
Examples:
• www.freightcenter.com
• www.staples.com

Chat and Instant Messaging
Web-based instant messaging and chat rooms.
Examples:
• www.icq.com
• www.meebo.com

Cheating and Plagiarism
Promoting cheating and selling written work, such as term papers, for plagiarism.
Examples:
• www.bestessays.com
• www.superiorpapers.com
Child Abuse Content
Worldwide illegal child sexual abuse content.

Computer Security
Offering security products and services for corporate and home users.
Examples:
• www.computersecurity.com
• www.symantec.com

Computers and Internet
Information about computers and software, such as hardware, software, software support; information for software engineers, programming and networking; website design; the web and Internet in general; computer science; computer graphics and clipart. "Freeware and Shareware" is a separate category.
Examples:
• www.xml.com
• www.w3.org

Dating
Dating, online personals, matrimonial agencies.
Examples:
• www.eharmony.com
• www.match.com

Digital Postcards
Enabling sending of digital postcards and e-cards.
Examples:
• www.all-yours.com
• www.e-cards.com

Dining and Drinking
Eating and drinking establishments; restaurants, bars, taverns, and pubs; restaurant guides and reviews.
Examples:
• www.hideawaybrewpub.com
• www.restaurantrow.com
Dynamic and Residential

IP addresses of broadband links that usually indicates users attempting to access their home network, for example for a remote session to a home computer.

Examples:

- http://109.60.192.55
- http://dynalink.co.jp
- http://ipads1.net

Education

Education-related, such as schools, colleges, universities, teaching materials, and teachers' resources; technical and vocational training; online training; education issues and policies; financial aid; school funding; standards and testing.

Examples:

- www.education.com
- www.greatschools.org

Entertainment

Details or discussion of films; music and bands; television; celebrities and fan websites; entertainment news; celebrity gossip; entertainment venues. Compare with the "Arts" category.

Examples:

- www.eonline.com
- www.ew.com

Extreme

Material of a sexually violent or criminal nature; violence and violent behavior; tasteless, often gory photographs, such as autopsy photos; photos of crime scenes, crime and accident victims; excessive obscene material; shock websites.

Examples:

- www.car-accidents.com
- www.crime-scene-photos.com

Fashion

Clothing and fashion; hair salons; cosmetics; accessories; jewelry; perfume; pictures and text relating to body modification; tattoos and piercing; modeling agencies. Dermatological products are classified as "Health and Nutrition."

Examples:

- www.fashion.net
- www.findabeautysalon.com
File Transfer Services

File-transfer services with the primary purpose of providing download services and hosted file sharing.

Examples:
- www.rapidshare.com
- www.yousendit.com

Filter Avoidance

Promoting and aiding undetectable and anonymous web usage, including cgi, php and glype anonymous proxy services.

Examples:
- www.bypassschoolfilter.com
- www.filterbypass.com

Finance

Primarily financial in nature, such as accounting practices and accountants, taxation, taxes, banking, insurance, investing, the national economy, personal finance involving insurance of all types, credit cards, retirement and estate planning, loans, mortgages. Stock and shares are classified as “Online Trading.”

Examples:
- finance.yahoo.com
- www.bankofamerica.com

Freeware and Shareware

Providing downloads of free and shareware software.

Examples:
- www.freewarehome.com
- www.shareware.com

Gambling

Casinos and online gambling; bookmakers and odds; gambling advice; competitive racing in a gambling context; sports booking; sports gambling; services for spread betting on stocks and shares. Websites dealing with gambling addiction are classified as “Health and Nutrition.” Government-run lotteries are classified as “Lotteries.”

Examples:
- www.888.com
- www.gambling.com
Games

Various card games, board games, word games, and video games; combat games; sports games; downloadable games; game reviews; cheat sheets; computer games and Internet games, such as role-playing games.

Examples:

- www.games.com
- www.shockwave.com

Government and Law

Government websites; foreign relations; news and information relating to government and elections; information relating to the field of law, such as attorneys, law firms, law publications, legal reference material, courts, dockets, and legal associations; legislation and court decisions; civil rights issues; immigration; patents and copyrights; information relating to law enforcement and correctional systems; crime reporting, law enforcement, and crime statistics; military, such as the armed forces, military bases, military organizations; anti-terrorism.

Examples:

- www.usa.gov
- www.law.com

Hacking

Discussing ways to bypass the security of websites, software, and computers.

Examples:

- www.hackthissite.org
- www.gohacking.com

Hate Speech

Websites promoting hatred, intolerance, or discrimination on the basis of social group, color, religion, sexual orientation, disability, class, ethnicity, nationality, age, gender, gender identity; sites promoting racism; sexism; racist theology; hate music; neo-Nazi organizations; supremacism; Holocaust denial.

Examples:

- www.kkk.com
- www.nazi.org
Health and Nutrition

Health care; diseases and disabilities; medical care; hospitals; doctors; medicinal drugs; mental health; psychiatry; pharmacology; exercise and fitness; physical disabilities; vitamins and supplements; sex in the context of health (disease and health care); tobacco use, alcohol use, drug use, and gambling in the context of health (disease and health care); food in general; food and beverage; cooking and recipes; food and nutrition, health, and dieting; cooking, including recipe and culinary websites; alternative medicine.

Examples:

• www.health.com
• www.webmd.com

Humor

Jokes, sketches, comics and other humorous content. Adult humor likely to offend is classified as "Adult."

Examples:

• www.humor.com
• www.jokes.com

Illegal Activities

Promoting crime, such as stealing, fraud, illegally accessing telephone networks; computer viruses; terrorism, bombs, and anarchy; websites depicting murder and suicide as well as explaining ways to commit them.

Examples:

• www.ekran.com
• www.thedisease.net

Illegal Downloads

Providing the ability to download software or other materials, serial numbers, key generators, and tools for bypassing software protection in violation of copyright agreements. Torrents are classified as "Peer File Transfer."

Examples:

• www.keygenguru.com
• www.zcrack.com

Illegal Drugs

Information about recreational drugs, drug paraphernalia, drug purchase and manufacture.

Examples:

• www.cocaine.org
• www.hightimes.com
Infrastructure and Content Delivery Networks
Content delivery infrastructure and dynamically generated content; websites that cannot be classified more specifically because they are secured or otherwise difficult to classify.

Examples:
- www.akamai.net
- www.webstat.net

Internet Telephony
Telephonic services using the Internet.

Examples:
- www.evaphone.com
- www.skype.com

Job Search
Career advice; resume writing and interviewing skills; job placement services; job databanks; permanent and temporary employment agencies; employer websites.

Examples:
- www.careerbuilder.com
- www.monster.com

Lingerie and Swimsuits
Intimate apparel and swimwear, especially when modeled.

Examples:
- www.swimsuits.com
- www.victoriassecret.com

Lotteries
Sweepstakes, contests and state-sponsored lotteries.

Examples:
- www.calottery.com
- www.flalottery.com
Mobile Phones
Short Message Services (SMS); ringtones and mobile phone downloads. Cellular carrier websites are included in the “Business and Industry” category.
Examples:
- www.cbfSMS.com
- www.zedge.net

Nature
Natural resources; ecology and conservation; forests; wilderness; plants; flowers; forest conservation; forest, wilderness, and forestry practices; forest management (reforestation, forest protection, conservation, harvesting, forest health, thinning, and prescribed burning); agricultural practices (agriculture, gardening, horticulture, landscaping, planting, weed control, irrigation, pruning, and harvesting); pollution issues (air quality, hazardous waste, pollution prevention, recycling, waste management, water quality, and the environmental cleanup industry); animals, pets, livestock, and zoology; biology; botany.
Examples:
- www.enature.com
- www.nature.org

News
News; headlines; newspapers; television stations; magazines; weather; ski conditions.
Examples:
- www.cnn.com
- news.bbc.co.uk

Non-governmental Organization
Non-governmental organizations such as clubs, lobbies, communities, non-profit organizations and labor unions.
Examples:
- www.panda.org
- www.unions.org

Non-sexual Nudity
Nudism and nudity; naturism; nudist camps; artistic nudes.
Examples:
- www.artenuda.com
- www.naturistsociety.com
Online Communities

Affinity groups; special interest groups; web newsgroups; message boards. Excludes websites classified as "Professional Networking" or "Social Networking."

Examples:
- www.igda.com
- www.ieee.com

Online Storage and Backup

Offsite and peer-to-peer storage for backup, sharing, and hosting.

Examples:
- www.adrive.com
- www.dropbox.com

Online Trading

Online brokerages; websites that enable the user to trade stocks online; information relating to the stock market, stocks, bonds, mutual funds, brokers, stock analysis and commentary, stock screens, stock charts, IPOs, stock splits. Services for spread betting on stocks and shares are classified as "Gambling." Other financial services are classified as "Finance."

Examples:
- www.tdameritrade.com
- www.scottrade.com

Organizational Email

Websites used to access business email (often via Outlook Web Access).

Parked Domains

Websites that monetize traffic from the domain using paid listings from an ad network, or are owned by "squatters" hoping to sell the domain name for a profit. These also include fake search websites which return paid ad links.

Examples:
- www.domainzaar.com
- www.parked.com

Peer File Transfer

Peer-to-peer file request websites. This does not track the file transfers themselves.

Examples:
- www.bittorrent.com
- www.limewire.com
**Personal Sites**

Websites about and from private individuals; personal homepage servers; websites with personal contents; personal blogs with no particular theme.

Examples:

- www.karymullis.com
- www.stallman.org

**Photo Searches and Images**

Facilitating the storing and searching for, images, photographs, and clip-art.

Examples:

- www.flickr.com
- www.photobucket.com

**Politics**

Websites of politicians; political parties; news and information on politics, elections, democracy, and voting.

Examples:

- www.politics.com
- www.thisnation.com

**Pornography**

Sexually explicit text or depictions. Includes explicit anime and cartoons; general explicit depictions; other fetish material; explicit chat rooms; sex simulators; strip poker; adult movies; lewd art; web-based explicit email.

Examples:

- www.redtube.com
- www.youporn.com

**Professional Networking**

Social networking for the purpose of career or professional development. See also “Social Networking.”

Examples:

- www.linkedin.com
- www.europeanpwn.com
Real Estate
Information that would support the search for real estate; office and commercial space; real estate listings, such as rentals, apartments, and homes; house building.
Examples:
• www.realtor.com
• www.zillow.com

Reference
City and state guides; maps, time; reference sources; dictionaries; libraries.
Examples:
• www.wikipedia.org
• www.yellowpages.com

Religion
Religious content, information about religions; religious communities.
Examples:
• www.religionfacts.com
• www.religioustolerance.org

SaaS and B2B
Web portals for online business services; online meetings.
Examples:
• www.netsuite.com
• www.salesforce.com

Safe for Kids
Directed at, and specifically approved for, young children.
Examples:
• kids.discovery.com
• www.nickjr.com
Science and Technology
Science and technology, such as aerospace, electronics, engineering, mathematics, and other similar subjects; space exploration; meteorology; geography; environment; energy (fossil, nuclear, renewable); communications (telephones, telecommunications).

Examples:
- www.physorg.com
- www.science.gov

Search Engines and Portals
Search engines and other initial points of access to information on the Internet.

Examples:
- www.bing.com
- www.google.com

Sex Education
Factual websites dealing with sex; sexual health; contraception; pregnancy.

Examples:
- www.avert.org
- www.scarleteen.com

Shopping
Bartering; online purchasing; coupons and free offers; general office supplies; online catalogs; online malls.

Examples:
- www.amazon.com
- www.shopping.com

Social Networking
Social networking. See also "Professional Networking."

Examples:
- www.facebook.com
- www.twitter.com
Social Science

Sciences and history related to society; archaeology; anthropology; cultural studies; history; linguistics; geography; philosophy; psychology; women's studies.

Examples:
- www.archaeology.com
- www.anthropology.com

Society and Culture

Family and relationships; ethnicity; social organizations; genealogy; seniors; child-care.

Examples:
- www.childcare.gov
- www.familysearch.org

Software Updates

Websites that host updates for software packages.

Examples:
- www.softwarepatch.com
- www.versiontracker.com

Sports and Recreation

All sports, professional and amateur; recreational activities; fishing; fantasy sports; public parks; amusement parks; water parks; theme parks; zoos and aquariums; spas.

Examples:
- www.espn.com
- www.recreation.gov

Streaming Audio

Real-time streaming audio content including Internet radio and audio feeds.

Examples:
- www.live-radio.net
- www.shoutcast.com
**Streaming Video**

Real-time streaming video including Internet television, web casts, and video sharing.

Examples:

- www.hulu.com
- www.youtube.com

**Tobacco**

Pro-tobacco websites; tobacco manufacturers; pipes and smoking products (not marketed for illegal drug use). Tobacco addiction is classified as "Health and Nutrition."

Examples:

- www.bat.com
- www.tobacco.org

**Transportation**

Personal transportation; information about cars and motorcycles; shopping for new and used cars and motorcycles; car clubs; boats, airplanes, recreational vehicles (RVs), and other similar items. Note, car and motorcycle racing is classified as "Sports and Recreation."

Examples:

- www.cars.com
- www.motorcycles.com

**Travel**

Business and personal travel; travel information; travel resources; travel agents; vacation packages; cruises; lodging and accommodation; travel transportation; flight booking; airfares; car rental; vacation homes.

Examples:

- www.expedia.com
- www.lonelyplanet.com

**Weapons**

Information relating to the purchase or use of conventional weapons such as gun sellers, gun auctions, gun classified ads, gun accessories, gun shows, and gun training; general information about guns; other weapons and graphic hunting sites may be included. Government military websites are classified as "Government and Law."

Examples:

- www.coldsteel.com
- www.gunbroker.com
Web Hosting

Website hosting; bandwidth services.
Examples:
- www.bluehost.com
- www.godaddy.com

Web Page Translation

Translation of web pages between languages.
Examples:
- babelfish.yahoo.com
- translate.google.com

Web-based Email

Public web-based email services. Websites enabling individuals to access their company or organization's email service are classified as "Organizational Email."
Examples:
- mail.yahoo.com
- www.hotmail.com

Configuring Signature and Engine Updates

Applications and application types, URL categories, and web reputation are defined by signatures and applied by Security Application Scanner (SAS) engines. Updates to these features are made available frequently on an update server. You can configure an update window for SAS engine upgrades and an HTTP proxy to use for obtaining all 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, or application types.
- Changes to existing URL categories, applications, application behaviors, or application types. 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 website is categorized can alter how traffic for the application, or traffic to the website, 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 Policies > 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 Device > Updates.
The Updates page shows the various signature packages and engines 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. Packages include the following:

• AVC—Application Visibility and Control. The components in this package define the applications and application types for which you can configure policies.
• WBRS—Metascan web reputation filters. The components in this package define web reputation scores and URL categories.
• SAS—Security Application Scanners. The SAS engines evaluate traffic to determine the application, web category, or web reputation associated with the destination.

Step 2 Select I want to > Edit Settings.
Step 3 Configure the following settings as desired:

• Updates—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 still checked every 5 minutes throughout the day for signature updates. However, engine and telemetry client updates are checked 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.
  Note The time window is limited to a single day. You cannot specify a time window that straddles midnight.
  * Never check—The update server is never checked. Use this setting temporarily or if you decide to not purchase feature licenses.
• **HTTP Proxy Server: Enable/Disable**—The proxy server through which updates will be downloaded. If you do not configure a proxy server, updates are obtained through the management interface, so you need to ensure there is a route to the Internet from your management network. To configure a proxy server, configure the following properties:

  ◦ **HTTP Proxy Server: Enable**.

  ◦ **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.

**Step 4** Click Save.

---

**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. If you configure an update window for engine updates, you might find that a newly downloaded signature update cannot be installed immediately. 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 267
- Configuring SSL/TLS Decryption, page 272
- Troubleshooting TLS/SSL Decryption, page 285

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.
- If the traffic is HTTPS, it is inspected (HTTPS traffic only is inspected, other traffic types are not 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 277.

---

**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 traffic, ASA CX does not inspect it. 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 are applied and allow or drop decisions are based only on the exposed characteristics of the traffic flow, such as network (IP address), service (ports, TCP/UDP), and user identity policy objects. For URL objects, the domain name only is matched, which can also result in a web category match, but you cannot specify differentiated behavior for different resources on the same web server or domain. The encrypted traffic flow will never match specifications that include application or user agent policy objects.

In addition, any profiles that you apply to allowed traffic flows are ignored for encrypted traffic. For example, file filtering profiles that prevent certain types of file uploads or downloads, or web reputation profiles that drop traffic from low reputation web sites, cannot be applied. The entire encrypted flow is allowed because the content of the encrypted flow is not known.

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.

• **Block low reputation sources**—You can use web reputation profiles to selectively block content hosted from low reputation sources, protecting users while they visit otherwise acceptable web sites.

• **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.
Decrypted Traffic Flow

Encrypted traffic flows that are decrypted are handled using the following process.

**Figure 22: 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 23: 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.

  **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, do not decrypt is the decision.

- 5, 6—CX device terminates the traffic flow separately with the client and server.

- 7—The client retries the connection.
The CX device remembers that this flow should not be decrypted and allows it to bypass decryption processing and make its own connection to the server. The flow is not inspected.

**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.

- Although any type of encrypted traffic can be decrypted, HTTPS is the only protocol that is subsequently inspected after decryption.

- 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 283**. You can also try relaxing decryption processing by selecting **Deny Transactions to Servers; If the Secure Sessions Handshake Fails: Off** in the decryption settings.

**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 273.

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 279. 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 283.

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 277. 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 Device > Decryption.

**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 274.

**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 276.

**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 277.

The following procedure explains how to generate or upload the certificate required by decryption policies.

**Procedure**

**Step 1**

Select **Device > Decryption**. Ensure that **Enable Decryption Policies: On** is selected.

**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.

• **PrivateKey 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:

```bash
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:

```bash
openssl rsa -inform DER -in key_in_DER -outform PEM -out out_file_name
```

For DSA keys, use the following command:

```bash
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 website’s security certificate. Usually, the error message says that the website’s security certificate was not issued by a trusted certificate authority or the website was certified by an unknown authority, 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.
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.

a) Select Device > Decryption.

b) 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.

a) In Firefox, select Tools > Options.

b) Select Advanced, then select the Encryption tab.

c) Click View Certificates to open the Certificate Manager.

d) Select the Authorities tab.

e) Click Import, locate and select the downloaded file (ca.crt.pem), and click OK. The Downloading Certificate dialog box opens.

f) 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 Flow Deny events in Event Viewer where the Deny Reason column says "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.

---

**Procedure**

**Step 1** Select **Device > 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 based on the inspected content of the traffic flow, such as application, URL category, web reputation, and so forth.

---

**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 **Policies > Policies**.

The policies are organized in policy sets, and each policy set is a separate ordered list of policies. To see the commands related to a policy set, you must mouse-over the name of the policy set. To see the commands related to an individual policy, you must mouse-over the name of the policy. You can then select the desired command.

If you need to work with an existing policy, use the filter controls to help you locate the policy you want to change.
Step 2  Do one of the following:

- To create a new policy at the top of the list, mouse over the decryption policy set name and click **Add New Policy**.
- To insert a new policy into the list, mouse over the decryption policy immediate below the desired location and click **Add Above**.
- To edit an existing policy, mouse over the decryption policy name and click **Edit Policy**.
- To base a new policy on a similar existing policy, mouse over the decryption policy name and click **Duplicate Policy**.

A form opens with the decryption policy properties. For detailed information about these properties, see **Decryption Policy Properties**, on page 280.

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  Click **Save Policy**.

Step 6  On the Policies page, if necessary, move the policy so that it is in priority order within the policy set. Policies within a policy set 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.

You can drag and drop policies, or use the **Move Up, Move Down** links that appear when you mouse over a policy.

---

**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 based on the inspected content of the traffic flow, such as application, URL category, web reputation, and so forth.

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.

(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 websites, 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.

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.)

Navigation Path

- To create a decryption policy, select **Policies > Policies**, then mouse over the name of the decryption policy set and click **Add New Policy**.

- To edit a decryption policy, select **Policies > Policies**, then mouse over the policy and click **Edit Policy**.
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 Complete 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 Event Viewer, look for Flow Deny events where the Deny Reason column says "The server presented an untrusted or invalid certificate." In these cases, you might be able to resolve the problem by uploading a supplemental certificate from the untrusted CA or server (select Device > 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 Flow Deny events where the deny reason indicates 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.
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 **Policies** > **Policies**.

**Step 2** Mouse over the decryption policy set and click **Add New Policy**.

**Step 3** Enter a name for the policy, for example, Bypass AIM.

**Step 4** Create and select the object:

a) Click the **Create New Object** link beneath the **Destination** field.

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 Flow Deny events in Event Viewer for the user’s access attempt. The Deny Reason column should explain why the flow was denied.

If the flow was denied by policy, then the flow matches an access policy that is denying it. If instead the flow should be allowed, adjust your access policies.

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 Device > 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 Flow Deny events in Event Viewer for the user’s access attempt. The Deny Reason column should explain why the flow was denied.

If the deny reason indicates 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. You can also relax this restriction and allow these transactions by selecting Deny Transactions to Servers; If the Secure Sessions Handshake Fails: Off in the decryption settings.

Applications that prompt for a client certificate during the connection, such as iTunes, can also experience handshake failures.

Also consider TLS Complete events for the flow that show raw OpenSSL errors in the Error Details field.

**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

- Device Logging, page 291
Device Logging

The ASA logging page lets you enable system logging, configure logging options, and define the syslog servers to which messages are sent.

- Logging Configuration, page 291
- Syslog Servers, page 292

Logging Configuration

Use the Logging Configuration screen to enable and configure system logging on a security appliance.

Procedure

**Step 1** Open the device configuration page by selecting Device > Devices, mousing over the device and clicking Device Configuration.

**Step 2** Click Logging Configuration in the Device Logging Configuration section of the Device Configuration screen. The Logging Configuration screen is displayed.

**Step 3** Define or alter the logging parameters, as necessary:

- **Logging** – Click this switch to turn logging on the security appliance On or Off.
  
  If you turn off logging on the ASA, the current settings are retained.

- **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 syslog messages that the appliance can hold in its queue before sending them to the output destination; the default value is 512.

Valid values are from 0 to 8192 messages, depending on device. If the Logging Queue is set to zero, the queue is the maximum configurable size for the device. For the ASA 5505, the maximum is 1024; for the ASA 5510 it is 2048; for all other ASAs, the maximum is 8192 messages.

• **Send as EMBLEM Format** – Use this switch to 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. See [Syslog Servers, on page 292](#) for more information.

• **Allow user traffic when TCP server 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.

• **Send debug as syslog** – 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.

  **Step 4** Click **Save** to save the updated logging-configuration information. You are returned to the device-configuration screen.

---

**Syslog Servers**

The Syslog Servers screen lets you specify one or more syslog servers to which the selected security appliance will send syslog messages. By directing syslog records generated by a security appliance to a syslog server, you can process and study the records.
Creating and Editing Syslog Server Definitions

You can add and edit syslog server definitions as part of a device configuration. These definitions specify target servers to which the security appliance sends syslog messages. (See Deleting A Syslog Server Definition, on page 294 for information about removing a definition.)

There is a limit of four syslog servers per context.

Procedure

Step 1 Open the device configuration page by selecting Device > Devices, mousing over the device and clicking Device Configuration.

Step 2 Click Syslog Servers in the Device Logging Configuration section of the Device Configuration screen. The list of currently configured syslog servers is displayed.

Step 3 Do one of the following:

• To add a new syslog target server, click the Add button to open the new syslog server-configuration screen.

• To edit an existing syslog target, simply click anywhere in the desired server entry to open the syslog server-configuration screen, which displays the current parameters for that server.

Step 4 Define or alter the following Syslog Server parameters, as necessary:

• Interface – Choose the interface on which the syslog server is contacted—this list displays all available interfaces.

• IP Address – Enter the IP address of the syslog server.

• Protocol – Choose a packet-transmission protocol—UDP or TCP—for communication with the syslog server; UDP is the default. TCP ports work only with a security appliance syslog server.

  Note You must choose UDP if you intend to use the EMBLEM format.

• Port – Enter the number of the port from which the security appliance sends either UDP or TCP syslog messages. This port must be the same port on which the syslog server listens.

The default UDP and TCP ports are:

  • 514 (UDP).
  • 1470 (TCP) – TCP ports work only with a security appliance syslog server.
• **Send Syslog in EMBLEM Format** – Check this box to generate syslog messages using Cisco’s EMBLEM format, which is the format used by Cisco IOS routers and switches.

  **Note**  
  To use this option, you must choose UDP as the Protocol.

• **Enable Secure Syslog Using SSL/TLS** – Check this box to secure the connection to the syslog server using SSL/TLS over TCP, and to encrypt the syslog message content.

  A secure logging connection can only be established with a SSL/TLS-capable syslog server. If a SSL/TLS connection cannot be established, all new connections will be denied.

  **Note**  
  To use this option, you must choose TCP as the Protocol.

**Step 5**  
Click **Save** to save the new or updated syslog server definition. You are returned to the list of syslog servers.

---

### Deleting A Syslog Server Definition

You can delete a syslog server definition from a device configuration.

See [Creating and Editing Syslog Server Definitions](#) on page 293 for information about adding and editing definitions.

**Procedure**

**Step 1**  
Click **Syslog Servers** in the Device Logging Configuration section of the Device Configuration screen. (See [Working with the Device Configuration](#) on page 88 for information about accessing the Device Configuration screen.) The list of currently configured syslog servers is displayed.

**Step 2**  
Click anywhere in the desired server entry to open that syslog server-configuration screen.

**Step 3**  
Click the **Delete** button to discard this syslog server definition. After you confirm the deletion, you are returned to the list of syslog servers.
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 295
- Installing a Server Certificate, page 303
- Basic Troubleshooting, page 306
- Maintaining the System, page 314

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 299.
  - **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 301.

• **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 296.

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>
<thead>
<tr>
<th>Menu</th>
<th>Role Administrator</th>
<th>Security Administrator</th>
<th>System Administrator</th>
<th>Reporting Administrator</th>
<th>Help Desk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard, all items</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Menu</td>
<td>Role</td>
<td>Administrator</td>
<td>Security Administrator</td>
<td>System Administrator</td>
<td>Reporting Administrator</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>------</td>
<td>---------------</td>
<td>-------------------------</td>
<td>----------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Events</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Policies &gt; Policies</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Policies &gt; Objects</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Policies &gt; Applications</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Policies &gt; Device Groups</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
</tr>
<tr>
<td>Device &gt; Devices (including the device configuration page)</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
</tr>
<tr>
<td>Device &gt; Directory Realm</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
</tr>
<tr>
<td>Device &gt; AD Agent</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Device &gt; Authentication</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Device &gt; Decryption</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Device &gt; Certificates</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Device &gt; Updates</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
</tr>
<tr>
<td>Device &gt; Packet Capture</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Device &gt; Monitor-only Mode</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; Users</td>
<td></td>
<td>R/W all accounts</td>
<td>R/W own account</td>
<td>R/W all accounts</td>
<td>R/W own account</td>
</tr>
<tr>
<td>Administration &gt; Licenses</td>
<td></td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; PRSM Logs</td>
<td></td>
<td>R/W</td>
<td>RO</td>
<td>R/W</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; Server Certificates</td>
<td></td>
<td>R/W</td>
<td>No</td>
<td>R/W</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; Change History</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; Database Backup</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
### 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
Do not change the admin password on the device after adding it to the inventory, or communication with the device will fail. You will have to delete the device from the inventory and add it again to use the new password.

- 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.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Role</th>
<th>Security Administrator</th>
<th>System Administrator</th>
<th>Reporting Administrator</th>
<th>Help Desk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration &gt; Upgrade</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; End User Notification</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Administration &gt; About PRSM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Commit and Deploy Changes</td>
<td>R/W</td>
<td>R/W</td>
<td>R/W</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

#### 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.
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**

1. **Step 1** If the directory realm you want to use is not yet defined, create it.
   - a) Select Device > 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.

2. **Step 2** Select Administration > Users.

3. **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.

4. **Step 4** Select the directory realm.
   Select None to remove support for remote user definitions.

5. **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.) These users are defined in an external SSO directory, which enables integration between PRSM and supported network management applications.
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 300.

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.) These users are defined in an external SSO directory, which enables integration between PRSM and supported network management applications.
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 296.

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 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.


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 Device > 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 new 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.
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 304.

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.
Forexample,iftheservercertificatewassignedybyarootcertificate,thefilewouldlooklikethefollowing
(parts of the example are redacted as indicated; do not include the annotations):

```
-----BEGIN CERTIFICATE-----
MIIDzjCCArag...(bulk of server certificate redacted)...
ng51GTC5xeJz48Xkh3npFynf
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIID2TCCAsGg...(bulk of CA root certificate redacted)...
9DT4XfXcg+A0EaY1/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** 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 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.
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 aspdrop.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 **Device > Packet Capture** to configure the following global settings:

- **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.

- **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.

Click **Save** if you make changes.
Step 2  To configure the global capture of dropped packets, do the following:
   a) Select Device > Packet Capture.
   b) Select Capture: On in the Dropped Packets section.
   c) Click Save to save your changes.
   d) Click the Changes Pending link in the menu bar, then the Commit button on the Commit and Deploy Changes page, to commit your changes.
   e) Perform the network activity whose packets you are trying to capture.
   f) Edit the packet capture settings again, but this time select Capture: Off. Save your changes.
   g) Commit your changes.
   The packet capture file is written to disk.

Step 3  To configure packet capture for individual access policies, do the following:
   a) Select Policies > Policies.
   b) Mouse over the access policy and click Edit Policy.
   c) Select Capture Packets: On.
   d) 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.
   e) Click the Changes Pending link in the menu bar, then the Commit button on the Commit and Deploy Changes page, to commit your changes.
   f) Perform the network activity whose packets you are trying to capture.
   g) Edit the policy again, but this time select Capture Packets: Off. Save your changes.
   h) 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. Manually create diagnostic archive
Please enter your choice (Ctrl+C to exit): 2

=== Manual Diagnostic ===
 1. Add files to package
 2. View files in package
 3. Upload package
Please enter your choice (Ctrl+C to exit): 1

=== Add files 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
> 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
PDTS                    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
HFM 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
PPTS             | 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
HMP 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
```

User Guide for ASA CX and Cisco Prime Security Manager 9.1
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.

a) Do one of the following:

   - CX (Single Device mode), PRSM—Select **Administration > PRSM Logs**.
   - CX device managed in PRSM Multiple Device mode (managed mode)—Open the device configuration page by selecting **Device > Devices**, mousing over the device and clicking **Device Configuration**.

b) Adjust the logging levels as described in **Logging Configuration Properties (CX, PRSM)**, on page 313.

c) If you changed the logging levels for a CX device in managed mode, commit your changes and check deployment status to ensure that the device has been updated to apply the new levels.
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 homepage.

**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.
Navigation Path

- CX (Single Device mode), PRSM—Select Administration > PRSM Logs.
- CX device managed in PRSM Multiple Device mode (managed mode)—Open the device configuration page by selecting Device > Devices, mousing over the device and clicking Device Configuration.

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.

- 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.
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
```
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.
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.
```
Step 3 Enter 1 to reset the password, then enter the new password twice when prompted.

Example:

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 321
- Cisco Prime Security Manager Installation, page 322
- Upgrading the System, page 329
- Reimaging the ASA 5585-X CX SSP, page 334
- Reimaging the ASA CX Software Module, page 337
- Open CX and PRSM Ports, page 341

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](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) 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 23: Recommended PRSM Virtual Machine Sizing

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Default Values</th>
<th>10 Devices</th>
<th>25 Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cores (virtual CPUs)</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
<td>6 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>Disk Space</td>
<td>Two disks, 276 GB total:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 40 GB primary disk (disk 1) for application and database.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 256 GB secondary disk (disk 2) for event and report data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 TB secondary disk space.</td>
<td>3 TB secondary disk space.</td>
<td></td>
</tr>
</tbody>
</table>

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 322). 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.
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:

a) 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.

b) On the Source page, enter the URL of the OVA file or click Browse to select the file from your workstation. Click Next.

c) On the OVF Template Details page, view the product details and click Next.

d) On the End User License Agreement page, click Accept and then click Next.

e) 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.

f) 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.

g) 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.

h) 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 327.

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
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...
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.

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:
   a) In the CLI, enter the `show services status` command and verify that all processes are up.
   b) Log into the web interface to verify that it is accessible.
   c) 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select Administration &gt; Upgrade.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the Upgrade Packages tab.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select I want to &gt; Upload an Upgrade Package.</td>
</tr>
<tr>
<td>Step 4</td>
<td>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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <em>Administration</em> &gt; <em>Upgrade</em>.</td>
</tr>
<tr>
<td>2</td>
<td>Select the <em>Upgrade Packages</em> tab.</td>
</tr>
<tr>
<td>3</td>
<td>Mouse over the package you want to install and click <em>Upgrade</em>. 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.</td>
</tr>
<tr>
<td>4</td>
<td>Select the device you want to upgrade. Clicking a device toggles between selecting and deselecting the device. Selected devices are highlighted.</td>
</tr>
<tr>
<td>5</td>
<td>Click <em>Upgrade</em>. You are asked to confirm that you want to start the upgrade on the selected devices.</td>
</tr>
<tr>
<td>6</td>
<td>Click <em>Start Upgrade</em>. The system starts processing the upgrade request. If the upgrade fails, the system automatically reverts to the previously installed version.</td>
</tr>
</tbody>
</table>

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 reimagine 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 reimagine 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/asacximages/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/asa-cx-boot.img
rommon #5> sync

Updating NVRAM Parameters...
```

**Step 4** Initiate the TFTP boot:
Example:

```bash
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:

```bash
asacx-boot> partition
....
Partition Successfully Completed
asacx-boot>
```

**Step 7** Use the setup command to configure the system:

Example:

```bash
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:

```bash
For example, the following command will upgrade the system with the asacx-sys-9.0.2.pkg package. Enter **Y** to install the upgrade.
```

```bash
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.

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.
Reimaging the ASA CX Software Module

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.

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 210, 215
    LDAP/AD directory properties (CX) 215
supported (CX) 210
abandoning changes 31
About page 30
access policies 166
dashboard 166
access policies, context-aware 231, 232, 234, 237, 238, 239, 240, 241, 242, 243, 244, 246, 247, 248, 263, 265
application filtering 242, 243, 244, 263, 265
    compared to URL filtering 243
    configuring updates 263
    controlling 244
decryption requirements 244
    overview 242
tips 244
troubleshooting updates 265
    configuring 232
controlling network access 231
default behavior 232
    notifying end users of blocks 237, 238, 239, 240, 241
        editing message 240
overview 237
reference 239
variables 241
when sent 238
overview 231
properties 234
URL filtering 242, 243, 246, 247, 248, 263, 265
    controlling URL access 246
determining URL Category 247
category descriptions 248
    compared to application filtering 243
    configuring updates 263
overview 242
troubleshooting updates 265
active authentication 222
    enabling 222
Active Directory (AD) 215
    properties (CX) 215
    Active Directory (AD) agent 51, 227
        configuring passive authentication 51
identifying 227
admin user 298, 318
    characteristics 298
    resetting password 318
alerts 26, 145
    icons 26
    responding to 145
AnyConnect 62, 168
    monitoring and controlling clients 62
    user devices dashboard 168
    application objects 122
        reference 122
    application service objects 125
        reference 125
    application types 170
dashboard 170
Application Visibility and Control (AVC) 50, 62, 65, 242, 243, 244, 245, 263, 265
    controlling applications 50, 244
    controlling applications for Secure Mobility clients 62
dashboard 169
filtering 50, 62, 242, 243, 244, 263, 265
dashboard 169
    controlling 50, 62, 244
    compared to URL filtering 243
    configuring updates 263
    controlling 50, 62, 244
decryption requirements 244
tips on application filtering 244
troubleshooting updates 265
applications 50, 62, 169, 242, 243, 244, 245, 263, 265
viewing details 245
applications with malicious transactions 157, 161
   dashboard 157, 161
ASA 9, 12, 13
   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
ASA CX 1, 3, 7, 9, 12, 13, 14, 16, 17, 19, 23, 39, 43, 85, 321, 330, 333, 334, 337
   adding to inventory 85
   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 321, 334, 337
      boot image (5585-X) 334
      boot image (software modules) 337
      overview of packages 321
   installing upgrades 330, 333, 334
   CLI 330
      troubleshooting 334
   web interface 333
   introduction 1
   logging in 23
      CLI console 23
   monitoring mode 43
   overview 3
   preparing for management 7
   redirecting traffic to 14, 16, 17, 19
      configuring monitor-only mode 16
      overview 14
      troubleshooting PRSM 19
      using ASA CLI 14
      using PRSM 17
   setting up software 9
   transparent mode 39
   use cases 39
ASA devices 14, 16, 17, 19, 79, 81, 82, 85, 87, 88, 89, 105, 291
   adding to inventory 85
   assigning device groups 105
   device configuration 88
   discovery 82
   managing 79
   preparing for management 81
   redirecting traffic to ASA CX 14, 16, 17, 19
      configuring monitor-only mode 16
      overview 14
      troubleshooting PRSM 19
      using ASA CLI 14
      using PRSM 17
   refreshing certificate 87
ASA devices (continued)
   troubleshooting discovery 89
   logging 291
authentication services (ASA CX) 51, 54
   configuring passive authentication 51
   controlling access by user group 54
authentication services (CX) 209, 210, 211, 212, 213, 215, 217, 218, 220, 222, 224, 225, 226, 228
   configuring 211
   configuring directory realms 213
   configuring identity policies 218
   configuring settings 228
   deleting directories 217
   deleting directory realms 217
   directory properties 215
   directory realm overview 212
   enabling active authentication 222
   enabling transparent authentication 224
   enabling transparent authentication (Firefox) 226
   enabling transparent authentication (Internet Explorer) 225
   identity policy properties 222
   identity types 210
   managing 209
   overview 209
   supported servers and methods 210
   transparent authentication requirements 225
   what to tell users 211

B

backup 314, 316, 317
   database 314
   PRSM virtual machine 317
   scheduling database 316
basic authentication 224
bootstrapping 7, 81
ASA CX 7
ASA devices, for management 81
browser 21
   requirements 21

C

CA certificates 277
ASA CX 277
   downloading, installing the CA certificate 277
categories (web, URL) 159, 165
   dashboard 165
   malicious transactions dashboard 159
category (URL) 246, 247, 248, 263, 265
   configuring updates 263
category (URL) (continued)
  determining 247
  filtering 246
  troubleshooting updates 265
  descriptions 248
certificates 87, 274, 276, 278, 303, 304
  configuring decryption certificate 274
  configuring supplemental trusted 278
  converting certificate formats 276
  installing server 303
  obtaining server 304
  refreshing device 87
change history 35, 36
  viewing 35
  when changes become active 36
Cisco Technical Assistance Center 312
  creating diagnostic file 312
columns 151
  dashboard and report 151
Commit and Deploy Changes page 31, 33, 34, 35, 36
  committing changes 31
  discarding changes 31
  managing jobs 34
  overview 33
  viewing change history 35
  when changes become active 36
configurations 89
  troubleshooting discovery 89
connectivity (system) 306
  checking 306
console 23
  logging into ASA CX 23
  logging into PRSM 23
context-aware access policies 231, 232, 234, 237, 238, 239, 240, 241, 242, 243, 244, 246, 247, 248, 263, 265
  application filtering 242, 243, 244, 246, 247, 248, 263, 265
  compared to URL filtering 243
  configuring updates 263
  controlling 244
  decryption requirements 244
  overview 242
  tips 244
  troubleshooting updates 265
configuring 232
  controlling network access 231
  default behavior 232
  notifying end users of blocks 237, 238, 239, 240, 241
    editing message 240
    overview 237
    reference 239
    variables 241
    when sent 238
  overview 231
  properties 234
context-aware access policies (continued)
  URL filtering 242, 243, 246, 247, 248, 263, 265
  controlling URL access 246
  determining URL Category 247
  category descriptions 248
  compared to application filtering 243
  configuring updates 263
  overview 242
  troubleshooting updates 265
Context-Aware Security 1, 21
  getting started 21
  overview 1
  backing up database 314
  capturing packets 307
  checking connectivity 306
  committing changes 31
  discarding changes 31
  discovery 82
  installing upgrades 321, 329, 332
    overview of packages 321
    overview 329
  uploading packages 332
introduction 1
licenses 65, 66, 68, 69, 70, 71, 72, 73, 74
  apply or renew license reference 73
  applying 71
  enabling features 69
  revoking 74
  uploading 70
  assigning 71
  implications of expiration 66
  overview 65
  renewing 72
  using evaluation 68
logging in 22
  overview 22
  web interface 22
maintaining 295
managing 79
managing in multiple device mode 79
managing licenses 65
open management ports 341
resetting admin password 318
resetting to factory defaults 319
restoring database 314
scheduling database backups 316
supported AAA servers and methods 210
troubleshooting 295
<table>
<thead>
<tr>
<th><strong>D</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>dashboards 139, 142, 143, 145, 148, 149, 151, 154, 155, 157, 158, 159, 160, 161, 162, 164, 165, 166, 168, 169, 170, 172, 174</td>
<td></td>
</tr>
<tr>
<td>application types 170</td>
<td></td>
</tr>
<tr>
<td>applications 169</td>
<td></td>
</tr>
<tr>
<td>applications with malicious transactions 161</td>
<td></td>
</tr>
<tr>
<td>changing time range 148</td>
<td></td>
</tr>
<tr>
<td>columns 151</td>
<td></td>
</tr>
<tr>
<td>controlling data 149</td>
<td></td>
</tr>
<tr>
<td>data collection and quality 142</td>
<td></td>
</tr>
<tr>
<td>devices 172</td>
<td></td>
</tr>
<tr>
<td>drilling into 143</td>
<td></td>
</tr>
<tr>
<td>interface 174</td>
<td></td>
</tr>
<tr>
<td>malicious traffic 157</td>
<td></td>
</tr>
<tr>
<td>malware types 158</td>
<td></td>
</tr>
<tr>
<td>network overview 155</td>
<td></td>
</tr>
<tr>
<td>overview 139</td>
<td></td>
</tr>
<tr>
<td>policies 166</td>
<td></td>
</tr>
<tr>
<td>reference 154</td>
<td></td>
</tr>
<tr>
<td>responding to alerts 145</td>
<td></td>
</tr>
<tr>
<td>user devices, remote access VPN 168</td>
<td></td>
</tr>
<tr>
<td>users 162</td>
<td></td>
</tr>
<tr>
<td>users with malicious transactions 159</td>
<td></td>
</tr>
<tr>
<td>using 142</td>
<td></td>
</tr>
<tr>
<td>viewing 139</td>
<td></td>
</tr>
<tr>
<td>web (URL) categories 165</td>
<td></td>
</tr>
<tr>
<td>web categories with malicious transactions 159</td>
<td></td>
</tr>
<tr>
<td>web destinations 164</td>
<td></td>
</tr>
<tr>
<td>web destinations with malicious transactions 160</td>
<td></td>
</tr>
<tr>
<td>database 317, 319</td>
<td></td>
</tr>
<tr>
<td>resetting to factory defaults 319</td>
<td></td>
</tr>
<tr>
<td>VMware snapshots 317</td>
<td></td>
</tr>
<tr>
<td>decryption policies 267, 269, 270, 271, 272, 273, 274, 276, 277, 278, 279, 280, 283, 285</td>
<td></td>
</tr>
<tr>
<td>bypassing 283</td>
<td></td>
</tr>
<tr>
<td>configuration overview 272</td>
<td></td>
</tr>
<tr>
<td>configuring 279</td>
<td></td>
</tr>
<tr>
<td>configuring decryption certificate 274</td>
<td></td>
</tr>
<tr>
<td>configuring settings 273</td>
<td></td>
</tr>
<tr>
<td>configuring supplemental trusted certificates 278</td>
<td></td>
</tr>
<tr>
<td>converting certificate formats 276</td>
<td></td>
</tr>
<tr>
<td>decrypted traffic flow 270</td>
<td></td>
</tr>
<tr>
<td>do not decrypt traffic flow 271</td>
<td></td>
</tr>
<tr>
<td>downloading, installing the CA certificate 277</td>
<td></td>
</tr>
<tr>
<td>managing 267</td>
<td></td>
</tr>
<tr>
<td>overview 267</td>
<td></td>
</tr>
<tr>
<td>properties 280</td>
<td></td>
</tr>
<tr>
<td>purpose of decryption 269</td>
<td></td>
</tr>
<tr>
<td>tips, limitations 272</td>
<td></td>
</tr>
<tr>
<td>troubleshooting 285</td>
<td></td>
</tr>
<tr>
<td>deployment jobs (continued)</td>
<td></td>
</tr>
<tr>
<td>committing changes 31</td>
<td></td>
</tr>
<tr>
<td>managing 33, 34, 35, 36, 37</td>
<td></td>
</tr>
<tr>
<td>Commit and Deploy Changes page 33</td>
<td></td>
</tr>
<tr>
<td>committing changes 31</td>
<td></td>
</tr>
<tr>
<td>managing jobs 34</td>
<td></td>
</tr>
<tr>
<td>viewing change history 35</td>
<td></td>
</tr>
<tr>
<td>when changes become active 36</td>
<td></td>
</tr>
<tr>
<td>Deployment Manager 31, 33, 34, 35, 36</td>
<td></td>
</tr>
<tr>
<td>Commit and Deploy Changes page 33</td>
<td></td>
</tr>
<tr>
<td>committing changes 31</td>
<td></td>
</tr>
<tr>
<td>discarding changes 31</td>
<td></td>
</tr>
<tr>
<td>managing jobs 34</td>
<td></td>
</tr>
<tr>
<td>viewing change history 35</td>
<td></td>
</tr>
<tr>
<td>when changes become active 36</td>
<td></td>
</tr>
<tr>
<td>destination object groups 127</td>
<td></td>
</tr>
<tr>
<td>reference 127</td>
<td></td>
</tr>
<tr>
<td>devices 37, 79, 82, 84, 85, 87, 88, 89, 105, 172, 174</td>
<td></td>
</tr>
<tr>
<td>adding to inventory 85</td>
<td></td>
</tr>
<tr>
<td>assigning to device groups 105</td>
<td></td>
</tr>
<tr>
<td>changing management IP 87</td>
<td></td>
</tr>
<tr>
<td>dashboard 172</td>
<td></td>
</tr>
<tr>
<td>dashboard, interface 174</td>
<td></td>
</tr>
<tr>
<td>deleting from inventory 89</td>
<td></td>
</tr>
<tr>
<td>deployment status 37</td>
<td></td>
</tr>
<tr>
<td>device configuration 88</td>
<td></td>
</tr>
<tr>
<td>managing 79</td>
<td></td>
</tr>
<tr>
<td>managing CX 79</td>
<td></td>
</tr>
<tr>
<td>managing inventory 84</td>
<td></td>
</tr>
<tr>
<td>refreshing certificate 87</td>
<td></td>
</tr>
<tr>
<td>troubleshooting discovery 89</td>
<td></td>
</tr>
<tr>
<td>understanding discovery 82</td>
<td></td>
</tr>
<tr>
<td>viewing inventory 84</td>
<td></td>
</tr>
<tr>
<td>out-of-band changes 88</td>
<td></td>
</tr>
<tr>
<td>devices, user 168</td>
<td></td>
</tr>
<tr>
<td>dashboard 168</td>
<td></td>
</tr>
<tr>
<td>diagnostics file 312, 313</td>
<td></td>
</tr>
<tr>
<td>creating 312</td>
<td></td>
</tr>
<tr>
<td>logging properties 313</td>
<td></td>
</tr>
<tr>
<td>directory 212, 213, 215, 217, 301</td>
<td></td>
</tr>
<tr>
<td>configuring realms 213</td>
<td></td>
</tr>
<tr>
<td>configuring SSO realms 301</td>
<td></td>
</tr>
<tr>
<td>deleting 217</td>
<td></td>
</tr>
<tr>
<td>overview 212</td>
<td></td>
</tr>
<tr>
<td>properties 215</td>
<td></td>
</tr>
</tbody>
</table>
directory realm 212, 213, 217, 301
  configuring 213
  configuring SSO 301
  deleting 217
  overview 212
directory realms 299
  configuring global for user management 299
discovery 82
  understanding 82
disk space (PRSM VM) 327
  managing 327
documentation overview 3

deleting 217

directory realm 212, 213, 217, 301
  configuring 213
  configuring SSO 301
  deleting 217
  overview 212
directory realms 299
  configuring global for user management 299
discovery 82
  understanding 82
disk space (PRSM VM) 327
  managing 327
documentation overview 3

E
disk space (PRSM VM) 327
  managing 327
documentation overview 3

disk space (PRSM VM) 327
  managing 327
documentation overview 3

E
end user notifications 237, 238, 239, 240, 241
  editing notification page 240
  overview 237
  reference 239
  variables 241
  when sent 238
Event Viewer 177, 181, 182, 183, 184, 185, 186, 190, 199
  filter rules 183
  filtering events 182
  message reference 185, 186, 190, 199
    columns 199
    Context-Aware Security traffic events 186
    CX, PRSM system events 190
    overview 185
  overview 177
  working with events 184
  views 181, 182
    configuring custom 181
    deleting custom 181
    switching between real time and historical 182
    using 181
events 177, 181, 182, 183, 184, 185, 186, 190, 199, 327
  filter rules 183
  filtering 182
  managing PRSM storage space 327
  reference 185, 186, 190, 199
    columns 199
    Context-Aware Security traffic events 186
    CX, PRSM system events 190
    overview 185
  viewing 177
  views 181
  working with individual 184

F
failover 42
  configuring 42
feature licenses 65, 66, 68, 69, 70, 71, 72, 73, 74
  apply or renew license reference 73
  applying licenses 71
  enabling features 69
  overview 65
  renewing licenses 72
  revoking licenses 74
  uploading licenses 70
  assigning licenses 71
  implications of expiration 66
  using evaluation 68
file filtering profile objects 130
  reference 130
file transfers 50
  controlling 50
filters 182, 183
  configuring event 182
  event rules 183

H
help, getting 30
high availability 42
  configuring 42
HTTPS 81, 267, 269, 270, 271, 272, 273, 274, 276, 277, 278, 279, 280, 283, 285, 303, 304
  decryption (ASA CX) 267, 269, 270, 271, 272, 273, 274, 276, 277, 278, 279, 280, 283, 285
  bypassing 283
  configuration overview 272
  configuring decryption certificate 274
  configuring policies 279
  configuring settings 273
  configuring supplemental trusted certificates 278
  converting certificate formats 276
  decrypted traffic flow 270
  decryption policy properties 280
  do not encrypt traffic flow 271
  downloading, installing the CA certificate 277
  managing traffic flows 267
  overview 267
  purpose 269
  tips, limitations 272
  troubleshooting 285
  installing server certificate 303
  obtaining server certificate 304
  preparing ASA devices for management 81
icons, policy and alert 26
identity 162
    users dashboard 162
identity objects 54, 116
    controlling access by user group 54
    CX, reference 116
identity policies 162, 218, 220, 222, 224, 225
    configuring 218
    enabling active authentication 222
    enabling transparent authentication 224
    properties 220
    transparent authentication requirements 225
    users dashboard 162
identity services (ASA CX) 51, 54
    configuring passive authentication 51
    controlling access by user group 54
identity services (CX) 209, 210, 211, 212, 213, 215, 217, 218, 220, 222, 224, 225, 226, 228
    configuring 211
    configuring authentication settings 228
    configuring directory realms 213
    configuring identity policies 218
    deleting directories 217
    deleting directory realms 217
    directory properties 215
    directory realm overview 212
    enabling active authentication 222
    enabling transparent authentication 224
    enabling transparent authentication (Firefox) 226
    enabling transparent authentication (Internet Explorer) 225
identity policy properties 220
identity types 210
    managing 209
    overview 209
    supported servers and methods 210
    transparent authentication requirements 225
    what to tell users 211
integrated Windows authentication 224
interface role objects 134
    reference 134
interfaces 174
    dashboard 174
inventory 79, 82, 84, 85, 87, 88, 89
    adding devices 85
    deleting from inventory 89
    device configuration 88
    managing 84
    managing CX 79
    out-of-band changes 88
    refreshing device certificate 87
    troubleshooting discovery 89
    understanding discovery 82
inventory (continued)
    viewing 84
K
    Kerberos authentication 224
    Known Users CX identity object 116
L
    LDAP server 215
    properties (CX) 215
    licenses 65, 66, 67, 68, 69, 70, 71, 72, 73, 74
    apply or renew license reference 73
    applying 71
    CX feature 65, 66
    implications of expiration 66
    enabling features 69
    licenses page 67
    managing CX and PRSM 65
    PRSM 66
    overview 66
    revoking 74
    uploading 70
    using evaluation 68
    assigning 71
    CX feature 65, 66
    overview 65
    renewing 72
    local policies 97, 100
        configuring policy sets 97
        deleting policy sets 100
    logging 291, 293, 294
        device settings 291
        syslog server 293, 294
        create and edit 293
        delete 294
    logging configuration (ASA) 291, 292
        accessing 292
        syslog server 292
    logging configuration (CX, PRSM) 312, 313
        downloading diagnostics file 312
        properties 313
        setting log levels 312
M
    malware 158
        types dashboard 158
    menus, web interface 24
monitor-only mode, configuring 16

N

network 145, 155
  overview dashboard 155
  responding to alerts 145
network group objects 112
  reference 112
NTLM authentication 224

O

objects (policy) 107, 109, 110, 112, 114, 116, 118, 121, 122, 124, 125, 127, 128, 130, 132, 134
  configuring 109
  deleting 110
  managing 107
  overview 107
  reference 110, 112, 114, 116, 118, 121, 122, 124, 125, 127, 128, 130, 132, 134
    application objects 122
    application service objects 125
    common properties 110
    CX identity objects 116
    destination object groups 127
    file filtering profile objects 130
    interface roles 134
    network groups 112
    Secure Mobility objects 124
    service groups 114
    source object groups 128
    URL objects 118
    user agent objects 121
    web reputation profile objects 132
out-of-band changes 88
  dealing with 88

P

packets 307
  capturing 307
policies 26, 31, 94, 95, 96, 100, 104, 105, 106, 166
  abandoning changes 31
  assigning device groups 105
  committing changes 31
  concepts 94
  configuring 98
  configuring device groups 104
  dashboard 166
  policies (continued)
    deleting 100
    deleting device groups 106
    icons 26
    managing device groups 100
    overview 95
policy objects 107, 109, 110, 112, 114, 116, 118, 121, 122, 124, 125, 127, 128, 130, 132, 134
  configuring 109
  deleting 110
  managing 107
  overview 107
  reference 110, 112, 114, 116, 118, 121, 122, 124, 125, 127, 128, 130, 132, 134
    application objects 122
    application service objects 125
    common properties 110
    CX identity objects 116
    destination object groups 127
    file filtering profile objects 130
    interface roles 134
    network groups 112
    Secure Mobility objects 124
    service groups 114
    source object groups 128
    URL objects 118
    user agent objects 121
    web reputation profile objects 132
policy sets 97, 100
  configuring 97
  copying 97
  deleting 100
ports 341
  open management 341
processes (system) 310
  managing 310
  backing up database 314
  backing up VM 317
  changing management IP 87
  checking connectivity 306
  committing changes 31
  discarding changes 31
  features 5
  getting started 21
  installation 321, 322, 323
    overview 322
    overview of packages 321
    preparing server 322
    virtual machine 323
  installing upgrades 329, 330, 332, 333, 334
    CLI 330
enabling features 69
revoking 74
uploading 70
assigning 71
overview 66
renewing 72
using evaluation 68

logging in 22, 22
CLI console 23
overview 22
web interface 22
maintaining 295
managing disk space 327
managing licenses 65
open management ports 341
overview 1, 3
resetting admin password 318
resetting to factory defaults 319
restoring database 314
restoring VM 317
scheduling database backups 316
troubleshooting 295

recovery user account 318
remote access VPN 62, 168
monitoring and controlling clients 62
user devices dashboard 168
reports 139, 142, 151, 153, 327
columns 151
creating 153
data collection and quality 142
generating 153
managing PRSM storage space 327
overview 139
properties 153
types 153
viewing 139
reputation 157, 158, 159, 160, 161
dashboard, applications with malicious transactions 161
dashboard, malicious traffic 157
reputation (continued)
dashboard, malware type 158
dashboard, users with malicious transactions 159
dashboard, web categories with malicious transactions 159
dashboard, web destinations with malicious transactions 160
reputation (web) profile objects 132
reference 132
restarting system processes 310
restore 314, 317
database 314
PRSM virtual machine 317

S
Secure Mobility objects 62, 124
monitoring and controlling VPN clients 62
reference 124
server requirements 322
PRSM installation 322
service group objects 114
reference 114
shared policies 97, 100, 104, 105, 106
assigning device groups 105
configuring device groups 104
configuring policy sets 97
deleting device groups 106
deleting policy sets 100
managing device groups 100
single sign-on 301
generic 301
snapshots 317
PRSM virtual machine 317
software installation 321, 329, 330, 332, 333, 334
overview of packages 321
upgrades 329, 330, 332, 333, 334
CLI 330
overview 329
troubleshooting 334
uploading packages 332
web interface 333
source object groups 128
reference 128
SSL 81, 87, 267, 269, 270, 271, 272, 273, 274, 276, 277, 278, 279, 280, 283, 285, 303, 304
decryption (ASA CX) 267, 269, 270, 271, 272, 273, 274, 276, 277, 278, 279, 280, 283, 285
bypassing 283
configuration overview 272
configuring decryption certificate 274
configuring policies 279
configuring settings 273
configuring supplemental trusted certificates 278
SSL (continued)
decryption (ASA CX) (continued)
converting certificate formats 276
decrypted traffic flow 270
decryption policy properties 280
do not decrypt traffic flow 271
downloading, installing the CA certificate 277
managing traffic flows 267
overview 267
purpose 269
tips, limitations 272
troubleshooting 285
installing server certificate 303
obtaining server certificate 304
preparing ASA devices for management 81
refreshing device certificates 87
status 37
deployment jobs and devices 37
storage space 327
managing PRSM 327
support, technical 312
creating diagnostic file 312
syslog 291, 292, 293, 294
accessing 292
logging configuration 291
servers 292, 293, 294
create and edit 293
delete 294
system events (CX, PRSM) 190

T

threats 157, 158, 159, 160, 161
applications with malicious transactions dashboard 161
dashboard, web destinations with malicious transactions 160
malicious traffic dashboard 157
malware type dashboard 158
users with malicious transactions dashboard 159
web categories with malicious transactions dashboard 159
time range 148
changing dashboard 148
TLS 267, 268, 270, 271, 272, 273, 274, 276, 277, 278, 279, 280, 283, 285, 303, 304
decryption (ASA CX) 267, 269, 270, 271, 272, 273, 274, 276, 277, 278, 279, 280, 283, 285,
277, 278, 279, 280, 283, 285
bypassing 283
configuration overview 272
configuring decryption certificate 274
configuring policies 279
configuring settings 273
configuring supplemental trusted certificates 278
converting certificate formats 276

TLS (continued)
decryption (ASA CX) (continued)
decrypted traffic flow 270
decryption policy properties 280
do not decrypt traffic flow 271
downloading, installing the CA certificate 277
managing traffic flows 267
overview 267
purpose 269
tips, limitations 272
troubleshooting 285
installing server certificate 303
obtaining server certificate 304
traffic events (CX) 186
transparent authentication 224, 225, 226
enabling 224
enabling in Firefox 226
enabling in Internet Explorer 225
requirements 225
transparent mode 39
configuring for ASA CX 39
troubleshooting 19, 30, 36, 37, 89, 145, 265, 283, 285, 306, 310, 312, 313, 319
checking system 306
configuring logging properties 313
creating diagnostics file 312
deployment status 37
discovery 89
managing system processes 310
PRSM traffic redirection 19
resetting system to factory defaults 319
responding to alerts 145
signature and engine updates 265
TLS/SSL decryption 285
unknown CA or bad certificate errors 283
web interface problems 30
when configuration changes become active 36
trusted certificates 278, 303, 304
configuring supplemental 278
installing server 303
obtaining server 304

U

undoing changes 31
Unknown Users CX identity object 116
Updater Connection events 265
updates 263, 265
configuring signature and engine 263
troubleshooting signature and engine 265
Upgrade Manager 321, 329, 331, 332, 333, 334
installing upgrades 333
Upgrade Manager (continued)
- overview 331
- overview of packages 321
- system upgrades 329
- troubleshooting 334
- uploading packages 332

upgrade packages 321, 329, 330, 332, 333, 334
- installation overview 329
- installing from CLI 330
- installing from web interface 333
- overview 321
- troubleshooting 334
- uploading 332

URL categories 159, 165
- dashboard 165
- malicious transactions dashboard 159

URL filtering 58, 60, 118, 242, 243, 246, 247, 248, 263, 265
- acceptable use policies 58
- configuring URL objects 118
- controlling URL access 246
- determining URL Category 247
- filtering by web reputation 60
- overview 242
- category descriptions 248
- compared to application filtering 243
- configuring updates 263
- troubleshooting updates 265

URL objects 58, 118
- acceptable use policies 58
- reference 118

use cases 39, 42, 43, 50, 51, 54, 58, 60, 62
- acceptable use policies (URL filtering) 58
- configuring passive authentication 51
- controlling access by user group 54
- controlling application use 50
- controlling Secure Mobility devices 62
- filtering by web reputation 60
- gaining insight into traffic 43
- overview 39
- transparent mode 39
- configuring high availability 42

user account 24
- effect on web interface 24

user agent objects 121
- reference 121

user devices 168
- dashboard 168

user groups 54
- controlling access by user group 54

user identity 228
- configuring authentication settings 228

users 159, 162, 295, 296, 298, 299, 300, 301, 302, 303
- admin 298
- changing password 302

users (continued)
- configuring 299
- configuring global directory realm 299
- configuring SSO 301
- dashboard 162
- deleting 303
- malicious transactions dashboard 159
- managing 295
- page reference 295
- properties 300
- roles and privileges 296

V

views 181, 182, 183, 184
- configuring custom 181
- deleting custom 181
- filter rules 183
- filtering events 182
- switching between real time and historical 182
- using event 181
- working with individual 184

virtual machine (VM) 323, 327
- installing PRSM 323
- managing disk space 327

VPN, remote access 168
- user devices dashboard 168

W

web categories 159, 165
- dashboard 165
- malicious transactions dashboard 159

web destinations 160, 164
- dashboard 164
- malicious transactions dashboard 160

web interface 24, 26, 27, 30
- about PRSM 30
- basics 24
- getting help 30
- icons 26
- lists and tables 26
- menus 24
- mousing over items 27
- selecting items 27
- troubleshooting 30
- user role affect on 24

web reputation 60, 157, 158, 159, 160, 161
- dashboard, applications with malicious transactions 161
- dashboard, malicious traffic 157
- dashboard, malware types 158
web reputation (continued)
dashboard, users with malicious transactions 159
dashboard, web categories with malicious transactions 159
dashboard, web destinations with malicious transactions 160
filtering by 60
web reputation profile objects 60, 132
   filtering by web reputation 60

web reputation profile objects (continued)
   reference 132
Web Security Essentials 65
   license 65
web servers 160, 164
   dashboard 164
   malicious transactions dashboard 160