Security

Security features

Hewlett Packard Enterprise recommends following security best practices by protecting and isolating management networks from production data networks. To ensure high availability, and to guard against various network attacks, isolate the HPE Synergy Composer management network using the appropriate mechanisms such as firewalls and intrusion detection systems.

To ensure a secure platform for data center management, the frame link module includes features such as the following.

- Separation of the data and management environments, which is critical to protect against Denial of Service (DoS) attacks.
- Protection against DoS attacks on the management ring with traffic prioritization and rate limiting.
- Audit logging of all frame link module activity.
- Verification of certificates for Transport Layer Security (TLS).
- Hardware enforced write protection to ensure integrity and prevent unauthorized modification of the currently running frame link module firmware image.

HPE Synergy 4-Port Frame Link Module security features

- Hardware Root of Trust ensures that only firmware signed by Hewlett Packard Enterprise can be used to boot the frame link module.
- Management data stored on the frame link module is encrypted by default. The encryption is rooted in the integrated Trusted Platform Module (TPM) present on the HPE Synergy 4-Port Frame Link Module.

Frame link module and HPE OneView certificate validation

When HPE OneView claims a frame link module, a certificate is presented to HPE OneView. HPE OneView uses this certificate to verify that it is communicating with a frame link module. These certificates can be reviewed in the **FLM Certificates** section of the HPE Synergy Console.

To verify that the certificates match, compare the values in HPE OneView with the values in the HPE Synergy Console.

For information about verifying the certificate in HPE OneView, see "Automatic initial trust" in the *HPE OneView User Guide for HPE Synergy* (**http://www.hpe.com/info/synergy-docs**). Certificate validation information is also available by clicking the **?** icon on the HPE OneView **Manage Certificates** screen.

Verifying a frame link module certificate

To verify that the certificates match, compare the values in HPE OneView with the values in the HPE Synergy Console.

Procedure

1. Log in to HPE OneView.
2. Select **Settings** > **Security**.

   Make note of these attributes for comparison.

   - Fingerprints
   - Names

- Serial number
- Validity dates

3. Connect to an HPE Synergy Console.
4. Navigate to the **Frame Health & Inventory** screen.

   The frame link module certificates are located in the **FLM Certificates** section at the bottom on the screen.
5. Compare the certificates and verify that they match.

Frame link module ports required for HPE Synergy 12000 Frame management network

HPE Synergy Frame Link Module requires specific ISO layer 4 ports to be available to the appliance to communicate with HPE OneView, compute modules, frames, and interconnects.

Port Number	Protocol	Direction	Description
22	TCP6	Inbound	HPE OneView uses SSH to communicate with FLM.
22	TCP6	Outbound	FLM uses SSH to communicate with HPE iLO.
123	UDP6	Outbound	FLM uses NTP service hosted on HPE OneView.
443	TCP6	Inbound	HPE OneView uses HTTPS to manage the frame.
443	TCP6	Outbound	FLM sends management events to OneView.

Ports required by the frame link module front panel network

The front panel laptop port is an RJ45 connector located on the HPE Synergy 12000 Frame Front Panel. It allows a single laptop to connect to the HPE Synergy Console for initial hardware setup and troubleshooting. This is a private network and is isolated from all other networks.

Port Number	Protocol	Direction	Description
67	UPD4	Inbound	External device obtains address from FLM DHCP Server.
68	UDP4	Outbound	FLM responds to DHCP request

Table Continued

Port Number	Protocol	Direction	Description
5800	TCP4	Inbound	External device connects to NoVNC data stream. Loads NoVNC web page.
5900	TCP4	Inbound	External device obtains VNC HTML5 client. VNC protocol, not HTML.

Compliance

The HPE Synergy Frame Link Module is compliant with the HPE security policies such as code signing and is free from malware and backdoors.

Authentication

HPE OneView uses a secure communication channel to communicate with the frame link module. When HPE OneView claims a frame link module, it changes the authentication credentials and other settings. HPE OneView retains the credentials for accessing the frame link module.

Default algorithms supported by the frame link module

This section lists the algorithms that are enabled by default after a factory reset for each version of the frame link module firmware. If a version is not listed, then there were no changes from the version last listed.

NOTE: Upgrading from one firmware version to the next version generally maintains the settings from the previous version. For example, if a frame link module with 2.00 firmware is upgraded to a future version that disables TLS 1.1, then TLS 1.1 will remain enabled until the frame link module is reset to factory defaults or explicitly disabled.

TLS protocols

Protocol	FLM-2.00, FLM-2.01, FLM-2.02, FLM-2.04, FLM-3.00
TLS 1.0	Disabled
TLS 1.1	Enabled
TLS 1.2	Enabled

TLS ciphers

RFC Cipher Name	FLM-2.00, FLM-2.01	FLM-2.02, FLM-2.04, FLM 3.00
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Enabled	Enabled
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Enabled	Enabled
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Enabled	Enabled

Table Continued

RFC Cipher Name	FLM-2.00, FLM-2.01	FLM-2.02, FLM-2.04, FLM 3.00
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	Enabled	Enabled
TLS_RSA_WITH_AES_256_GCM_SHA384	Enabled	—
TLS_RSA_WITH_AES_256_CBC_SHA256	Enabled	—
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Enabled	Enabled
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Enabled	Enabled
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Enabled	Enabled
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Enabled	Enabled
TLS_RSA_WITH_AES_128_GCM_SHA256	Enabled	—
TLS_RSA_WITH_AES_128_CBC_SHA256	Enabled	—
TLS_RSA_WITH_AES_256_CBC_SHA	Enabled	—
TLS_RSA_WITH_AES_128_CBC_SHA	Enabled	—

TLS Certificates

The default key sizes for self-signed and certificate signing requests are:

- RSA: 3072 bits, SHA 384
- ECDSA: 384 bits, SHA384

When obtaining a CA signed certificate, ensure that the leaf, intermediate, and root are signed using SHA256 or better. Likewise ensure that all intermediates and root key lengths are greater than or equal to 2048 bit for RSA keys and 256 bits for ECDSA keys.

SSH Host Keys

Frame link module version	Enabled by default
FLM 2.01	ECDSA/384, RSA/3072, ED25519/256
FLM 2.02	ECDSA/384, RSA/3072
FLM 2.04, FLM 3.00	RSA/3072

SSH Key Exchange

	FLM-2.00, FLM-2.01, FLM-2.02	FLM-2.04, FLM-3.00
ecdh-sha2-nistp256	Enabled	Enabled
ecdh-sha2-nistp384	Enabled	Enabled
ecdh-sha2-nistp521	Enabled	Enabled
diffie-hellman-group-exchange-sha256	Enabled	Enabled
diffie-hellman-group14-sha1	—	Enabled

SSH Message Authentication Code

	FLM-2.00, FLM-2.01, FLM-2.02	FLM-2.04, FLM-3.00
hmac-sha1	Enabled	Enabled
hmac-sha2-256	Enabled	Enabled
hmac-sha2-512	Enabled	Enabled

SSH Ciphers

	FLM-2.00, FLM-2.01, FLM-2.02	FLM-2.04, FLM-3.00
aes256-gcm@openssh.com	Enabled	Enabled
aes128-gcm@openssh.com	Enabled	Enabled
aes128-cbc	Enabled	Enabled
aes256-cbc	Enabled	Enabled
aes256-ctr	—	Enabled
chacha20-poly1305@openssh.com	Enabled	—