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

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*.