

Enable FIPS in the Local Policy

- About FIPS, NGE, and Cisco Secure Client, on page 1
- Configure FIPS for AnyConnect VPN, on page 4
- Configure FIPS for the Network Access Manager, on page 5

About FIPS, NGE, and Cisco Secure Client

Cisco Secure Client incorporates the Cisco Common Cryptographic Module (C3M). This Cisco SSL implementation includes Federal Information Processing Standard (FIPS) 140-2 compliant cryptography modules and National Security Agency (NSA) Suite B cryptography as part of its Next Generation Encryption (NGE) algorithms.

Next Generation Encryption introduces new encryption, authentication, digital signatures, and key exchange algorithms for escalating security and performance requirements. RFC 6379 defines the Suite B cryptography algorithms that must conform to meet U.S. FIPS 140-2 standards.

Cisco Secure Client components negotiate and use FIPS standard cryptography based on the configuration of the headend, the Secure Firewall ASA or the IOS router. The following Cisco Secure Client client modules support FIPS:

- AnyConnect VPN—FIPS compliance for the VPN client is enabled using a FIPS-mode parameter in the local policy file on the user computer. Suite B cryptography is available for TLS/DTLS and IKEv2/IPsec VPN connections. See Configure FIPS for the AnyConnect Core VPN Client for details and procedures.

  The AnyConnect local policy file, AnyConnectLocalPolicy.xml, contains additional security settings beyond FIPS-mode that apply to the local client. It is not deployed by the Secure Firewall ASA and must be installed manually, or deployed using an enterprise software deployment system. You also have the option to deploy this AnyConnectLocalPolicy.xml file from Secure Client Cloud Management. See The AnyConnect Local Policy for details on using this profile.

- Secure Firewall Posture—Just as AnyConnect VPN, FIPS compliance is enabled using a FIPS-mode parameter in the local policy file on the user computer.

- Cisco Secure Client Network Access Manager—FIPS compliance for the Network Access Manager is enabled using the FIPS-mode parameter in the configuration.xml file (located in C:\ProgramData\Cisco\Cisco Secure Client\Network Access Manager\System directory) and the FIPS-mode parameter in the Network Access Manager profile. FIPS for the Network Access Manager is supported on Windows. See Configure FIPS for the Network Access Manager for details and procedures.

FIPS Features in Cisco Secure Client



Note CiscoSSL 8 Exceptions

When FIPS mode is enabled, RSA-based cipher suites that do not provide Perfect Forward Secrecy are removed from the supported cipher list. Additionally, ECDH and MODP groups, which provide Perfect Forward Secrecy remain supported and are the preferred key exchange mechanisms under FIPS.

Feature	Core VPN Module	Network Access Manager Module
AES-GCM support for symmetric encryption and integrity.	128-, 192-, and 256-bit keys for IKEv2 payload encryption and authentication. ESP packet encryption and authentication.	128-bit and 256-bit keys for 802.1AE (MACsec) for wired traffic encryption in software (Windows).
AES-CBC encryption	128-, 192-, and 256-bit key sizes	128-, 192-, and 256-bit key sizes
SHA-2 support for hashing, SHA with 256/384/512 bits.	IKEv2 payload authentication and ESP packet authentication. (Windows 7 or later and macOS 10.7 or later).	Ability to use certificates with SHA-2 in TLS-based EAP methods.
SHA-1	IKEv2 PRF and integrity/authentication as well as PFS. IPsec/ESP integrity/authentication.	n/a
ECDH support for key exchange.	Groups 19, 20, and 21 IKEv2 key exchange and IKEv2 PFS.	Ability to use ECDH in TLS-based EAP methods (Windows).
MODP for key exchange (in addition to the ECDH support listed above)	Groups 15 and 16	Groups 15 and 16
ECDSA support for digital signature, asymmetric encryption, and authentication, 256-, 384-, 521-bit elliptic curves.	IKEv2 user authentication and server certificate verification.	Ability to use certificates with ECDSA in TLS-based EAP methods.
Pseudo Random Functions	SHA1, SHA256, SHA384, and SHA512	SHA1, SHA256, SHA384, and SHA512
Integrity algorithms	SHA1, SHA256, SHA384, and SHA512	SHA1, SHA256, SHA384, and SHA512

Feature	Core VPN Module	Network Access Manager Module
Diffie Hellman	Groups 15, 16, 19, 20, 21 (15 and 16 are the older Modular Exponential (MODP) DH groups, while 19, 20, and 21 are elliptical curve DH groups)	Groups 15, 16, 19, 20, 21 (15 and 16 are the older Modular Exponential (MODP) DH groups, while 19, 20, and 21 are elliptical curve DH groups)
Additional support:	All required crypto algorithms for IPsecV3 except for NULL encryption. RSA certificates with 4096 bit keys for TLS/DTLS and IKEv2.	n/a

[1] On Linux, only the Cisco Secure Client file store is supported for ECDSA. To add certificates to a file store, see .

[2] IPsecV3 also specifies that Extended Sequence Numbers (ESN) must be supported, but Cisco Secure Client does not support ESN.

Cisco Secure Client FIPS Requirements

- Suite B cryptography is available for TLS/DTLS and IKEv2/IPsec VPN connections.
- FIPS and/or Suite B support is required on the secure gateway. Cisco provides Suite B capability on the Secure Firewall ASA version 9.0 and later, and FIPS capability on the Secure Firewall ASA version 8.4.1 and later.
- ECDSA certificate requirements:
  - Must have a Digest strength equal or greater than the Curve strength. For example, an EC-384 key must use SHA2-384 or greater.
  - Support on Windows 7 or later, macOS 10.7 or later, Red Hat Enterprise Linux 6.x or 6.4 (64-bit) or later, and Ubuntu 12.4 and 12.10 (64-bit) or later. ECDSA smart cards are supported only on Windows 7 (and later).

Limitations of Cisco Secure Client FIPS

No EAP methods support SHA-2 except in TLS-based EAP when validating certificates signed using SHA-2.

Guidelines for Cisco Secure Client FIPS

- The Cisco Secure Client Statistics panel (under the Transport Information heading) shows the name of the cipher being used.
- Because AES-GCM is computationally intensive algorithms, you may experience a lower overall data rate when using these algorithms. Some processors contain special instructions specifically introduced to improve the performance of AES-GCM. Cisco Secure Client automatically detects whether the processor on which it is running supports these new instructions. If so, Cisco Secure Client uses the new instructions to significantly improve VPN data rates as compared to those processors that do not have the special

instructions. Contact your CPU manufacturer to determine which models of their CPUs support AES-GCM optimization.

- Combined-mode encryption algorithms, where both encryption and integrity verifications are performed in one operation, are supported only on SMP ASA gateways with hardware crypto acceleration (such as 5585 and 5515-X). AES-GCM is the combined-mode encryption algorithm that Cisco supports.



Note An IKEv2 policy can include either a normal- or a combined-mode encryption algorithm, but not both types. When a combined-mode algorithm is configured in the IKEv2 policy, all normal-mode algorithms are disabled, so the only valid integrity algorithm is NULL.

The IKEv2 IPsec proposals use a different model and can specify both normal- and combined-mode encryption algorithms in the same proposal. With this usage, you are required to configure integrity algorithms for both, which leaves a non-NULL integrity algorithm configured with AES-GCM encryption.

- When the Secure Firewall ASA is configured with a different server certificate for SSL and IPsec, use trusted certificates. A Posture Assessment or Downloader failure can occur if using Suite B (ECDSA) untrusted certificates having different IPsec and SSL certificates.

Avoiding Endpoint Problems from Cisco Secure Client FIPS Registry Changes

Enabling FIPS for the AnyConnect VPN changes Windows registry settings on the endpoint. Other components of the endpoint may detect that AnyConnect VPN has enabled FIPS. For example, the Microsoft Terminal Services client Remote Desktop Protocol (RDP) will not work, because RDP requires that servers use FIPS compliant cryptography.

To avoid these problems, you can temporarily disable FIPS encryption in the Windows Local System Cryptography settings by changing the parameter *Use FIPs compliant algorithms for encryption, hashing, and signing* to Disabled. Be aware that rebooting the endpoint device changes this setting back to enabled.

AnyConnect VPN sets the FIPSAlgorithmPolicy value to 1 in the Windows registry key HKLM\System\CurrentControlSet\ Control\Lsa. Note that disabling FIPS mode in the AnyConnect local policy file does not cause AnyConnect VPN to alter the FIPSAlgorithmPolicy value.

Configure FIPS for AnyConnect VPN

Enable FIPS for AnyConnect VPN (or SFP or ZTA)

These steps are the same for enabling FIPS for Secure Firewall Posture and Zero Trust Access.

Procedure

Step 1 Open or create a VPN Local Policy profile in the Cisco Secure Client Profile Editor - VPN Local Policy.

Step 2 Select **FIPS Mode**.

Step 3 Save the VPN Local Policy profile.

We recommend that you name the profile to indicate that FIPS is enabled.

Enable FIPS During Windows Installation

For Windows installations, you can apply a Cisco MST file to the standard MSI installation file to enable FIPS in the AnyConnect Local Policy. For information about where you can download this MST file, see the licensing information you received for FIPS. The installation generates an AnyConnect Local Policy file with FIPS enabled. Update the user's system after running this utility.

Note This MST only enables FIPS. It does not change other parameters. To change other local policy settings during Windows installation, see Enable Local Policy Parameters in an MST File.

Configure FIPS for the Network Access Manager

The Network Access Manager can be configured to connect to both FIPS and non-FIPS networks simultaneously, or to FIPS networks only.

Procedure

Step 1 Enable FIPS for the Network Access Manager, page 9-5.

Enabling FIPS allows the Network Access Manager to connect to both FIPS and non-FIPS networks.

Step 2 If desired, Enforce FIPS Mode for the Network Access Manager, page 9-6.

Enforcing FIPS mode restricts the Network Access Manager connections to FIPS networks only.

Enable FIPS for the Network Access Manager

Enable FIPs mode in the Cisco Secure Client Network Access Manager client profile. For Windows 10 and 11, you must enable FIPS on your operating system to be FIPS compliant, besides just enabling FIPS for the Network Access Manager.

Procedure

Step 1 Open or create a Network Access Manager profile in the Cisco Secure Client Profile Editor.

Step 2 Select the **Client Policy** configuration window.

Step 3 Under the **Administrative Status** section select **Enable** for **FIPS Mode**.

Step 4 Save the Network Access Manager profile as configuration.xml.

Enforce FIPS Mode for the Network Access Manager

Force enterprise employees to only connect to FIPS-compliant networks by restricting the allowed association and encryption modes, and the authentication methods in the Network Access Manager profile.

You must first Enable FIPS for the Network Access Manager to enforce FIPS mode.

Procedure

Step 1 Open your Network Access Manager profile in the Cisco Secure Client Profile Editor.

Step 2 Network Access Manager FIPS compliance requires FIPS-approved AES encryption modes including WPA2 Personal (WPA2-PSK) and WPA2 Enterprise (802.1X).

Step 3 The Network Access Manager FIPS support includes EAP methods EAP-TLS, EAP-TTLS, PEAP, EAP-FAST and LEAP.

Step 4 Save the Network Access Manager profile as configuration.xml.