FIPS Compliance

For supported software information, click here.

You can operate Versa Operating System™ (VOS™) devices in Federal Information Processing Standards (FIPS) mode in environments that require FIPS compliance. This article provides information about FIPS compliance for VOS devices.

FIPS Compliance Overview

For VOS software images that are FIPS compliant, you can run VOS devices in FIPS mode. VOS devices running in FIPS mode meet the standards defined in the FIPS 140-2: Security Requirements for Cryptographic Modules publication for FIPS 140-2 Level 1 certification.

The FIPS 140-2 standard was created by the National Institute of Standards and Technology (NIST) to coordinate requirements and standards for cryptography modules that include hardware and software components. A device that meets the FIPS 140-2 standard has been tested and formally validated as compliant to the security standard by the United States and Canadian governments. In United States Federal organizations, you are often required to deploy FIPS-compliant devices that use cryptography modules to protect sensitive and valuable data. The use of FIPS-compliant networking equipment is also a common requirement for security-conscious government and non-government organizations worldwide that implement the standard in their networks as a security benchmark.

FIPS Compliance Implementation Details

All VOS software modules use a FIPS-compliant version of OpenSSL and have been modified to use FIPS-compliant APIs, with the following exception: the TLS/SSL proxy feature does not use FIPS-compliant OpenSSL and therefore is not FIPS compliant. All other components within the FIPS cryptographic boundary that are dependent on OpenSSL are FIPS compliant.

VOS software includes IPsec for encryption and cryptographic operation. All cryptographic algorithms in the VOS IPsec component are FIPS compliant.

The following changes take effect when you enable FIPS mode:

- Integrity checks are performed periodically on cryptographic modules and when the system restarts and reboots.
- Self-tests are executed when the system restarts and reboots.

- Conditional tests are executed when keys are generated.
- Selection of cryptographic keys, algorithms, and ciphers are restricted to FIPS-approved keys, algorithms, and ciphers.

FIPS-Compliant Ciphers and IPsec and IKE Transforms

For Releases 21.2 and later.

VOS devices support the following FIPS-compliant ciphers and IPsec and IKE transforms:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Enable FIPS Mode

By default, FIPS mode is disabled. To enable FIPS mode, issue the following CLI command:

```
% request system fips-mode enable
Restart all Versa services. Are you sure? [no,yes] yes
```

To enable FIPS mode, you must restart all Versa services. If you want to delay the restarting of Versa services to complete the FIPS mode change, answer **no** to the prompt and manually restart the Versa services at a later time.

To enable FIPS mode and automatically restart all services without being prompted, issue the following command:

> % **request system fips-mode enable no-confirm**

Disable FIPS Mode

If you have enabled FIPS mode, you can disable it by issuing the following command:

> % **request system fips-mode disable**
> Restart all Versa services. Are you sure? [no,yes] **yes**

To disable FIPS mode, you must restart all Versa services. If you want to delay the restarting of Versa services to complete the FIPS mode change, answer **no** to the prompt and manually restart the Versa services at a later time.

To disable FIPS mode and automatically restart all services without being prompted, issue the following command:

> % **request system fips-mode disable no-confirm**

Supported Software Information

Releases 21.1.1 and later support all content described in this article, except:

- Release 21.2 supports FIPS-compliant ciphers and IPsec and IKE transforms.

Additional Information

FIPS 140-2: Security Requirements for Cryptographic Modules