

ML-DSA signature for software image authenticity verification

- ML-DSA signature for software image authenticity verification, on page 1
- Verify the software authenticity public keys, on page 1
- Verify the authenticity information for the running software, on page 2

ML-DSA signature for software image authenticity verification

Starting from Cisco IOS XE Release 26.2.1, ML-DSA-87 digital signature verification for Cisco IOS XE software images is enabled on the routers. The ML-DSA-87 software authenticity verification proceeds automatically on the router during bootup.

Verify the software authenticity public keys

This task verifies that the router contains the public keys used to authenticate Cisco IOS XE software images. The output identifies each key's type, algorithm, version, and associated product.

Procedure

Use the **show software authenticity keys** command to verify the software-authenticity public keys.

Example:

```
Router# show software authenticity keys

Public Key #1 Information
-------------------------
Key Type              : Production
Public Key Algorithm : RSA
Modulus (256 bytes)   :
...
Exponent (3 bytes)    : 10001
Product Name          : IOSXE

Public Key #2 Information
-------------------------
```

```
Key Type             : Production
Public Key Algorithm : MLDSA87
Public Key Value (2592 bytes):
...
Product Name         : IOSXE_MLDSA_OS

Public Key #3 Information
-------------------------
Key Type             : Production
Public Key Algorithm : RSA
Modulus (512 bytes)  :
...
Exponent (3 bytes)   : 10001
Product Name         : IOSXE_RSA4K

Public Key #4 Information
-------------------------
Key Type             : Production
Public Key Algorithm : RSA
Modulus (256 bytes)  :
...
Exponent (3 bytes)   : 10001
Product Name         : XE_Containers

Public Key #5 Information
-------------------------
Key Type             : Production
Public Key Algorithm : MLDSA87
Public Key Value (2592 bytes)  :
...
Product Name         : XE_Containers_MLDSA

Public Key #6 Information
-------------------------
Key Type             : Production
Public Key Algorithm : RSA
Modulus (512 bytes)  :
...
Exponent (3 bytes)   : 10001
Product Name         : XE_Containers_RSA4K
```

Verify the authenticity information for the running software

Procedure

Use the **show software authenticity running** command to verify the authenticity information for the running software.

Example:

```
Router# show software authenticity running
PACKAGE ir1000-mono-universalk9.26.02.01.SPA.pkg
----------------------------------------------------------------------
Image type                   : Production
    Signer Information
        Common Name          : CiscoSystems
        Organization Unit    : IOS-XE
```

```
        Organization Name     : CiscoSystems
    Certificate Serial Number : 6AB2E312
    Hash Algorithm            : SHA512
    Signature Algorithm       : MLDSA87
    Key Version               : A

    Verifier Information
        Verifier Name         : mono
        Verifier Version      : 26.02.01

SYSTEM IMAGE
------------
Image type                    : Production
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 6ab2e312
    Hash Algorithm            : SHA512
    Signature Algorithm       : MLDSA
    Key Version               : A
    MLDSA Variant             : 87

    Verifier Information
        Verifier Name         : ROMMON
        Verifier Version      : Version 26.2.1.2(REL)

ROMMON
------
Image type                    : Production
    Signer Information
        Common Name           : IRG2_MLDSA_BL
        Organization Unit     : RELEASE
        Organization Name     : Cisco
    Certificate Serial Number : 5100000064714e78716a4166466572637133
    Hash Algorithm            : SHA512
    Signature Algorithm       : MLDSA
    MLDSA Variant             : 87

    Verifier Information
        Verifier Name         : Microloader
        Verifier Version      : 403

Image type                    : Production
    Signer Information
        Common Name           : IRG2_RSA4K
        Organization Unit     : RELEASE
        Organization Name     : Cisco
    Certificate Serial Number : 06263393962799786936
    Hash Algorithm            : SHA512
    Signature Algorithm       : RSA
    Modulus Size              : 4096-bit

    Verifier Information
        Verifier Name         : Microloader
        Verifier Version      : 403

Microloader
-----------
Image type                    : Release
    Signer Information
        Common Name           : CiscoSystems
        Organization Name     : CiscoSystems
    Certificate Serial Number : 01
```

```
    Hash Algorithm            : SHA512
    Signature Algorithm       : MLDSA
    MLDSA Variant             : 87

    Verifier Information
        Verifier Name         : Hardware Anchor
        Verifier Version      : 4

Image type                    : Release
    Signer Information
        Common Name           : CiscoSystems
        Organization Name     : CiscoSystems
    Certificate Serial Number : 01
    Hash Algorithm            : SHA512
    Signature Algorithm       : RSA
    Modulus Size              : 4096-bit

    Verifier Information
        Verifier Name         : Hardware Anchor
        Verifier Version      : 4
```