Configuring the ASA CX Module

This chapter describes how to configure the ASA CX module that runs on the ASA. This chapter includes the following sections:

- Information About the ASA CX Module, page 1-1
- Licensing Requirements for the ASA CX Module, page 1-4
- Guidelines and Limitations, page 1-4
- Default Settings, page 1-5
- Configuring the ASA CX Module, page 1-5
- Managing the ASA CX Module, page 1-14
- Monitoring the ASA CX Module, page 1-15
- Troubleshooting the ASA CX Module, page 1-20
- Feature History for the ASA CX Module, page 1-21

Information About the ASA CX Module

The ASA CX module lets 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), the time of the attempted access (when), and the properties of the device used for the access (how). With the ASA CX module, 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.

This section includes the following topics:

- How the ASA CX Module Works with the ASA, page 1-2
- Information About ASA CX Management, page 1-2
- Information About Authentication Proxy, page 1-3
- Information About VPN and the ASA CX Module, page 1-4
- Compatibility with ASA Features, page 1-4

How the ASA CX Module Works with the ASA

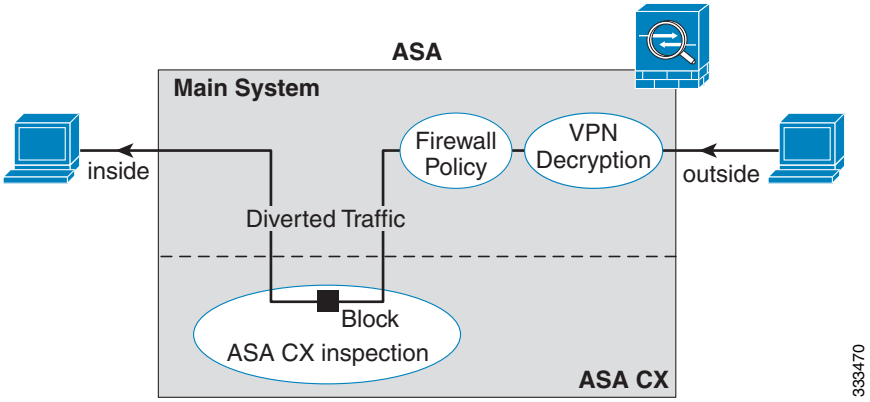
The ASA CX module runs a separate application from the ASA. The ASA CX module includes external management interface(s) so you can connect to the ASA CX module directly. Any data interfaces on the ASA CX module are used for ASA traffic only.

Traffic goes through the firewall checks before being forwarded to the ASA CX module. When you identify traffic for ASA CX inspection on the ASA, traffic flows through the ASA and the ASA CX module as follows:

1. Traffic enters the ASA.
2. Incoming VPN traffic is decrypted.
3. Firewall policies are applied.
4. Traffic is sent to the ASA CX module.
5. The ASA CX module applies its security policy to the traffic, and takes appropriate actions.
6. Valid traffic is sent back to the ASA; the ASA CX module might block some traffic according to its security policy, and that traffic is not passed on.
7. Outgoing VPN traffic is encrypted.
8. Traffic exits the ASA.

Figure 1-1 shows the traffic flow when using the ASA CX module. In this example, the ASA CX module automatically blocks traffic that is not allowed for a certain application. All other traffic is forwarded through the ASA.

Figure 1-1 ASA CX Module Traffic Flow in the ASA



Note If you have a connection between hosts on two ASA interfaces, and the ASA CX service policy is only configured for one of the interfaces, then all traffic between these hosts is sent to the ASA CX module, including traffic orginiating on the non-ASA CX interface (the feature is bidirectional). However, the ASA only performs the authentication proxy on the interface to which the service policy is applied, because this feature is ingress-only.

Information About ASA CX Management

- Initial Configuration, page 1-3

- Policy Configuration and Management, page 1-3

Initial Configuration

For initial configuration, you must use the CLI on the ASA CX module to run the **setup** command and configure other optional settings.

To access the CLI, you can use the following methods:

- ASA CX console port—The ASA CX console port is a separate external console port.
- ASA CX Management 1/0 interface using SSH—You can connect to the default IP address (192.168.8.8), or you can use ASDM to change the management IP address and then connect using SSH. The ASA CX management interface is a separate external Gigabit Ethernet interface.

Note You cannot access the ASA CX module CLI over the ASA backplane using the **session** command.

Policy Configuration and Management

After you perform initial configuration, configure the ASA CX policy using Cisco Prime Security Manager (PRSM). Then configure the ASA policy for sending traffic to the ASA CX module using ASDM or the ASA CLI.

Note When using PRSM in multiple device mode, you can configure the ASA policy for sending traffic to the ASA CX module within PRSM, instead of using ASDM or the ASA CLI. Using PRSM lets you consolodate management to a single management system. However, PRSM has some limitations when configuring the ASA service policy; see the ASA CX user guide for more information.

Information About Authentication Proxy

When the ASA CX needs to authenticate an HTTP user (to take advantage of identity policies), you must configure the ASA to act as an authentication proxy: the ASA CX module redirects authentication requests to the ASA interface IP address/proxy port. By default, the port is 885 (user configurable). Configure this feature as part of the service policy to divert traffic from the ASA to the ASA CX module. If you do not enable the authentication proxy, only passive authentication is available.

Note If you have a connection between hosts on two ASA interfaces, and the ASA CX service policy is only configured for one of the interfaces, then all traffic between these hosts is sent to the ASA CX module, including traffic orginiating on the non-ASA CX interface (the feature is bidirectional). However, the ASA only performs the authentication proxy on the interface to which the service policy is applied, because this feature is ingress-only.

Information About VPN and the ASA CX Module

The ASA includes VPN client and user authentication metadata when forwarding traffic to the ASA CX module, which allows the ASA CX module to include this information as part of its policy lookup criteria. The VPN metadata is sent only at VPN tunnel establishment time along with a type-length-value (TLV) containing the session ID. The ASA CX module caches the VPN metadata for each session. Each tunneled connection sends the session ID so the ASA CX module can look up that session's metadata.

Compatibility with ASA Features

The ASA includes many advanced application inspection features, including HTTP inspection. However, the ASA CX module provides more advanced HTTP inspection than the ASA provides, as well as additional features for other applications, including monitoring and controlling application usage.

To take full advantage of the ASA CX module features, see the following guidelines for traffic that you send to the ASA CX module:

- Do not configure ASA inspection on HTTP traffic.
- Do not configure Cloud Web Security (ScanSafe) inspection. If you configure both the ASA CX action and Cloud Web Security inspection for the same traffic, the ASA only performs the ASA CX action.
- Other application inspections on the ASA are compatible with the ASA CX module, including the default inspections.
- Do not enable the Mobile User Security (MUS) server; it is not compatible with the ASA CX module.
- Do not enable ASA clustering; they are not compatible; it is not compatible with the ASA CX module.
- If you enable failover, when the ASA fails over, any existing ASA CX flows are transferred to the new ASA, but the traffic is allowed through the ASA without being acted upon by the ASA CX module. Only new flows recieved by the new ASA are acted upon by the ASA CX module.

Licensing Requirements for the ASA CX Module

Model	License Requirement
All models	Base License.

The ASA CX module and PRSM require additional licenses. See the ASA CX documentation for more information.

Guidelines and Limitations

Context Mode Guidelines

Supported in single context mode only. Does not support multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

Failover Guidelines

Does not support failover directly; when the ASA fails over, any existing ASA CX flows are transferred to the new ASA, but the traffic is allowed through the ASA without being inspected by the ASA CX.

ASA Clustering Guidelines

Does not support clustering.

IPv6 Guidelines

Supports IPv6.

Model Guidelines

Supported only on the ASA 5585-X. See the *Cisco ASA Compatibility Matrix* for more information:

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

Additional Guidelines and Limitations

- See the "Compatibility with ASA Features" section on page 1-4.
- You cannot change the software type installed on the module; if you purchase an ASA CX module, you cannot later install other software on it.

Default Settings

Table 1-1 lists the default settings for the ASA CX module.

Table 1-1 Default Network Parameters

Parameters	Default
Management IP address	Management 1/0 192.168.8.8/24
Gateway	192.168.8.1/24
SSH Username	admin
Password	Admin123

Configuring the ASA CX Module

This section describes how to configure the ASA CX module and includes the following topics:

- Task Flow for the ASA CX Module, page 1-6
- Connecting the ASA CX Management Interface, page 1-7
- Configuring the ASA CX Management IP Address, page 1-8
- Configuring Basic ASA CX Settings at the ASA CX CLI, page 1-9

- Configuring the Security Policy on the ASA CX Module Using PRSM, page 1-11
- Redirecting Traffic to the ASA CX Module, page 1-12

Task Flow for the ASA CX Module

Configuring the ASA CX module is a process that includes configuration of the ASA CX security policy on the ASA CX module and then configuration of the ASA to send traffic to the ASA CX module. To configure the ASA CX module, perform the following steps:

Step 1 Cable the ASA CX management interfaces interface. See the "Connecting the ASA CX Management Interface" section on page 1-7.

Step 2 On the ASA, configure the ASA CX module management IP address for initial SSH access. See the "Configuring the ASA CX Management IP Address" section on page 1-8.

Step 3 On the ASA CX module, configure basic settings. You must use the CLI to configure these settings. See the "Configuring Basic ASA CX Settings at the ASA CX CLI" section on page 1-9.

Step 4 On the ASA CX module, configure the security policy using PRSM. See the "Configuring the Security Policy on the ASA CX Module Using PRSM" section on page 1-11.

Step 5 (Optional) On the ASA, configure the authentication proxy port. See the "(Optional) Configuring the Authentication Proxy Port" section on page 1-12.

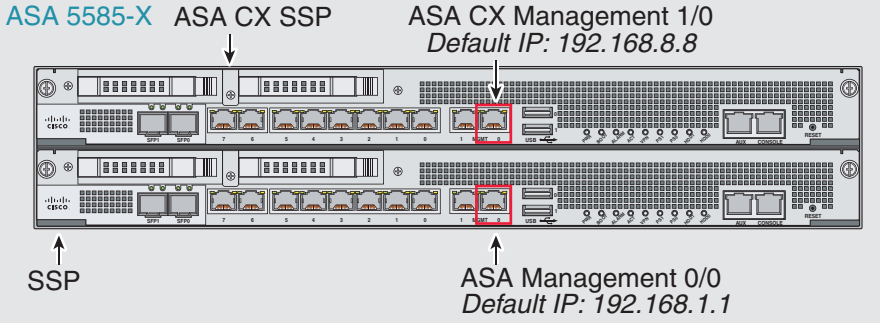
Step 6 On the ASA, identify traffic to divert to the ASA CX module. See the "Redirecting Traffic to the ASA CX Module" section on page 1-12.

Note When using PRSM in multiple device mode, you can configure the ASA policy for sending traffic to the ASA CX module within PRSM, instead of using ASDM or the ASA CLI. However, PRSM has some limitations when configuring the ASA service policy; see the ASA CX user guide for more information.

Connecting the ASA CX Management Interface

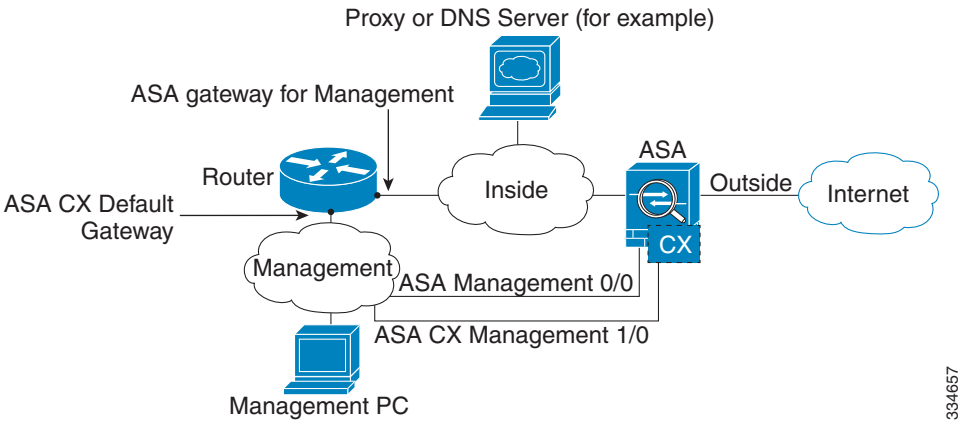
In addition to providing management access to the ASA CX module, the ASA CX management interface needs access to an HTTP proxy server or a DNS server and the Internet for signature updates and more. This section describes recommended network configurations. Your network may differ.

The ASA CX module includes a separate management interface from the ASA. For initial setup, you can connect with SSH to the ASA CX Management 1/0 interface using the default IP address (192.168.8.8/24). If you cannot use the default IP address, you can either use the console port or use ASDM to change the management IP address so you can use SSH.



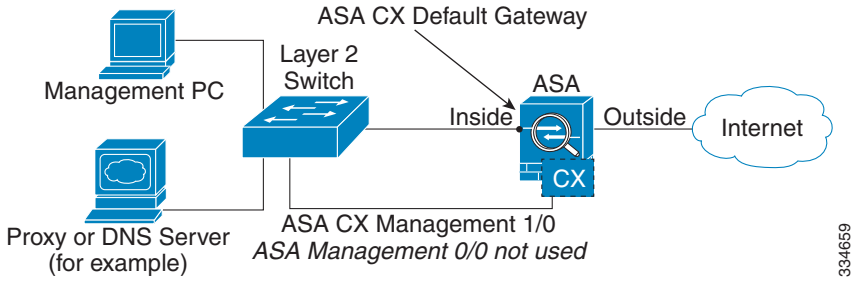
If you have an inside router

If you have an inside router, you can route between the management network, which can include both the ASA Management 0/0 and ASA CX Management 1/0 interfaces, and the ASA inside network for Internet access. Be sure to also add a route on the ASA to reach the Management network through the inside router.



If you do not have an inside router

If you have only one inside network, then you cannot also have a separate management network, which would require an inside router to route between the networks. In this case, you can manage the ASA from the inside interface instead of the Management 0/0 interface. Because the ASA CX module is a separate device from the ASA, you can configure the ASA CX Management 1/0 address to be on the same network as the inside interface.



What to Do Next

- Configure the ASA CX management IP address. See the "Configuring the ASA CX Management IP Address" section on page 1-8.

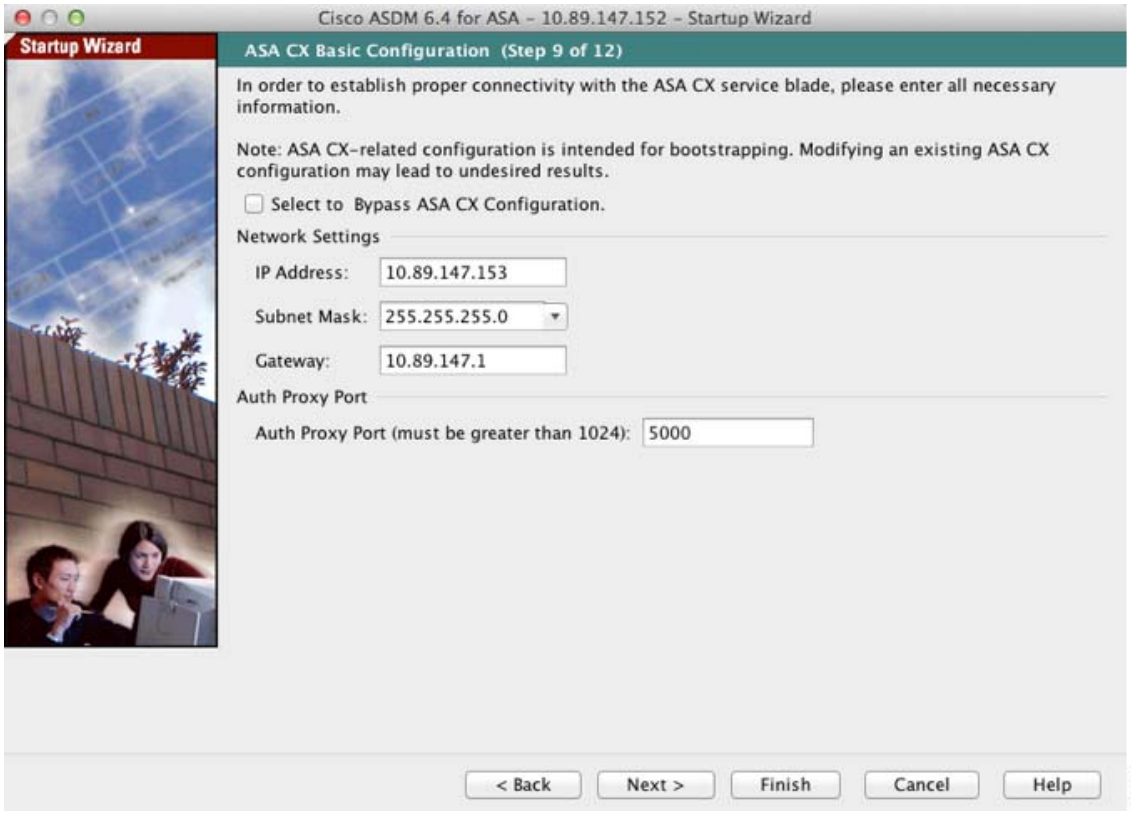
Configuring the ASA CX Management IP Address

If you cannot use the default management IP address (192.168.8.8), then you can set the management IP address from the ASA. After you set the management IP address, you can access the ASA CX module using SSH to perform initial setup.

Detailed Steps

Step 1 In ASDM, choose **Wizards > Startup Wizard**.

Step 2 Click **Next** to advance through the initial screens until you reach the ASA CX Basic Configuration screen.



Step 3 Enter the new management IP address, subnet mask, and default gateway.

Step 4 (Optional) Change the Auth Proxy Port. You can set this later if desired. See the "(Optional) Configuring the Authentication Proxy Port" section on page 1-12 for more information.

Step 5 Click **Finish** to skip the remaining screens, or click **Next** to advance through the remaining screens and complete the wizard.

Configuring Basic ASA CX Settings at the ASA CX CLI

You must configure basic network settings and other parameters on the ASA CX module before you can configure your security policy.

Detailed Steps

Step 1 Connect to the ASA CX CLI:

- Using SSH to the ASA CX Management 1/0 interface—Log in with the username **admin** and the password **Admin123**. You will change the password as part of this procedure.
- Using the ASA CX console port.

Step 2 Enter the following command:

```
asacx> setup
```

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. This example shows how to configure both IPv4 and IPv6 static addresses. You can configure IPv6 stateless auto configuration by answering **N** when asked if you want to configure a static IPv6 address.

```
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
...
Done.
Press ENTER to continue...
asacx>
```

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

Step 4 If you do not use NTP, configure the time settings. The default time zone is the UTC time zone. Use the **show time** command to see the current settings. You can use the following commands to change time settings:

```
asacx> config timezone
asacx> config time
```

Step 5 Change the admin password by entering the following command:

```
asacx> config passwd
```

Example:

```
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: Farscape1
Confirm password: Farscape1
SUCCESS: Password changed for user admin
```

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

Configuring the Security Policy on the ASA CX Module Using PRSM

This section describes how to launch PRSM to configure the ASA CX module application. For details on using PRSM to configure your ASA CX security policy, see the ASA CX user guide.

Detailed Steps

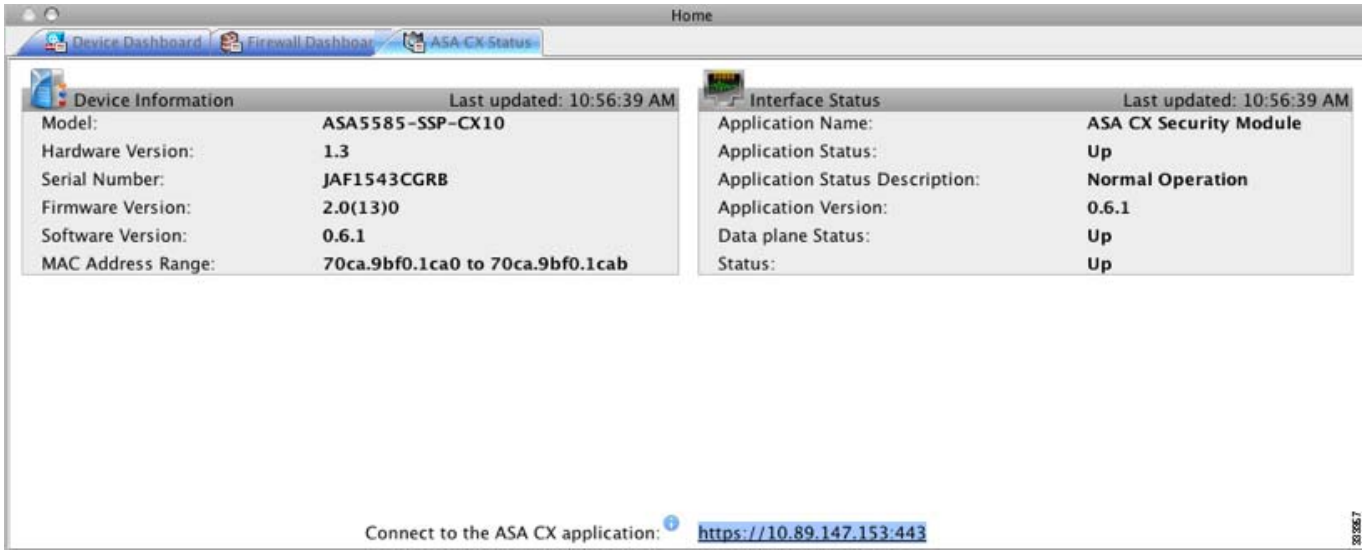
You can launch PRSM from your web browser, or you can launch it from ASDM.

- Launch PRSM from a web browser by enter the following URL:

  `https://`*`ASA_CX_management_IP`*

  Where the ASA CX management IP address is the one you set in the "Configuring Basic ASA CX Settings at the ASA CX CLI" section on page 1-9.

- Launch PRSM from ASDM by choosing **Home > ASA CX Status**, and clicking the **Connect to the ASA CX application** link.



What to Do Next

- (Optional) Configure the authentication proxy port. See the "(Optional) Configuring the Authentication Proxy Port" section on page 1-12.

- Divert traffic to the ASA CX module. See the "Redirecting Traffic to the ASA CX Module" section on page 1-12.

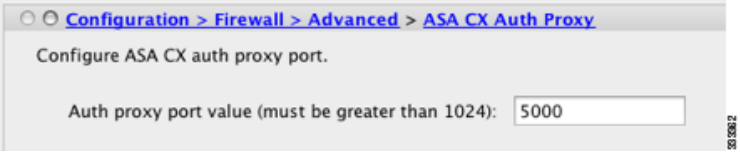
(Optional) Configuring the Authentication Proxy Port

The default authentication port is 885. To change the authentication proxy port, perform the following steps. For more information about the authentication proxy, see the "Information About Authentication Proxy" section on page 1-3.

Note You can also set the port as part of the ASDM startup wizard. See the "Configuring Basic ASA CX Settings at the ASA CX CLI" section on page 1-9.

Detailed Steps

Step 1 In ASDM, choose **Configuration > Firewall > Advanced > ASA CX Auth Proxy**.



Step 2 Enter a port greater than 1024. The default is 885.

Step 3 Click **Apply**.

Redirecting Traffic to the ASA CX Module

This section identifies traffic to redirect from the ASA to the ASA CX module. Configure this policy on the ASA.

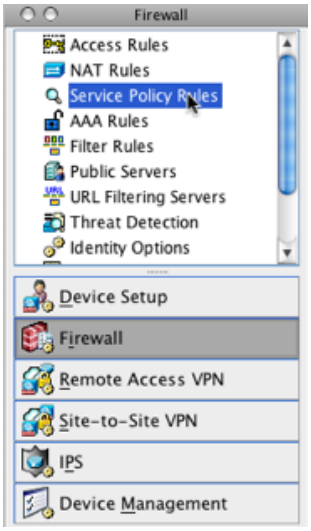
Note When using PRSM in multiple device mode, you can configure the ASA policy for sending traffic to the ASA CX module within PRSM, instead of using ASDM or the ASA CLI. However, PRSM has some limitations when configuring the ASA service policy; see the ASA CX user guide for more information.

Prerequisites

If you enable the authentication proxy on the ASA using this procedure, be sure to also configure a directory realm for authentication on the ASA CX module. See the ASA CX user guide for more information.

Detailed Steps

Step 1 Choose **Configuration > Firewall > Service Policy Rules**.

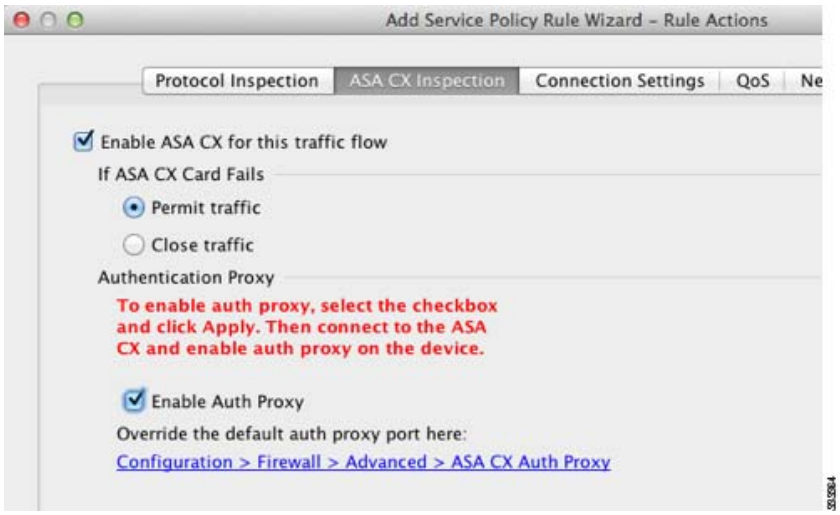


Step 2 Choose **Add > Add Service Policy Rule**. The Add Service Policy Rule Wizard - Service Policy dialog box appears.

Step 3 Complete the Service Policy dialog box, and then the Traffic Classification Criteria dialog box as desired. See the ASDM online help for more information about these screens.

Step 4 Click **Next** to show the Add Service Policy Rule Wizard - Rule Actions dialog box.

Step 5 Click the **ASA CX Inspection** tab.



Step 6 Check the **Enable ASA CX for this traffic flow** check box.

Step 7 In the If ASA CX Card Fails area, click **Permit traffic** or **Close traffic**. The Close traffic option sets the ASA to block all traffic if the ASA CX module is unavailable. The Permit traffic option sets the ASA to allow all traffic through, uninspected, if the ASA CX module is unavailable.

Step 8 To enable the authentication proxy, which is required for active authentication, check the **Enable Auth Proxy** check box.

Step 9 Click **OK** and then **Apply**.

Step 10 Repeat this procedure to configure additional traffic flows as desired.

Managing the ASA CX Module

This section includes procedures that help you manage the module and includes the following topics:

- Resetting the Password, page 1-14
- Reloading or Resetting the Module, page 1-15
- Shutting Down the Module, page 1-15

Note You can install or upgrade your image from within the ASA CX module. See the ASA CX module documentaiton for more information.

Resetting the Password

You can reset the module password to the default. For the user **admin**, the default password is **Admin123**. After resetting the password, you should change it to a unique value using the module application.

Resetting the module password causes the module to reboot. Services are not available while the module is rebooting.

If you cannot connect to ASDM with the new password, restart ASDM and try to log in again. If you defined a new password and still have an existing password in ASDM that is different from the new password, clear the password cache by choosing **File > Clear ASDM Password Cache**, then restart ASDM and try to log in again.

To reset the module password to the default of Admin123, perform the following steps.

Detailed Steps

Step 1 From the ASDM menu bar, choose **Tools > ASA CX Password Reset**.

The Password Reset confirmation dialog box appears.

Step 2 Click **OK** to reset the password to the default **Admin123**.

A dialog box displays the success or failure of the password reset.

Step 3 Click **Close** to close the dialog box.

Reloading or Resetting the Module

To reload or reset the module, enter one of the following commands at the ASA CLI.

Detailed Steps

Command	Purpose
hw-module module 1 reload **Example:** `hostname# hw-module module 1 reload`	Reloads the module software.
hw-module module 1 reset **Example:** `hostname# hw-module module 1 reset`	Performs a reset, and then reloads the module.

Shutting Down the Module

If you restart the ASA, the module is not automatically restarted. To shut down the module, perform the following steps at the ASA CLI.

Detailed Steps

Command	Purpose
hw-module module 1 shutdown **Example:** `hostname# hw-module module 1 shutdown`	Shuts down the module.

Monitoring the ASA CX Module

Use Tools > Command Line Interface to use monitoring commands.

- Showing Module Status, page 1-16
- Showing Module Statistics, page 1-16
- Monitoring Module Connections, page 1-17
- Capturing Module Traffic, page 1-20

- Problems with the Authentication Proxy, page 1-20

Note For ASA CX-related syslog messages, see the syslog messages guide. ASA CX syslog messages start with message number 429001.

Showing Module Status

See the "ASA CX Status Tab" section on page 1-31.

Showing Module Statistics

To show module statistics, enter the following command:

Command	Purpose
show service-policy cxsc	Displays the ASA CX statistics and status per service policy.

Examples

The following is sample output from the **show service-policy** command showing the ASA CX policy and the current statistics as well as the module status when the authentication proxy is disabled:

```
hostname# show service-policy cxsc
Global policy:
  Service-policy: global_policy
    Class-map: bypass
      CXSC: card status Up, mode fail-open, auth-proxy disabled
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

The following is sample output from the **show service-policy** command showing the ASA CX policy and the current statistics as well as the module status when the authentication proxy is enabled; in this case, the proxied counters also increment:

```
hostname# show service-policy cxsc
Global policy:
  Service-policy: pmap
    Class-map: class-default
      Default Queueing      Set connection policy: random-sequence-number disable
        drop 0
      CXSC: card status Up, mode fail-open, auth-proxy enabled
        packet input 7724, packet output 7701, drop 0, reset-drop 0, proxied 10
```

Monitoring Module Connections

To show connections through the ASA CX module, enter the one of the following commands:

Command	Purpose
show asp table classify domain cxsc	Shows the NP rules created to send traffic to the ASA CX module.
show asp table classify domain cxsc-auth-proxy	Shows the NP rules created for the authentication proxy for the ASA CX module.
show asp drop	Shows dropped packets. The following drop types are used: Frame Drops: • cxsc-bad-tlv-received—This occurs when ASA receives a packet from CXSC without a Policy ID TLV. This TLV must be present in non-control packets if it does not have the Standy Active bit set in the actions field. • cxsc-request—The frame was requested to be dropped by CXSC due a policy on CXSC whereby CXSC would set the actions to Deny Source, Deny Destination, or Deny Pkt. • cxsc-fail-close—The packet is dropped because the card is not up and the policy configured was 'fail-close' (rather than 'fail-open' which allows packets through even if the card was down). • cxsc-fail—The CXSC configuration was removed for an existing flow and we are not able to process it through CXSC it will be dropped. This should be very unlikely. • cxsc-malformed-packet—The packet from CXSC contains an invalid header. For instance, the header length may not be correct. Flow Drops: • cxsc-request—The CXSC requested to terminate the flow. The actions bit 0 is set. • reset-by-cxsc—The CXSC requested to terminate and reset the flow. The actions bit 1 is set. • cxsc-fail-close—The flow was terminated because the card is down and the configured policy was 'fail-close'.
show asp event dp-cp cxsc-msg	This output shows how many ASA CX module messages are on the dp-cp queue. Currently, only VPN queries from the ASA CX module are sent to dp-cp.
show conn	This command already shows if a connection is being forwarded to an module by displaying the ‘X - inspected by service module’ flag. Connections being forwarded to the ASA CX module will also display the ‘X’ flag.

Examples

The following is sample output from the **show asp table classify domain cxsc** command:

```
hostname# show asp table classify domain cxsc
Input Table
```

```
in  id=0x7ffedb4acf40, priority=50, domain=cxsc, deny=false
    hits=15485658, user_data=0x7ffedb4ac840, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=outside, output_ifc=any
in  id=0x7ffedb4ad4a0, priority=50, domain=cxsc, deny=false
    hits=992053, user_data=0x7ffedb4ac840, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=inside, output_ifc=any
in  id=0x7ffedb4ada00, priority=50, domain=cxsc, deny=false
    hits=0, user_data=0x7ffedb4ac840, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=m, output_ifc=any

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

The following is sample output from the **show asp table classify domain cxsc-auth-proxy** command. For the first rule in the output below, the destination "port=2000" is the auth-proxy port configured by the **cxsc auth-proxy port 2000** command, and the destination "ip/id=192.168.0.100" is the ASA interface IP address.

```
hostname# show asp table classify domain cxsc-auth-proxy
Input Table
in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=inside, output_ifc=identity
in  id=0x7ffed86cce20, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=2.2.2.2, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=new2, output_ifc=identity
in  id=0x7ffed86cd7d0, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=172.23.58.52, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=mgmt, output_ifc=identity
in  id=0x7ffed86caa80, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.5.172, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=outside, output_ifc=identity
in  id=0x7ffed86cb3c0, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=::/0, port=0
        dst ip/id=fe80::5675:d0ff:fe5b:1102/128, port=2000
    input_ifc=outside, output_ifc=identity
in  id=0x7ffed742be10, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=::/0, port=0
    dst ip/id=1:1:1:1::10/128, port=2000
    input_ifc=outside, output_ifc=identity
```

```
Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

The following is sample output from the **show asp drop** command. This output is just an example and lists all the possible reasons for a dropped frame or flow from the ASA CX module:

```
hostname# show asp drop
Frame drop:
  CXSC Module received packet with bad TLV's (cxsc-bad-tlv-received)           2
  CXSC Module requested drop (cxsc-request)                                    1
  CXSC card is down (cxsc-fail-close)                                          1
  CXSC config removed for flow (cxsc-fail)                                     3
  CXSC Module received malformed packet (cxsc-malformed-packet)                1

Last clearing: 18:12:58 UTC May 11 2012 by enable_15

Flow drop:
  Flow terminated by CXSC (cxsc-request)                                       2
  Flow reset by CXSC (reset-by-cxsc)                                           1
  CXSC fail-close (cxsc-fail-close)                                            1

Last clearing: 18:12:58 UTC May 11 2012 by enable_15
```

The following is sample output from the **show asp event dp-cp cxsc-msg** command:

```
hostname# show asp event dp-cp cxsc-msg
DP-CP EVENT QUEUE                   QUEUE-LEN  HIGH-WATER
Punt Event Queue                            0           5
Identity-Traffic Event Queue                0           0
General Event Queue                         0           4
Syslog Event Queue                          4          90
Non-Blocking Event Queue                    0           2
Midpath High Event Queue                    0          53
Midpath Norm Event Queue                 8074        8288
SRTP Event Queue                            0           0
HA Event Queue                              0           0
Threat-Detection Event Queue                0           3
ARP Event Queue                             0        2048
IDFW Event Queue                            0           0
CXSC Event Queue                            0           1
EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
cxsc-msg                1          0        1        0        1          0
```

The following is sample output from the **show conn detail** command:

```
hostname# show conn detail
0 in use, 105 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
```

```
TCP outside 208.80.152.2:80 inside 192.168.1.20:59928, idle 0:00:10, bytes 79174, flags
XUIO
```

Capturing Module Traffic

To configure and view packet captures for the ASA CX module, enter one of the following commands:

Command	Purpose
capture *name* **interface asa_dataplane**	Captures packets between ASA CX module and the ASA on the backplane.
copy capture	Copies the capture file to a server.
show capture	Shows the capture at the ASA console.

Note Captured packets contain an additional AFBP header that your PCAP viewer might not understand; be sure to use the appropriate plugin to view these packets.

Troubleshooting the ASA CX Module

- Problems with the Authentication Proxy, page 1-20

Problems with the Authentication Proxy

If you are having a problem using the authentication proxy feature, follow these steps to troubleshoot your configuration and connections:

1. Check your configurations.
   - On the ASA, check the output of the **show asp table classify domain cxsc-auth-proxy** command and make sure there are rules installed and that they are correct.
   - In PRSM, ensure the directory realm is created with the correct credentials and test the connection to make sure you can reach the authentication server; also ensure that a policy object or objects are configured for authentication.
2. Check the output of the **show service-policy cxsc** command to see if any packets were proxied.
3. Perform a packet capture on the backplane, and check to see if traffic is being redirected on the correct configured port. See the "Capturing Module Traffic" section on page 1-20. You can check the configured port using the **show running-config cxsc** command or the **show asp table classify domain cxsc-auth-proxy** command.

Note If you have a connection between hosts on two ASA interfaces, and the ASA CX service policy is only configured for one of the interfaces, then all traffic between these hosts is sent to the ASA CX module, including traffic orginiating on the non-ASA CX interface (the feature is bidirectional). However, the ASA only performs the authentication proxy on the interface to which the service policy is applied, because this feature is ingress-only.

Example 1-1 Make sure port 2000 is used consistently:

1. Check the authentication proxy port:

```
hostname# show running-config cxsc
cxsc auth-proxy port 2000
```

2. Check the authentication proxy rules:

```
hostname# show asp table classify domain cxsc-auth-proxy

Input Table
in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=inside, output_ifc=identity
```

3. In the packet captures, the redirect request should be going to destination port 2000.

Feature History for the ASA CX Module

Table 1-2 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 1-2 Feature History for the ASA CX Module

Feature Name	Platform Releases	Feature Information
ASA 5585-X support for the ASA CX SSP	8.4(4.1)	ASA CX module lets 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), the time of the attempted access (when), and the properties of the device used for the access (how). With the ASA CX module, 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. We introduced the following screens: Home > ASA CX Status Wizards > Startup Wizard > ASA CX Basic Configuration Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > ASA CX Inspection *This feature is not available in Version 8.6(1).*