Cisco Firepower 4100/9300 FXOS Hardening Guide

First Published: 2019-05-10

Last Modified: 2023-02-10

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

CHAPTER 1

Introduction

This document provides information to help you harden your Cisco Firepower eXtensible Operating System (FXOS) on 4100 and 9300 platform devices, which increases the overall security of your network. For hardening information on other components of your Firepower deployment, see the following documents:

- Cisco Guide to Harden ASA Firewall
- Cisco Firepower Management Center Hardening Guide, Version 6.4
- Cisco Firepower Threat Defense Hardening Guide, Version 6.4

The three functional planes of a network - the management, control, and data planes, each provide a different functionality that must be protected.

Management Plane
The management plane contains the logical group of all traffic that supports provisioning, maintenance, and monitoring functions for Cisco FXOS. Traffic in this group includes HTTP/HTTPS, SSH, FTP, Simple Network Management Protocol (SNMP), Syslog, TACACS+, Remote Authentication Dial-In User Service (RADIUS), and DNS. Management plane traffic is always destined to the local Cisco FXOS.

Control Plane
The control plane contains the logical group of all switching, signaling, link-state, and other control protocols that are used to create and maintain the state of the network and interfaces such as Link Layer Discovery Protocol (LLDP), and Link Aggregation Control Protocol (LACP). Control plane traffic is always destined to the local Cisco FXOS device.

Data Plane
The data plane contains the logical group of customer application traffic generated by hosts, clients, servers, and applications that are sourced from and destined to other similar devices supported by the network.

This document is structured in three sections:

- Secure Network Operations
- Management Plane Hardening
- User Management

Although most of this document is devoted to secure configuration of a Cisco FXOS device, configurations alone do not completely secure a network. The operational procedures in use on the network, as well as the people who administer the network, contribute as much to security as the configuration of the underlying devices. Where possible and appropriate, this document contains recommendations that, if implemented, help secure a Cisco FXOS deployment.

- Security Certifications Compliance, on page 2

Security Certifications Compliance

Note that your organization might be required to use only equipment and software that comply with security standards established by the U.S. Department of Defense or other governmental certification organizations.

When configured in accordance with certification-specific guidance documents the Firepower System supports compliance with the following certification standards:

- Common Criteria (CC): a global standard established by the international Common Criteria Recognition Arrangement, defining requirements for security products.
- Department of Defense Information Network Approved Products List (DoDIN APL): a list of products meeting security requirements established by the U.S. Defense Information Systems Agency (DISA). NOTE: The U.S. Government has changed the name of the Unified Capabilities Approved Products List (UCAPL) to the DoDIN APL. References to UCAPL in Firepower documentation and the Firepower Management Center web interface can be interpreted as references to DoDIN APL.
- Federal Information Processing Standards (FIPS) 140: a requirements specification for encryption modules.

Certification guidance documents are available separately once product certifications have completed; publication of this hardening guide does not guarantee completion of any of these product certifications.

CHAPTER 2

Secure Network Operations

Securing network operations is a substantial topic. Although most of this document is devoted to the secure configuration of a Firepower 4100/9300 device running FXOS, configurations alone do not completely secure a network. The operational procedures in use on the network, as well as the people who administer the network, contribute as much to security as the configuration of the underlying devices.

The following sections contain operational recommendations that FXOS administrators are advised to implement. These sections highlight specific critical areas of network operations and are not comprehensive.

- Monitor Cisco Security Advisories, on page 3
- Update to Latest Version of FXOS, on page 3
- Customize the Pre-Login Banner, on page 4
- Enable Common Criteria or FIPS Mode , on page 4
- Secure the Network Time Protocol (NTP), on page 5
- Secure the Domain Name System (DNS), on page 5
- Leverage Authentication, Authorization, and Accounting, on page 5
- Use Secure Protocols, on page 6
- Configuration Management, on page 6

Monitor Cisco Security Advisories

The Cisco Product Security Incident Response Team (PSIRT) creates and maintains publications, commonly referred to as Cisco Security Advisories, for security-related issues in Cisco products. Security advisories are available at http://www.cisco.com/go/psirt.

For information about Cisco PSIRT vulnerability reporting, see the Cisco Security Vulnerability Policy.

To maintain a secure system, Cisco FXOS administrators should be aware of the information communicated in Cisco Security Advisories. Detailed knowledge of the vulnerability is required before evaluating the threat that the vulnerability can pose to a network. For assistance with this evaluation process, see Risk Triage for Security Vulnerability Announcements.

Update to Latest Version of FXOS

Important security updates are included in each new platform bundle release of FXOS. We recommend you update your FXOS system to the latest available version as soon as possible.

For more information on supported compatibility and upgrade paths for FXOS in various configurations, see the *Cisco Firepower 4100/9300 FXOS Compatibility* guide and the *Cisco Firepower 4100/9300 Upgrade Guide* on Cisco.com.

Customize the Pre-Login Banner

You can specify the message that FXOS displays to users before they log into Firepower Chassis Manager or the FXOS CLI. From a hardening perspective, this message should be used to discourage unauthorized access.

The following CLI example creates a pre-login banner for the FXOS Chassis Manager and FXOS CLI:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
 You must have explicit, authorized permission to access or configure this device.
 Unauthorized attempts and actions to access or use this system may result in civil and/or

criminal penalties.
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

Enable Common Criteria or FIPS Mode

If your organization is required to use only equipment and software that comply with security standards established by the U.S. Department of Defense or other governmental certification organizations, you can enable Common Criteria or FIPS mode to apply multiple hardening changes with a single setting. Note that if your organization is not required to comply with security certifications compliance standards, you may still enable FIPS or Common Criteria modes for FXOS, but be aware that this may cause compatibility issues on your device.

The options to enable Common Criteria or FIPS mode appear under **Platform Settings** > **FIPS/Common Criteria** mode in the Firepower Chassis Manager web interface.

Note

- Enabling security certifications compliance does not guarantee strict compliance with all requirements of the security mode selected. Additional settings recommended to harden your deployment above and beyond those provided by Common Criteria or FIPS modes are described in this document. For full information on hardening procedures required for complete compliance, refer to the guidelines for this product provided by the certifying entity.
- Use FIPS compliant tool for device access when FIPS, Common Criteria, or both are enabled.

Secure the Network Time Protocol (NTP)

We strongly recommend using a trusted Network Time Protocol (NTP) server to synchronize system time on your Firepower 4100/9300 FXOS device and its associated servers.

To enable NTP for FXOS, you must first generate NTP key IDs and key values, then add the NTP server to the FXOS chassis using the following workflow in FXOS Chassis Manager: **Platform Settings** > **Set Time Source** > **Use NTP Server**. To further harden NTP, configure NTP server authentication.

For full instructions on how to configure an NTP server and NTP server authentication for FXOS, see the Setting the Date and Time Using NTP topic of the Platform Settings chapter in the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.

Note

- When enabled, the NTP authentication feature is global for all configured servers associated with FXOS.
- Only SHA1 is supported for NTP server authentication.
- You need the key ID and the key value to authenticate a server. The key ID is used to tell both the client and server which key value to use when computing the message digest. The key value is a fixed value that is derived using nip-keygen.

Secure the Domain Name System (DNS)

Computers communicating with each other in a networked environment depend on the DNS protocol to provide mapping between IP addresses and host names.

DNS can be susceptible to specific types of attacks tailored to take advantage of weak points in a DNS server that is not configured with security in mind. Be sure your local DNS server is configured in keeping with industry-recommended best practices for security; Cisco offers guidelines in this document: https://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html.

Leverage Authentication, Authorization, and Accounting

The Authentication, Authorization, and Accounting (AAA) framework is critical to securing interactive access to network devices. The AAA framework provides a highly configurable environment that can be tailored based on the needs of the network.

RADIUS and TACACS+ are both supported on the FXOS system. TACACS+ encrypts the entire TCP payload, which includes both the username and password. Radius encrypts only the password. Additionally, TACACS+ provides for command authorization, whereas RADIUS only provides authentication and accounting. Therefore, we suggest you use TACACS+ for maximum authentication security.

Additionally, you can use LDAP for user authentication. To encrypt the LDAP authentication exchange, use the CLI option to use SSL.

```
Firepower /security/ldap/server # set ssl yes
```

For more information and complete procedures on how to configure AAA, see the "Configuring AAA" section of the Platform Settings chapter in the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.

Use Secure Protocols

Cisco FXOS uses many protocols in order to carry sensitive network management data. You must use secure protocols whenever possible. A secure protocol choice includes the use of SSH instead of Telnet so that both authentication data and management information are encrypted. In addition, you must use secure file transfer protocols when you copy configuration data. For example, the use of Secure Copy Protocol (SCP) in place of FTP or TFTP. For additional details on how to use secure protocols, see the Management Plane, on page 7 section of this document.

Configuration Management

Configuration management is a process by which configuration changes are proposed, reviewed, approved, and deployed.

The configuration of a Cisco FXOS device contains many sensitive details, including usernames, passwords, and the contents of access control lists (ACLs). The repository used to archive Cisco FXOS device configurations should be secured and access should be restricted to only those roles and functions that require access. Insecure access to this information can undermine the security of the entire network.

CHAPTER 3

Management Plane

The management plane consists of functions that achieve the management goals of the network. These goals include interactive management sessions using SSH, as well as statistics gathering with SNMP. When considering the security of a network device, it is critical that the management plane be protected. If a security incident undermines the functions of the management plane, network recovery or stabilization may not be possible.

The following sections detail the security features and configurations available in Cisco FXOS that help fortify the management plane:

- Harden the Management Plane, on page 7
- Control and Encrypt Management Sessions, on page 8
- Install a Trusted Identity Certificate, on page 8
- Certificates, Key Rings, and Trusted Points, on page 9
- Configure HTTPS, on page 10
- Configure SSH, on page 10
- Secure SNMP, on page 11
- Secure Syslog, on page 12
- Configure the IP Access List, on page 12
- Configure IPSec Secure Channel, on page 12
- About the Certificate Revocation List Check, on page 13
- Configure Static CRL for a Trustpoint, on page 17

Harden the Management Plane

The management plane is used to access, configure, and manage a device, as well as monitor its operations and the network on which it is deployed. The management plane receives and sends traffic for operations of these functions. Both the management plane and control plane of a device must be secured, because operations of the control plane directly affect operations of the management plane. The following list includes protocols used by the management plane:

- SNMP
- Telnet
- SSH
- SFTP

- FTP
- TFTP
- HTTP/HTTPS
- Secure Copy Protocol (SCP)
- TACACS+
- RADIUS
- LDAP
- Network Time Protocol (NTP)
- Syslog

Administrators must take measures to ensure the integrity of the management and control planes during security incidents. If one of these planes is successfully exploited, all planes can be compromised.

Control and Encrypt Management Sessions

Because information can be disclosed during an interactive management session, traffic must be encrypted so that a malicious user cannot read the data that is being transmitted. Encrypting the traffic allows a secure remote access connection to the device. If the traffic for a management session is sent over the network in plain text, an attacker could obtain sensitive information about the device and the network. The following protocols are supported on FXOS:

- SSH
- TLS
- HTTPS
- SNMP
- LDAP
- Telnet

Note Telnet is not a secure protocol, and we advise administrators of FXOS not to use it.

The following sections detail hardening configuration options for management session protocols.

Install a Trusted Identity Certificate

After initial configuration, a self-signed SSL certificate is generated for use with the FXOS chassis web application. Because that certificate is self-signed, client browsers do not automatically trust it. The first time a new client browser accesses the FXOS chassis web interface, the browser will throw an SSL warning, requiring the user to accept the certificate before accessing the FXOS chassis. You must generate a Certificate Signing Request (CSR) using the FXOS CLI and install the resulting identity certificate for use with the FXOS chassis. This identity certificate allows a client browser to trust the connection, and bring up the web interface with no warnings.

For the full procedure on installing a trusted identity certificate, see the "Install a Trusted Identity Certificate" topic in the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.

Certificates, Key Rings, and Trusted Points

HTTPS uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices, such as a client's browser and the Firepower 9300 chassis.

Encryption Keys and Key Rings

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys, one kept private and one made public, stored in an internal key ring. A message encrypted with either key can be decrypted with the other key. To send an encrypted message, the sender encrypts the message with the receiver's public key, and the receiver decrypts the message using its own private key. A sender can also prove its ownership of a public key by encrypting (also called 'signing') a known message with its own private key. If a receiver can successfully decrypt the message using the public key in question, the sender's possession of the corresponding private key is proven. Encryption keys can vary in length, with typical lengths from 512 bits to 2048 bits. In general, a longer key is more secure than a shorter key. FXOS provides a default key ring with an initial 2048-bit key pair, and allows you to create additional key rings.

The default key ring certificate must be manually regenerated if the cluster name changes or the certificate expires.

Certificates

To prepare for secure communications, two devices first exchange their digital certificates. A certificate is a file containing a device's public key along with signed information about the device's identity. To merely support encrypted communications, a device can generate its own key pair and its own self-signed certificate. When a remote user connects to a device that presents a self-signed certificate, the user has no easy method to verify the identity of the device, and the user's browser will initially display an authentication warning. By default, FXOS contains a built-in self-signed certificate containing the public key from the default key ring.

Trusted Points

To provide stronger authentication for FXOS, you can obtain and install a third-party certificate from a trusted source, or trusted point, that affirms the identity of your device. The third-party certificate is signed by the issuing trusted point, which can be a root certificate authority (CA) or an intermediate CA or trust anchor that is part of a trust chain that leads to a root CA. To obtain a new certificate, you must generate a certificate request through FXOS and submit the request to a trusted point.

Important The certificate must be in Base64 encoded X.509 (CER) format.

Configure HTTPS

Use the following workflow to configure and harden HTTPS on your FXOS chassis:

1. Create a key ring (see the "Creating a Key Ring" topic in the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*).

2. Create a certificate request for a key ring (see the "Creating a Certificate Request for a Key Ring with Advanced Options" topic in the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*).

3. Create a trusted point (see the "Creating a Trusted Point" topic in the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*).

4. Import the certificate into the key ring (see the "Importing a Cerificate Into a Key Ring" topic in the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*).

Use the following additional options to harden HTTPS:

- Specify the level of Cipher Suite security used by the domain (**set https cipher-suite-mode**). We recommend a value of **strong** or **custom**. If you choose custom, you must specify a custom level of Cipher Suite security for the domain (**set https cipher-suite** *cipher-suite-spec-string*).

- Enable the certificate revocation list check.

Configure SSH

We recommend using SSHv2, which is enabled by default using TCP port 22. Note the following SSH hardening configuration options that can be enabled on the server and client:

RSA Key Strength (set ssh-server host-key rsa/set ssh-client host-key rsa)

The modulus value (in bits) is in multiples of 8 from 1024 to 2048. The larger the key modulus size you specify, the longer it takes to generate an RSA key pair. We recommend a value of 2048.

Encryption Algorithms (set ssh-server encrypt-algorithm/set ssh-client encrypt-algorithm)

The following encryption algorithms are supported on FXOS:

```
3des-cbc    3DES  CBC
aes128-cbc  AES128 CBC
aes128-ctr  AES128 CTR
aes192-cbc  AES192 CBC
aes192-ctr  AES192 CTR
aes256-cbc  AES256 CBC
aes256-ctr  AES256 CTR
```

Note 3des-cbc is not Common Criteria-compliant.

Diffie-Hellman Key Exchange Algorithm (set ssh-server kex-algorithm/set ssh-client kex-algorithm)

The DH key exchange provides a shared secret that cannot be determined by either party alone. The key exchange is combined with a signature and the host key to provide host authentication. This key-exchange method provides explicit server authentication. For more information about using DH key-exchange methods, see RFC 4253.

The following DH algorithms are supported on FXOS:

```
diffie-hellman-group14-sha1  Diffie-Hellman Group14 SHA1
```

Server and Client MAC Algorithms (set ssh-server mac-algorithm/set ssh-client mac-algorithm)

The following MAC algorithms are supported on FXOS:

```
hmac-sha1      Hmac SHA1
hmac-sha2-256  HMAC SHA2 256
hmac-sha2-512  HMAC SHA2 512
```

Volume Rekey Limit (set ssh-server rekey-limit volume/set ssh-client rekey-limit volume)

Determines the amount of traffic in KB allowed over the connection before FXOS disconnects from the session.

Time Rekey Limit (set ssh-server rekey-limit time/set ssh-client rekey-limit time)

Determines the number of minutes that an SSH session can be idle before FXOS disconnects the session.

Set Strict Host Key Check (set ssh-client stricthostkeycheck)

Controls SSH host key checking:

- **enable** - The connection is rejected if the host key is not already in the FXOS known hosts file. You must manually add hosts using the FXOS CLI command **enter ssh-host** in the system/services scope.
- **prompt** - You are prompted to accept or reject the host key if it is not already stored on the chassis.
- **disable** - (The default) The chassis accepts the host key automatically if it was not stored before.

For complete procedures about configuring SSH on your FXOS chassis, see the Platform Settings chapter in the *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide*, and the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.

Secure SNMP

It is critical that your Simple Network Management Protocol (SNMP) be properly secured to protect the confidentiality, integrity, and availability of both the network data and the network devices through which this data transits. SNMP provides you with a wealth of information on the health of network devices. This information should be protected from malicious users that want to leverage this data to perform attacks against the network.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

SNMP community strings are passwords that are applied to the FXOS chassis to restrict both read-only and read-write access to the SNMP data on the device. These community strings, as with all passwords, should be carefully chosen to ensure they are not trivial. Community strings should be changed at regular intervals and in accordance with network security policies. For example, the strings should be changed when a network administrator changes roles or leaves the company.

For more information about supported levels of SNMP security models and levels, see the "Configure SNMP" section in the Platform Settings chapter of the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.

Secure Syslog

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. A syslog service accepts messages and stores them in files, or prints them according to a simple configuration file. This form of logging provides protected long-term storage for logs. Logs are useful both in routine troubleshooting and incident handling.

Sending logging information to a remote syslog server makes it possible to correlate and audit network and security events across network devices more effectively. Note that syslog messages are transmitted in cleartext. For this reason, any protections that a network affords to management traffic (for example, encryption or out-of-band access) should be extended to include syslog traffic. To ensure that syslog traffic is never sent in clear text over untrusted networks, you can configure IPSec secure channel. IPSec provides end-to-end data encryption and authentication service on data packets going through the public network.

For more information on how to configure syslog on your FXOS chassis, see the Configuring Syslog section of the Platform Settings chapter in the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*. For more information on how to configure IPSec, see the Configure IPSec Secure Channel topic in the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.

Configure the IP Access List

By default, the FXOS chassis denies all access to the local web server. You must configure your IP Access List with the IP addresses of the hosts or subnets that are allowed for each protocol.

The IP Access List supports the following protocols:

- HTTPS
- SSH
- SNMP

For each list of IP addresses (v4 or v6), up to 100 different subnets can be configured for each service. A subnet of 0 and a prefix of 0 allows unrestricted access to a service.

For more information and complete procedures about configuring IP Access Lists on your FXOS chassis, see the "Configure the IP Access List" topic in the Platform Settings chapter of the *Cisco Firepower 4100/9300 FXOS Chassis Manager Configuration Guide*, and the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.

Configure IPSec Secure Channel

Configure IPSec on your Firepower 4100/9300 chassis to provide end-to-end data encryption and authentication service on data packets going through the public network.

Note If you are using an IPSec secure channel in FIPS mode, the IPSec peer must support RFC 7427.

For full instructions on how to configure an IPSec Secure Channel for your FXOS chassis, see the "Configure IPSec Secure Channel" topic in the Security Certifications Compliance chapter of the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.

About the Certificate Revocation List Check

You can configure your Certificate Revocation List (CRL) check mode to be either strict or relaxed in IPSec, HTTPS, and secure LDAP connections.

FXOS harvests dynamic (non-static) CRL information from the CDP information of an X.509 certificate, which indicates dynamic CRL information. System administration downloads static CRL information manually, which indicates local CRL information in the FXOS system. FXOS processes dynamic CRL information against the current processing certificate in the certificate chain. The static CRL is applied to the whole peer certificate chain.

For steps to enable or disable certificate revocation checks for your secure IPSec, LDAP, and HTTPS connections, see Configure IPSec Secure Channel, Creating an LDAP Provider and Configuring HTTPS.

Note

- If the Certificate Revocation Check Mode is set to Strict, static CRL is only applicable when the peer certificate chain has a level of 1 or higher. (For example, when the peer certificate chain contains only the root CA certificate and the peer certificate signed by the root CA.)
- When configuring static CRL for IPSec, the Authority Key Identifier (authkey) field must be present in the imported CRL file. Otherwise, IPSec considers it invalid.
- Static CRL takes precedence over Dynamic CRL from the same issuer. When FXOS validates the peer certificate, if a valid (determined) static CRL of the same issuer exists, FXOS ignores the CDP in the peer certificate.
- Strict CRL checking is enabled by default in the following scenarios:
  - Newly created secure LDAP provider connections, IPSec connections, or Client Certificate entries
  - Newly deployed FXOS chassis managers (deployed with an initial starting version of FXOS 2.3.1.x or later)

The following tables describe the connection results, depending on your certificate revocation list check setting and certificate validation.

Table 1: Certificate Revocation Check Mode set to Strict without a local static CRL

Without local static CRL	LDAP Connection	IPSec Connection	Client Certificate Authentication
Checking peer certificate chain	Full certificate chain is required	Full certificate chain is required	Full certificate chain is required

Without local static CRL	LDAP Connection	IPSec Connection	Client Certificate Authentication
Checking CDP in peer certificate chain	Full certificate chain is required	Full certificate chain is required	Full certificate chain is required
CDP checking for Root CA certificate of the peer certificate chain	Yes	Not applicable	Yes
Any certificate validation failure in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message	Connection fails with syslog message
Any certificate revoked in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message	Connection fails with syslog message
One CDP is missing in the peer certificate chain	Connection fails with syslog message	Peer certificate: connection fails with syslog message Intermediate CAs: connection fails	Connection fails with syslog message
One CDP CRL is empty in the peer certificate chain with valid signature	Connection succeeds	Connection succeeds	Connection fails with syslog message
Any CDP in the peer certificate chain cannot be downloaded	Connection fails with syslog message	Peer certificate: Connection fails with syslog message Intermediate CA: connection fails	Connection fails with syslog message
Certificate has CDP, but the CDP server is down	Connection fails with syslog message	Peer certificate: Connection fails with syslog message Intermediate CA: connection fails	Connection fails with syslog message
Certifcate has CDP, server is up, and CRL is on CDP, but the CRL has an invalid signature	Connection fails with syslog message	Peer certificate: Connection fails with syslog message Intermediate CA: connection fails	Connection fails with syslog message

Table 2: Certificate Revocation Check Mode set to Strict with a local static CRL

With local static CRL	LDAP Connection	IPSec Connection
Checking peer certificate chain	Full certificate chain is required	Full certificate chain is required

With local static CRL	LDAP Connection	IPSec Connection
Checking CDP in peer certificate chain	Full certificate chain is required	Full certificate chain is required
CDP checking for Root CA certificate of the peer certificate chain	Yes	Not applicable
Any certificate validation failure in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message
Any certificate revoked in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message
One CDP is missing in the peer certificate chain (Certificate Chain level is 1)	Connection succeeds	Connection succeeds
One CDP CRL is empty in the peer certificate chain (Certificate Chain level is 1)	Connection succeeds	Connection succeeds
Any CDP in the peer certificate chain cannot be downloaded (Certificate Chain level is 1)	Connection succeeds	Connection succeeds
Certificate has CDP, but the CDP server is down (Certificate Chain level is 1)	Connection succeeds	Connection succeeds
Certificate has CDP, server is up, and CRL is on CDP, but the CRL has an invalid signature (Certificate Chain level is 1)	Connection succeeds	Connection succeeds
Peer Certificate Chain level is higher than 1	Connection fails with syslog message	If combined with CDP, connection succeeds If there is no CDP, connection fails with syslog message

Table 3: Certificate Revocation Check Mode set to Relaxed without a local static CRL

Without local static CRL	LDAP Connection	IPSec Connection	Client Certificate Authentication
Checking peer certificate chain	Full certificate chain	Full certificate chain	Full certificate chain
Checking CDP in the peer certificate chain	Full certificate chain	Full certificate chain	Full certificate chain

Without local static CRL	LDAP Connection	IPSec Connection	Client Certificate Authentication
CDP checking for Root CA certificate of the peer certificate chain	Yes	Not applicable	Yes
Any certificate validation failure in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message	Connection fails with syslog message
Any certificate revoked in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message	Connection fails with syslog message
One CDP is missing in the peer certificate chain	Connection succeeds	Connection succeeds	Connection fails with syslog message
One CDP CRL is empty in the peer certificate chain with valid signature	Connection succeeds	Connection succeeds	Connection succeeds
Any CDP in the peer certificate chain cannot be downloaded	Connection succeeds	Connection succeeds	Connection succeeds
Certificate has CDP, but the CDP server is down	Connection succeeds	Connection succeeds	Connection succeeds
Certificate has CDP, server is up, and CRL is on CDP, but the CRL has an invalid signature	Connection succeeds	Connection succeeds	Connection succeeds

Table 4: Certificate Revocation Check Mode set to Relaxed with a local static CRL

With local static CRL	LDAP Connection	IPSec Connection
Checking peer certificate chain	Full certificate chain	Full certificate chain
Checking CDP in the peer certificate chain	Full certificate chain	Full certificate chain
CDP checking for Root CA certificate of the peer certificate chain	Yes	Not applicable
Any certificate validation failure in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message
Any certificate revoked in the peer certificate chain	Connection fails with syslog message	Connection fails with syslog message

With local static CRL	LDAP Connection	IPSec Connection
One CDP is missing in the peer certificate chain (Certificate Chain level is 1)	Connection succeeds	Connection succeeds
One CDP CRL is empty in the peer certificate chain (Certificate Chain level is 1)	Connection succeeds	Connection succeeds
Any CDP in the peer certificate chain cannot be downloaded (Certificate Chain level is 1)	Connection succeeds	Connection succeeds
Certificate has CDP, but the CDP server is down (Certificate Chain level is 1)	Connection succeeds	Connection succeeds
Certificate has CDP, server is up, and CRL is on CDP, but the CRL has an invalid signature (Certificate Chain level is 1)	Connection succeeds	Connection succeeds
Peer Certificate Chain level is higher than 1	Connection fails with syslog message	If combined with CDP, connection succeeds If there is no CDP, connection fails with syslog message

Configure Static CRL for a Trustpoint

Revoked certifications are kept in the Certification Revocation List (CRL). Client applications use the CRL to check the authentication of a server. Server applications utilize the CRL to grant or deny access requests from client applications which are no longer trusted.

You can configure your Firepower 4100/9300 chassis to validate peer certificates using Certification Revocation List (CRL) information.

Once you have configured to validate peer certificates using Certification Revocation List information, you can also configure your system to periodically download a CRL so that a new CRL is used every 1 to 24 hours to validate certificates.

For detailed instructions on how to configure a Certification Revocation List for a trustpoint, see the "Configure Static CRL for a Trustpoint" topic in the Security Certifications Compliance chapter of the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.

CHAPTER 4

Secure Role-Based Access Control

User roles are assigned privileges that define what that user can do on the system. The system contains the following user roles:

Administrator

Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed.

Read-Only

Read-only access to system configuration with no privileges to modify the system state.

Operations

Read-and-write access to NTP configuration, Smart Call Home configuration for Smart Licensing, and system logs, including syslog servers and faults. Read access to the rest of the system.

AAA Administrator

Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.

Using the FXOS Chassis Manager web interface or FXOS CLI, you can configure the following settings for each user account on the system:

- User Role - the role that represents the privileges you want to assign to the user account.

  All users are assigned the Read-Only role by default and this role cannot be deselected. To assign multiple roles, hold down `Ctrl`+ click the desired roles.

- Account Expiration Date

- Account Status - if the status is set to **Active**, the user can log into Firepower Chassis Manager and the FXOS CLI with their login ID and password.

For maximum security on locally-authenticaed accounts, configure SSH for encrypted sessions.

- Password Management, on page 20
- Harden Locally Authenticated User Accounts, on page 20
- Harden Remotely Authenticated User Accounts, on page 20

Password Management

Passwords control access to resources or devices, and administrators define passwords to authenticate requests. When FXOS recieves a request for access to a resource or device, the request is challenged for verification of the password and identity, and access is granted, denied, or limited based on the result. Security best practices dictate that passwords should be managed with an LDAP, TACACS+ or RADIUS authentication server. However, a locally configured password for access is still required in the event that LDAP, TACACS+ or RADIUS services fail. A device can also have other password information present within its configuration, such as an NTP key, or a SNMP community string.

Harden Locally Authenticated User Accounts

When configuring individual internal user roles, admin account users can use the following settings to harden the system against attacks through web interface login mechanisms:

- Set the maximum number of failed login attempts allowed before a user is locked out of the Firepower 4100/9300 chassis for a specified amount of time (**set max-login-attempts**)
- Set the amount of time the user should remain locked out of the system after exceeding the maximum number of login attempts (**set user-account-unlock-time**)
- Enforce a minimum password length (**set min-password-length**)
- Specify the minimum number of hours that a locally authenticated user must wait before changing a newly created password (**set no-change-interval**)
- Set the number of days local user accounts are valid (**set expiration**)
- Require strong passwords (**set enforce-strong-password yes**)
- Assign user access privileges appropriate only to the type of access the user requires (**create role**)

Harden Remotely Authenticated User Accounts

A remotely authenticated user account is any user account that is authenticated through LDAP, RADIUS, or TACACS+. Remote authentication allows for a maximum of 16 TACACS+ servers, 16 RADIUS servers, and 16 LDAP providers for a total of 48 providers.

AAA is a set of services for controlling access to computer resources, enforcing policies, assessing usage, and providing the information necessary to bill for services. These processes are considered important for effective network management and security.

Note that if a user maintains a local user account and a remote user account simultaneously, the roles defined in the local user account override those maintained in the remote user account.

TACACS+ is an authentication protocol that the FXOS chassis can use to authenticate management users against a remote AAA server. These management users can access the FXOS chassis via SSH, HTTPS, telnet, or HTTP. We recommend SSH for maximum security when accessing the FXOS chassis. Numerous authentication methods provide enhanced security.

TACACS+ authentication, or more generally AAA authentication, provides the ability to use individual user accounts for each network administrator. When you do not depend on a single shared password, the security of the network is improved and your accountability is strengthened.

RADIUS is a protocol similar in purpose to TACACS+; however, it encrypts only the password sent across the network. In contrast, TACACS+ encrypts the entire TCP payload, which includes both the username and password. For this reason, we recommend that you use TACACS+ in preference to RADIUS when TACACS+ is supported by the AAA server.

LDAP is a client-server protocol for accessing directory services, such as Microsoft Active Directory. LDAP does not require any security between the client and server. However, through the use of SSL, LDAP can encrypt user sessions between the client and server. This keeps all information transferred in LDAP transactions over the network secure. For this reason, we strongly recommend that you use LDAP in preference to TLS.

For more information and detailed procedures on how to configure RADIUS, TACAS+, and LDAP on your FXOS chassis, see the Configuring AAA section in the Platform Settings chapter of the *Cisco Firepower 4100/9300 FXOS CLI Configuration Guide*.