



Post-Quantum Cryptography

- [Feature History for PQC, on page 1](#)
- [Post-Quantum Cryptography Overview, on page 2](#)
- [LMS-signed bootloader, on page 2](#)
- [PQC Dual-sign support, on page 2](#)
- [Verify software authentication and system integrity, on page 3](#)

Feature History for PQC

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature name and description	Supported platform
Cisco IOS XE 26.2.1	PQC dual-sign support: Dual signing enhances software authenticity and integrity by preparing systems for post-quantum cryptographic requirements while maintaining backward compatibility. This approach adds both a legacy RSA signature and a quantum-resistant ML-DSA-87 signature to IOS-XE software images. Supported platforms verify the stronger quantum-resistant signature, while older systems continue to rely on the existing RSA signature. This method ensures seamless operation in mixed environments and reduces disruption during the transition to next-generation security standards.	Cisco C9350 Series Smart Switches Cisco C9550 Series Smart Switches Cisco C9610 Series Smart Switches

Release	Feature name and description	Supported platform
Cisco IOS XE 26.2.1	LMS-signed bootloader: LMS-signed bootloader feature support has been introduced.	Cisco C9350 Series Smart Switches Cisco C9550 Series Smart Switches
Cisco IOS XE 26.1.1a	LMS-signed bootloader: The device supports secure boot process based on LMS PQC algorithm.	Cisco C9610 Series Smart Switches

Post-Quantum Cryptography Overview

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to be secure against attacks from quantum computers which can break many classical encryption methods. Current widely used encryption methods—such as Diffie-Hellman (DH), and Elliptic Curve Diffie-Hellman (ECDH)—are vulnerable to being broken as quantum computing technology advances.

Implementing quantum-safe encryption now is critical for the long-term confidentiality and integrity of sensitive communications, particularly for government, military, and financial sectors.

The Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) defines the approved quantum-resistant algorithms that Cisco products use to maintain system integrity and data protection.

Key algorithms used in CNSA 2.0:

- **ML-DSA (CRYSTALS-Dilithium)**: Used for digital signatures to authenticate firmware and software.
- **ML-KEM (CRYSTALS-Kyber)**: Used for secure key establishment.
- **LMS (Leighton-Micali Signature)**: Used for digitally signing firmware and software.

LMS-signed bootloader

The device supports secure boot process based on Leighton-Micali Signature (LMS) Post-Quantum Cryptography (PQC) algorithm which is approved by National Institute of Standards and Technology (NIST). When the device boots up, the microloader residing in secure boot FPGA loads the bootloader (ROMMON) after verifying its authenticity.



Note Use the **show module** command to view the hardware version.

PQC Dual-sign support

Dual-signing IOS-XE images is a software authenticity approach that

- adds both a legacy signature, such as RSA, and a quantum-resistant signature, such as ML-DSA-87, to supported IOS-XE software artifacts,

- helps organizations move toward post-quantum security requirements while keeping existing deployments operational, and
- allows verification behavior to align with platform capabilities.

The PQC dual-signing supports a transition period in which some platforms continue to use legacy signature verification, while supported platforms verify the quantum-resistant signature. Dual-signing applies to IOS-XE bundle images and individual packages.

This approach improves software authenticity and integrity verification while helping customers prepare for evolving cryptographic requirements.

Benefits of PQC dual-signing

Dual-signing provides these benefits:

- Helps organizations prepare for CNSA 2.0 transition requirements.
- Maintains backward compatibility for platforms that do not support quantum-resistant verification.
- Supports mixed deployment environments during migration.
- Preserves image authenticity and integrity verification.
- Reduces operational disruption during the move from legacy signing to post-quantum signing.

Verify software authentication and system integrity

Starting with Cisco IOS XE 26.2.1 release, the device is updated from legacy RSA-based security to a quantum-resistant configuration. The quantum-resistant ML-DSA-87 signature is now added to IOS-XE software images. You can verify if all components are PQC-compliant by using the **show software authenticity running** command.

Verify software authenticity

Ensure system integrity by verifying device software authenticity. The **show software authenticity running** command validates running software signatures against new PQC standards.

To verify the signatures of the running software, use the **show software authenticity running** command in privileged EXEC mode. This command displays information related to software authentication for the current ROM monitor (ROMMON), and Cisco IOS image used for booting.

signature

Device# **show software authenticity running**

PACKAGE cisco9k-guestshell.BLD_POLARIS_DEV_LATEST_20260804_003747.SSA.pkg

```
-----
Image type                : Special
  Signer Information
    Common Name            : CiscoSystems
    Organization Unit      : IOS-XE
    Organization Name      : CiscoSystems
    Certificate Serial Number : 6A7148DA
    Hash Algorithm         : SHA512
    Signature Algorithm     : MLDSA87
```

```

Key Version                : A

Verifier Information
  Verifier Name            : rp_base
  Verifier Version         : BLD_POLARIS_DEV_LATEST_20260804_003747

PACKAGE cisco9k-rpbase.BLD_POLARIS_DEV_LATEST_20260804_003747.SSA.pkg
-----
Image type                  : Special
  Signer Information
    Common Name             : CiscoSystems
    Organization Unit       : IOS-XE
    Organization Name       : CiscoSystems
    Certificate Serial Number : 6A7148DA
    Hash Algorithm          : SHA512
    Signature Algorithm      : MLDSA87
    Key Version             : A

  Verifier Information
    Verifier Name           : rp_base
    Verifier Version        : BLD_POLARIS_DEV_LATEST_20260804_003747

PACKAGE cisco9k-srdriver.BLD_POLARIS_DEV_LATEST_20260804_003747.SSA.pkg
-----
Image type                  : Special
  Signer Information
    Common Name             : CiscoSystems
    Organization Unit       : IOS-XE
    Organization Name       : CiscoSystems
    Certificate Serial Number : 6A7148DA
    Hash Algorithm          : SHA512
    Signature Algorithm      : MLDSA87
    Key Version             : A

  Verifier Information
    Verifier Name           : rp_base
    Verifier Version        : BLD_POLARIS_DEV_LATEST_20260804_003747

PACKAGE cisco9k-webui.BLD_POLARIS_DEV_LATEST_20260804_003747.SSA.pkg
-----
Image type                  : Special
  Signer Information
    Common Name             : CiscoSystems
    Organization Unit       : IOS-XE
    Organization Name       : CiscoSystems
    Certificate Serial Number : 6A7148DA
    Hash Algorithm          : SHA512
    Signature Algorithm      : MLDSA87
    Key Version             : A

  Verifier Information
    Verifier Name           : rp_base
    Verifier Version        : BLD_POLARIS_DEV_LATEST_20260804_003747

PACKAGE cisco9k-lni.BLD_POLARIS_DEV_LATEST_20260804_003747.SSA.pkg
-----
Image type                  : Special
  Signer Information
    Common Name             : CiscoSystems
    Organization Unit       : IOS-XE
    Organization Name       : CiscoSystems
    Certificate Serial Number : 6A7148DA
    Hash Algorithm          : SHA512
    Signature Algorithm      : MLDSA87

```

```

Key Version                : A

Verifier Information
  Verifier Name            : rp_base
  Verifier Version         : BLD_POLARIS_DEV_LATEST_20260804_003747

PACKAGE cisco9k-cc_srdriver.BLD_POLARIS_DEV_LATEST_20260804_003747.SSA.pkg
-----
Image type                  : Special
  Signer Information
    Common Name             : CiscoSystems
    Organization Unit       : IOS-XE
    Organization Name       : CiscoSystems
    Certificate Serial Number : 6A7148DA
    Hash Algorithm          : SHA512
    Signature Algorithm      : MLDSA87
    Key Version             : A

  Verifier Information
    Verifier Name           : rp_base
    Verifier Version        : BLD_POLARIS_DEV_LATEST_20260804_003747

SYSTEM IMAGE
-----
Image type                  : Special
  Signer Information
    Common Name             : CiscoSystems
    Organization Unit       : IOS-XE
    Organization Name       : CiscoSystems
    Certificate Serial Number : 50000000432b4f642f4a413451594e677250
    Hash Algorithm          : SHA512
    Signature Algorithm      : MLDSA
    MLDSA Variant           : 87

  Verifier Information
    Verifier Name           : ROMMON
    Verifier Version        : Version 26.2.1r

ROMMON
-----
Image type                  : Production
  Signer Information
    Common Name             : CiscoSystems
    Organization Unit       : IOS-XE
    Organization Name       : CiscoSystems
    Certificate Serial Number : 8f77cd8f4460505a581a24f09bee0991
    Hash Algorithm          : SHA512
    Signature Algorithm      : LMS
    LMS Mode                 : LMS_SHA256_M24_H20
    LMOTS Mode               : LMOTS_SHA256_N24_W4
    LMS Hash Algorithm       : SHA-256/192
    Winternitz Parameter (w) : 4
    Height (h)               : 20

  Verifier Information
    Verifier Name           : Microloader
    Verifier Version        : MA2001R07.1020251204.28932b69

Microloader
-----
Image type                  : Release
  Signer Information
    Common Name             : CiscoSystems

```

```
Organization Name      : CiscoSystems
Certificate Serial Number :
bcd97103ff5874f0afdele383a41f711f4bb0c245eb5ac527fc4126068f191f0
Hash Algorithm         : SHA512
Signature Algorithm    : HMAC

Verifier Information
  Verifier Name        : Hardware Anchor
  Verifier Version     : F01378R25.00a833cba2026-04-03
```

Related commands:

- **show software authenticity file:** Displays the software authenticity related information for the loaded image file.
- **show software authenticity keys:** Displays the software public keys that are in the storage with the key types.