Cisco SD-Routing Commands

- clear sd-routing alarms , on page 2
- request platform software sd-routing activate chassis-number, on page 3
- request platform software sd-routing certificate install, on page 4
- request platform software sd-routing csr upload, on page 5
- request platform software sd-routing root-cert-chain install, on page 6
- request platform software sd-routing root-cert-chain uninstall, on page 8
- show sd-routing alarms detail, on page 9
- show sd-routing alarms summary, on page 10
- show sd-routing certificate installed, on page 11
- show sd-routing certificate reverse proxy, on page 13
- show sd-routing certificate root-ca-cert, on page 14
- show sd-routing certificate root-ca-crl, on page 16
- show sd-routing certificate serial, on page 17
- show sd-routing certificate signing-request, on page 18
- show sd-routing certificate validity, on page 20
- show sd-routing control connections detail, on page 21
- show sd-routing control connections history, on page 23
- show sd-routing control connections summary, on page 25
- show sd-routing control local-properties summary, on page 26
- show sd-routing control local-properties vbond, on page 28
- show sd-routing control local-properties wan detail, on page 29
- show sd-routing control local-properties wan ipv4, on page 30
- show sd-routing control local-properties wan ipv6, on page 31
- show sd-routing system status, on page 32

clear sd-routing alarms

To clear alarm details such as the timestamp, event name, and severity, use the **clear sd-routing alarms** command in privileged EXEC configuration mode.

clear sd-routing alarms

This command has no arguments or keywords

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.15.1a	This command was introduced.

Usage Guidelines

To clear the alarms, use the **clear sd-routing alarms** command in privilege EXEC Mode.

Example

The following is the example output for the **clear sd-routing alarms** command.

```
me1#show sd-routing alarms summary
time-stamp                      event-name                                  severity-level
-------------------------------------------------------------------------------------------
2024-03-29:17:43:36.609193      security-root-cert-chain-installed          minor
2024-03-29:17:37:24.560476      control-connection-state-change             major
2024-03-29:17:37:24.139871      non-yang-cli-file-generated                 minor
2024-03-29:17:37:09.967815      control-connection-state-change             major
2024-03-29:17:37:08.793288      system-reboot-complete                      major
2024-03-29:17:37:06.604089      control-connection-state-change             major
2024-03-29:17:37:03.287560      control-connection-tloc-ip-change           minor
2024-03-29:17:37:03.282644      vmanage-connection-preference-changed       minor


me1#clear sd-routing alarms
me1#show sd-routing alarms summary
me1#
```

request platform software sd-routing activate chassis-number

To activate the chassis number on a device operating in the SD-routing mode on request, use the **request platform software sd-routing activate chassis-number** command in privileged EXEC mode.

request platform software sd-routing activate chassis-number *chassis_number* **token** *token_id*

Syntax Description

chassis_number	Activates the chassis number on the device. Specify the chassis number for activation on request.
token*token_id*	Specify the token of the chassis number for activation.

Command Default

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router .

Example

The following example shows how to activate the chassis number on the device using the **request platform software sd-routing activate chassis-number** command:

```
Device#request platform software sd-routing activate chassis-number 123 token cisco
Device#
```

request platform software sd-routing certificate install

To install a client certificate on a device where you have enabled the SD-Routing feature, enter the **request platform software sd-routing certificate install** command in privileged EXEC mode.

request platform software sd-routing certificate install *path-to-certificate-file*

Syntax Description

path-to-certificate-file	Specify the absolute path fo the folder to upload the generated file. You can specify any name for the folder that is created within the *bootflash:ctrl_mng/* directory.

Command Default

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, and Cisco 1000 Series Integrated Services Routers.

Usage Guidelines

To install the client certificates for manually onboarding the SD-Routing software device, generate a Certificate Signed Request (CSR) for the device using the **request platform software sd-routing certificate install** command in privileged EXEC mode.

The following example shows how to install a client certificate located in a VPN.

```
Device# request platform software sd-routing certificate install bootflash:ctrl_mng/test
```

request platform software sd-routing csr upload

To generate a Certificate Signed Request (CSR) for the device and upload to the specificed folder, use the **request platform software sd-routing csr upload** command in privileged EXEC mode.

request platform software sd-routing csr upload *path-to-certificate-file*

Syntax Description

path-to-certificate-file	Specify the absolute path fo the folder to upload the generated file. You can specify any name for the folder that is created within the *bootflash:ctrl_mng/* directory.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, and Cisco 1000 Series Integrated Services Routers.

Usage Guidelines

To install the client certificates for manually onboarding the SD-Routing software device, generate a Certificate Signed Request (CSR) for the device using the **request platform software sd-routing csr upload** command in privileged EXEC mode.

Note You can use this command only when you onboard the software devices manually.

The following example shows how to generate a client certificate and upload to the specified folder.

```
Device# request platform software sd-routing csr upload bootflash:ctrl_mng/test
```

request platform software sd-routing root-cert-chain install

To install an enterprise root certificate on a device where you have enabled the SD-Routing feature, enter the **request platform software sd-routing root-cert-chain install** command in privileged EXEC mode.

request platform software sd-routing root-cert-chain install *filepath-filename* [**vpn** *rcci_leaf*]

Syntax Description

filepath-filename	Install the file containing the root certificate. Specify the absolute path to the file, including the filename. The root certificate chain can be stored in one of the following locations: • **bootflash:** • **crashinfo:** • **flash:**
vpn *rcci_leaf*	Specifies the VPN in which the certificate file is located.

Command Default

By default, the device is equipped with Public Key Infrastructure (PKI) and Symantec-signed root certificates.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, and Cisco 1000 Series Integrated Services Routers.

Usage Guidelines

If the overlay is Cisco PKI or Symantec, you do not have to install a root certificate

If it is an enterprise overlay, install enterprise root certificates by entering the **request platform software sd-routing root-cert-chain install** command in privileged EXEC mode.

Ensure that you have saved the enterprise root certificate that you want to install, in one of the supported locations.

After you have installed a root certificate, use the **show sd-routing control local-properties summary** to verify certificate installation. If installed correctly, the `root-ca-chain-status` field in the output displays value `Installed`.

The following example shows how to install an enterprise root certificate located in a VPN.

```
Device# request platform software sd-routing root-cert-chain install
bootflash:ent-root-cert-file vpn 1


Device#show sd-routing control local-properties summary
 personality                      vedge
sp-organization-name             vIPtela Inc Regression
organization-name                vIPtela Inc Regression
root-ca-chain-status             Installed
root-ca-crl-status               Not-Installed

certificate-status               Installed
```

```
certificate-validity              Valid
certificate-not-valid-before      Nov 27 08:53:44 2023 GMT
certificate-not-valid-after       Nov 26 08:53:44 2024 GMT

enterprise-cert-status            Not Applicable
enterprise-cert-validity          Not Applicable
enterprise-cert-not-valid-before  Not Applicable
enterprise-cert-not-valid-after   Not Applicable

dns-name                          vbond
site-id                           100
protocol                          dtls
tls-port                          0
system-ip                         172.16.255.21
chassis-num/unique-id             C8K-9bdc48d2-4987-4d49-8f28-e62e72900628
serial-num                        1234570D
subject-serial-num                N/A
enterprise-serial-num             Not Applicable
token                             Invalid
keygen-interval                   0:02:00:00
retry-interval                    0:00:00:18
no-activity-exp-interval          0:00:00:20
dns-cache-ttl                     0:00:02:00
port-hopped                       FALSE
time-since-last-port-hop          0:00:00:00
embargo-check                     success
number-vbond-peers                2
number-active-wan-interfaces      1
```

request platform software sd-routing root-cert-chain uninstall

To uninstall an enterprise root certificate on a device where you have enabled the SD-Routing feature, enter the **request platform software sd-routing root-cert-chain uninstall** command in privileged EXEC mode.

request platform software sd-routing root-cert-chain uninstall

Command Default

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router .

Usage Guidelines

To uninstall an enterprise root certificate on a device, use the **request platform software sd-routing root-cert-chain uninstall** command in privileged EXEC mode.

Example

The following example shows how to uninstall an enterprise root certificate on a device using the **request platform software sd-routing root-cert-chain uninstall** command:

```
Device#request platform software sd-routing root-cert-chain uninstall
Successfully uninstalled the root certificate chain
```

show sd-routing alarms detail

To view detailed information about the SD-Routing alarm, use the **show sd-routing alarms detail** command in privileged EXEC configuration mode.

show sd-routing alarms detail

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.15.1a	This command was introduced.

Usage Guidelines

To view the alarm detail, use the **show sd-routing alarms detail** command in privilege EXEC Mode.

Example

The following is the example output for the **show sd-routing alarms detail** command.

```
me1#show sd-routing alarms detail
2023-08-08:21:40:27.888885
event-name     vmanage-connection-preference-changed
severity-level minor
host-name      me1
kv-pair      [ system-ip=10.0.1.2 color=default vmanage-connection-preference=5 ]
-----------------------------------------------------------------------------

alarms 2023-08-08:21:40:30.145551
event-name
control-connection-tloc-ip-change
severity-level minor
host-name      me1
kv-pair   [ system-ip=10.0.1.2 personality=vedge old-public-ip=0.0.0.0 old-public-port=0
new-public-ip=10.1.1.2 new-public-port=0 ]
-----------------------------------------------------------------------------
```

show sd-routing alarms summary

To view alarm details such as the timestamp, event name, and severity in a tabular format, use the **show sd-routing alarms summary** command in privileged EXEC configuration mode.

show sd-routing alarms summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.15.1a	This command was introduced.

Usage Guidelines

To view the alarms summary, use the **show sd-routing alarms summary** command in privilege EXEC Mode.

Example

The following is the example output for **show sd-routing alarms summary** command.

```
me1#show sd-routing alarms summary
time-stamp                    event-name                                  severity-level

----------------------------------------------------------------------
2023-08-08:21:40:27.888885      vmanage-connection-preference-changed      minor
2023-08-08:21:40:30.145551      control-connection-tloc-ip-change          minor
2023-08-08:21:40:34.262999      system-reboot-complete                     major
```

show sd-routing certificate installed

To display the cretificate installed on a device operating in the SD-Routing mode, use the **show sd-routing ertificate installed** command in privileged EXEC mode.

show sd-routing certificate installed

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router .

Usage Guidelines

You can use this command when you are onboarding a device. The output helps you verify the certificate installed on the device .

The following is sample output of the **show sd-routing certificate installed** command:

```
Device#show sd-routing certificate installed
Installed device certificates
-----------------------------
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 305420038 (0x12345706)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Jose, OU = vIPtela System TB, O = vIPtela
 Inc, emailAddress = santosh@viptela.com
        Validity
            Not Before: Nov 10 05:28:10 2023 GMT
            Not After : Nov  9 05:28:10 2024 GMT
       Subject: L = San Jose, C = US, ST = California, O = Cisco Systems, OU = vIPtela Inc
 Regression, CN = vedge-C8K-0a4fecf0-79af-4495-8cc6-368749f0ebad-1.viptela.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d9:96:04:94:1d:c0:5e:60:25:12:bd:67:ca:ae:
                    db:c7:3a:62:34:85:05:09:cc:14:f2:40:5a:5c:42:
                    0e:b7:b6:02:47:e5:ca:ad:1a:55:8b:40:cf:41:49:
                    eb:5f:f3:7f:8d:02:47:81:92:93:2a:9e:ea:d3:9c:
                    98:e7:d5:d5:f9:19:30:12:bb:90:5c:bb:eb:2b:4d:
                    ca:c2:2a:26:53:51:2d:04:df:45:29:65:14:7b:8f:
                    b3:d7:ba:60:94:58:e7:96:32:6f:1d:46:0c:fc:7f:
                    c6:59:2e:ad:46:83:30:a8:1a:b0:79:35:f2:e8:19:
                    60:c2:5d:79:bf:b1:92:d2:68:da:0e:12:c2:e1:65:
                    1b:d4:a1:5b:3c:cc:9f:aa:1f:cf:2b:61:9b:6d:c7:
                    55:c7:d4:66:f4:ca:20:2e:9a:50:6d:1c:b0:12:61:
                    7d:07:09:eb:06:59:e8:c4:8b:d2:4f:3e:d2:99:fd:
                    82:86:94:3b:62:c7:26:9c:c0:65:d8:e1:b9:f8:dc:
                    71:b1:bd:64:cb:60:5c:92:27:67:c8:19:c5:20:4b:
                    22:5e:9b:26:b7:94:65:a7:dc:6d:cb:cb:e8:82:89:
                    58:2c:d4:1b:59:45:fb:55:f1:69:93:39:21:2c:f8:
                    f9:c6:c4:f7:6e:5c:ba:b3:b9:f5:6a:ef:e4:32:07:
```

```
                a1:a3
            Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         47:b7:3e:2d:ec:eb:c5:aa:88:b8:13:08:d8:8b:71:1b:cc:30:
         76:74:63:db:1f:15:2f:b7:1a:cd:22:c6:46:8d:84:53:7a:22:
         4c:d4:10:9a:e1:de:96:63:ee:fa:58:36:15:dd:ec:96:27:61:
         a5:93:07:d8:a2:97:a0:54:07:48:01:bd:c6:22:e6:57:df:23:
         54:ee:73:1e:4a:dd:51:1f:30:39:74:87:b0:7b:d5:96:18:ec:
         97:5d:cc:01:11:2c:76:8f:04:54:a7:ae:c2:89:31:20:aa:53:
         ab:11:24:62:4d:e0:27:d2:4a:f0:3f:c5:5d:73:54:1f:bd:86:
         84:d9:d3:17:c9:7d:00:7e:08:f8:7b:b9:ff:69:29:b2:58:5f:
         80:ed:ea:a3:b7:8d:33:fc:7b:82:a1:2f:85:01:40:f3:07:f8:
         59:da:af:c4:ec:7a:5e:2b:e0:61:9d:9c:b9:2a:95:72:26:b9:
         b1:b8:af:c5:76:5a:c2:9b:45:2a:5c:a0:b9:d6:bf:29:1a:7e:
         fe:1d:44:45:f0:ba:c5:be:e3:aa:4b:39:50:4e:38:40:86:ba:
         3d:26:21:86:46:48:28:f1:34:7a:bb:9c:7a:49:5d:7a:43:59:
         b7:74:2a:77:a7:59:40:89:ff:56:55:02:a9:db:b0:78:8b:24:
         e5:17:ab:48
```

show sd-routing certificate reverse proxy

To display the signed certificate installed on a SD-Routing device for Authentication with Reverse Proxy, use the **show sd-routing certificate reverse-proxy** command in privileged EXEC mode.

show sd-routing certificate reverse-proxy

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, and Cisco 1000 Series Integrated Services Routers.

Usage Guidelines

You can use this command when you are onboarding a device. The output helps you verify the he signed certificate installed on a SD-Routing device for Authentication with Reverse Proxy.

The following is sample output of the **show sd-routing certificate reverse-proxy** command:

show sd-routing certificate root-ca-cert

To display the root CS cretificate installed on a device operating in the SD-Routing mode, use the **show sd-routing ertificate root-ca-cert** command in privileged EXEC mode.

show sd-routing certificate root-ca-cert

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Routers .

Usage Guidelines

You can use this command when you are onboarding a device. The output helps you verify the root CA certificated installed on the device.

The following is sample output of the **show sd-routing certificate root-ca-cert** command:

```
Device#show sd-routing certificate root-ca-cert
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            92:e4:56:d8:7f:2f:6d:03
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C = US, ST = California, L = San Jose, OU = vIPtela System TB, O = vIPtela
 Inc, emailAddress = santosh@viptela.com
        Validity
            Not Before: Feb  7 21:54:23 2014 GMT
            Not After : Feb  5 21:54:23 2024 GMT
       Subject: C = US, ST = California, L = San Jose, OU = vIPtela System TB, O = vIPtela
 Inc, emailAddress = santosh@viptela.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:bd:ae:ad:62:cd:df:68:cd:75:66:58:d2:d7:0d:
                    5e:3e:34:30:55:56:52:c0:f6:fd:da:58:76:3e:a7:
                    31:17:6c:e2:35:6a:46:c0:b2:c5:b0:f4:58:a4:b4:
                    01:ed:13:ee:8e:0c:db:8a:8e:04:12:69:a9:f5:04:
                    eb:01:df:d9:af:41:93:f5:3c:ae:dc:af:94:32:11:
                    b6:3a:db:58:3a:42:5a:8a:c6:bd:69:58:2c:cb:89:
                    b0:17:71:b0:6c:cd:b4:7d:8d:70:73:a0:1b:71:ac:
                    a9:43:7b:38:29:09:d8:02:7b:40:a8:5a:f1:1b:37:
                    82:78:52:f7:ea:68:0f:b9:5d:65:c8:f7:80:f0:07:
                    9a:ec:64:0d:14:70:1e:38:36:cc:bf:63:b6:27:6f:
                    3d:d8:f5:3a:03:e9:58:3a:91:91:50:c6:48:a6:14:
                    bb:09:77:e3:84:88:40:95:ee:24:b7:da:2c:46:4a:
                    b4:c1:ec:bd:61:8a:28:30:8a:40:99:21:e5:ed:a7:
                    99:d0:3f:c1:2b:53:72:d6:12:5c:a4:0d:a7:16:a2:
                    b9:db:bf:86:49:9d:c2:d4:49:b5:30:b5:c8:95:a4:
                    ca:0c:a7:44:31:7c:72:da:68:22:bd:61:7d:ec:9e:
                    6c:3e:06:7a:a3:db:ba:f1:5b:1c:5c:9b:e5:8e:c8:
                    91:05
```

```
                Exponent: 65537 (0x10001)
            X509v3 extensions:
                X509v3 Basic Constraints:
                    CA:TRUE
                X509v3 Subject Key Identifier:
                    87:0A:05:91:FB:B0:D1:29:50:25:60:33:CD:06:32:5F:C4:45:A7:67
                X509v3 Authority Key Identifier:
                    keyid:87:0A:05:91:FB:B0:D1:29:50:25:60:33:CD:06:32:5F:C4:45:A7:67
                    DirName:/C=US/ST=California/L=San Jose/OU=vIPtela System TB/O=vIPtela
Inc/emailAddress=santosh@viptela.com
                    serial:92:E4:56:D8:7F:2F:6D:03

    Signature Algorithm: sha1WithRSAEncryption
         6a:d3:45:97:02:e5:1d:20:9e:3a:8a:31:eb:73:01:55:18:dc:
         b2:d9:95:07:1f:2d:33:b0:b0:4e:a1:a8:f5:df:4e:5c:aa:4b:
         f5:ef:82:3a:c3:57:b3:ec:4d:26:92:bf:fc:66:7a:40:55:44:
         39:68:40:36:6d:9a:1b:9c:67:c1:df:8f:1b:6d:e9:00:d4:d0:
         b8:69:67:28:94:6f:a6:89:04:90:56:48:fc:dc:d3:c8:28:f5:
         3a:da:0d:41:3d:5e:d7:44:69:5d:ca:9b:fe:60:dd:40:c8:07:
         a8:a1:3e:d0:fb:4b:91:96:23:70:b8:70:ae:16:dd:0b:38:5e:
         38:d7:b0:d8:e8:83:e5:3a:4e:79:2a:51:33:77:ab:81:1a:f4:
         74:2b:5e:c6:5c:9d:59:61:21:1d:78:a6:a5:0e:c5:44:5a:37:
         f1:a8:e4:37:04:c6:81:64:82:04:f9:25:3d:d3:88:b8:59:cf:
         38:83:48:04:f5:5d:84:a5:03:cb:e5:ed:59:1e:b1:5d:9e:ad:
         2f:9e:06:80:7e:8b:de:24:37:f7:37:f4:34:f3:af:75:81:be:
         a9:e3:ac:45:c0:18:a7:59:65:13:73:83:ce:60:55:c4:75:c6:
         f7:ce:37:7b:6b:45:26:00:e0:35:03:d2:06:9c:53:f0:09:f0:
         6c:eb:52:31
```

show sd-routing certificate root-ca-crl

To display the root certificate revocation list on a device operating in the SD-Routing mode, use the **show sd-routing ertificate root-ca-crl** command in privileged EXEC mode.

show sd-routing certificate root-ca-crl

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, and Cisco 1000 Series Integrated Services Routers.

Usage Guidelines

You can use this command when you are onboarding a device. The output helps you verify the list of root certificated revocated on the device .

The following is sample output of the **show sd-routing certificate root-ca-crl** command:

show sd-routing certificate serial

To display the chasis and serial numbers of the certificate installed on a SD-Routing device for Authentication with Reverse Proxy, use the **show sd-routing certificate serial** command in privileged EXEC mode.

show sd-routing certificate serial

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router .

Usage Guidelines

You can use this command when you are onboarding a device. The output helps you verify the chasis and serial numbers of the certificate installed on a SD-Routing device for Authentication with Reverse Proxy.

The following is sample output of the **show sd-routing certificate serial** command:

```
Device# show sd-routing certificate serial
Chassis number: C8K-9bdc48d2-4987-4d49-8f28-e62e72900628 serial number: 1234570D Subject
S/N: N/A
```

show sd-routing certificate signing-request

To display information about certificate signing request (CSR) installed on devices in the SD-Routing mode, enter the **show sd-routing certificate signing-request** command in privileged EXEC mode.

show sd-routing certificate signing-request [**decoded**]

Syntax Description

decoded	Display decoded certificate signing-request.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router .

Usage Guidelines

You can use this command when you are onboarding a device. The output helps you verify the certificate signing request installed on the device .

The following is sample output of the **show sd-routing certificate signing-request** command:

```
Device# show sd-routing certificate signing-request decoded
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = US, ST = California, L = San Jose, OU = vIPtela Inc Regression, O =
Cisco Systems, CN = vedge-C8K-9bdc48d2-4987-4d49-8f28-e62e72900628-1.viptela.com, emailAddress
 = support@viptela.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c2:40:46:38:52:e8:20:5d:16:a4:86:6c:a0:48:
                    23:0b:2c:6d:4b:81:92:0a:fa:b8:e1:57:3e:7d:3e:
                    f2:d1:30:49:3c:09:af:ad:3e:34:fe:b8:3b:42:16:
                    22:65:f5:3b:6b:ed:b8:96:48:2e:68:47:e4:19:fb:
                    49:16:f3:b7:fe:e0:b3:06:7a:0c:bb:3a:95:7c:65:
                    10:10:12:1e:31:e8:5a:02:9c:04:e0:dc:f9:be:fe:
                    12:b6:3f:c7:96:0a:49:f0:a4:6c:9c:2c:37:6f:6d:
                    f2:cd:d7:27:be:4e:96:34:ed:78:65:4d:4d:8d:e5:
                    ee:77:de:7b:70:d9:91:4d:dd:2d:fc:32:1b:c3:3a:
                    b8:61:ba:70:77:1c:f2:b0:32:0d:fd:25:04:4f:5e:
                    f1:03:73:14:24:f2:46:40:f8:38:7c:f8:4c:98:bf:
                    66:03:fa:0e:d4:7e:c9:d9:6c:a7:d7:df:c8:a1:f3:
                    82:84:37:26:db:e7:9e:cf:68:0a:32:00:c5:1d:d6:
                    de:2e:b4:ce:82:83:51:39:b1:3a:60:5f:0a:53:da:
                    d4:f7:e7:c0:9d:ea:e4:af:db:85:63:79:29:ee:9f:
                    09:2f:c3:6d:87:be:22:83:4e:f7:20:7e:02:96:ef:
                    46:ea:df:28:a5:6e:15:d9:3d:33:5c:39:23:9a:83:
                    fc:d7
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
```

```
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Subject Key Identifier:
            19:18:4B:17:4F:B0:53:A1:C3:2B:73:ED:2C:06:DB:12:80:12:E2:C9
Signature Algorithm: sha256WithRSAEncryption
     5d:f4:08:81:70:74:40:a3:ff:ea:07:6c:61:be:c3:40:53:20:
     c4:3f:ef:d6:aa:e1:db:0b:b5:e9:94:9d:16:2e:c0:ef:d6:82:
     af:91:93:6a:4f:c4:fa:91:3a:5b:62:ca:d7:c9:65:76:c3:5c:
     1c:50:22:73:4f:f9:c0:c8:fe:d0:63:1c:8f:48:f1:dc:77:46:
     8c:c2:fc:24:8e:e7:26:2e:4d:59:f8:fa:3b:0f:d9:c2:18:db:
     23:0e:51:f6:8e:b8:54:e9:5b:17:83:ce:40:d4:2d:30:fd:88:
     cf:7e:ed:a3:90:2c:77:c0:fa:41:6b:d4:ef:c9:2c:93:a9:51:
     57:87:34:5c:fc:4d:83:6a:fc:dc:4f:3a:27:0c:74:f1:0c:93:
     1a:0e:de:ad:13:cc:bb:b1:78:05:5a:7e:71:a7:69:58:08:24:
     fd:5a:b2:d0:9a:ba:a9:03:77:a7:ac:aa:b3:66:81:26:ff:c4:
     34:bc:a0:b9:18:1a:18:9b:b3:ab:d8:43:8c:69:74:d5:81:d5:
     3a:e2:66:0d:3a:17:ad:d3:02:2c:1d:62:04:ec:e4:c1:f0:ad:
     4f:64:0d:65:ea:07:95:dd:dd:d9:26:74:59:65:af:b1:32:de:
     91:b3:26:28:87:05:39:11:48:62:af:c2:5d:4c:da:dd:b4:41:
     2a:45:b3:3a
```

show sd-routing certificate validity

To display information about the validity of the certificate in the SD-Routing mode, enter the **show sd-routing certificate validity** command in privileged EXEC mode.

show sd-routing certificate validity

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router .

Usage Guidelines

You can use this command when you are onboarding a device. The output helps you verify the validity of the certificate installed on the device .

The following is sample output of the **show sd-routing certificate validity** command:

```
Device# show sd-routing certificate validity
The certificate is valid from  Nov 27 08:53:44 2023 GMT  (Current date is Tue Nov 28 05:33:51
 GMT 2023) & valid until  Nov 26 08:53:44 2024 GMT
```

show sd-routing control connections detail

To display detailed information about control-plane connections on a device operating in the SD-Routing mode, use the show **sd-routing control connections** command in privileged EXEC mode.

show sd-routing control connections detail

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, and Cisco 1000 Series Integrated Services Routers.

Usage Guidelines

You can use this command when you are onboarding a device. The output helps you verify control connections from the device to Cisco vManage, Cisco vBond, <any other components? > .

The following is sample output of the **show sd-routing control connections detail** command:

```
Device# show sd-routing control connections detail
------------------------------------------------------------------------------
 SYSTEM-IP- 172.16.255.22   PEER-PERSONALITY- vmanage
------------------------------------------------------------------------------
site-id             200
protocol            dtls
protocol-version    DTLSv1.2
cipher-name         ECDHE-RSA-AES256-GCM-SHA384
local-interface     TenGigabitEthernet0/0/2
private-ip          10.0.12.22
private-port        12546
public-ip           10.0.12.22
public-port         12546
org-name            vIPtela Inc Regression
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:01:58:31
hello interval      1000
hello tolerance     12000

  Tx Statistics-
  --------------
    hello                   7116
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      1
    challenge-ack           0
    teardown                0
    teardown-all            0
    vmanage-to-peer         0
    register-to-vmanage     1

  Rx Statistics-
  --------------
    hello                   7116
    connects                0
```

```
registers               0
register-replies        0
challenge               1
challenge-response      0
challenge-ack           1
teardown                0
vmanage-to-peer         1
register-to-vmanage     0
```

show sd-routing control connections history

To display information about control-plane connection attempts initiated by a device operating in the SD-Routing mode, enter the **show sd-routing control connections history** command in privileged EXEC mode.

show sd-routing control connections history [**detail**]

Syntax Description

detail	(Optional) Displays information about each control-plane connection attempt.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, and Cisco 1000 Series Integrated Services Routers.

Usage Guidelines

The following is sample output of the **show sd-routing control connections history** command:

```
Device# show sd-routing control connections history
Legend for Errors
ACSRREJ     - Challenge rejected by peer.                NOVMCFG     - No cfg in vmanage
for device.
BDSGVERFL   - Board ID Signature Verify Failure.         NOZTPEN     - No/Bad chassis-number
 entry in ZTP.
BIDNTPR     - Board ID not Initialized.                  NTPRVMINT   - Not preferred
interface to vManage.
BIDNTVRFD   - Peer Board ID Cert not verified.           OPERDOWN    - Interface went oper
 down.
BIDSIG      - Board ID signing failure.                  ORPTMO      - Server's peer timed
 out.
CERTEXPRD   - Certificate Expired                        PSEV6DISC   - Pseudo v6 interface
 disconnect.
CRTREJSER   - Challenge response rejected by peer.       RDSIGFBD    - Read Signature from
 Board ID failed.
CRTVERCRLFL - Fail to verify Peer Certificate Due to CRL. REGIDCHG    - Region ID config
update
CRTVERFL    - Fail to verify Peer Certificate.           REGIDMIS    - Region ID set
mismatch.
CTORGNMMIS  - Certificate Org name mismatch.             RESTRQFAIL  - Rest request failed.
DCONFAIL    - DTLS connection failure.                   RMGSPR      - Remove Global saved
 peer.
DEVALC      - Device memory Alloc failures.              RXTRDWN     - Received Teardown.
DHSTMO      - DTLS HandShake Timeout.                    SERNTPRES   - Serial Number not
present.
DISCVBD     - Disconnect vBond after register reply.     SSLNFAIL    - Failure to create
new SSL context.
DISTLOC     - TLOC Disabled.                             STENTRY     - Delete same tloc
stale entry.
DUPCLHELO   - Recd a Dup Client Hello, Reset Gl Peer.    STNMODETD   - Teardown extra vBond
 in STUN server mode.
DUPSER      - Duplicate Serial Number.                   SYSIPCHNG   - System-IP changed.
DUPSYSIPDEL - Duplicate System IP.                       SYSPRCH     - System property
changed.
EMBARGOFAIL - Embargo check failed                       TMRALC      - Timer Object Memory
```

```
 Failure.
HAFAIL      - SSL Handshake failure.                    TUNALC      - Tunnel Object Memory
 Failure.
HWCERTREN   - Hardware vEdge Enterprise Cert Renewed     TXCHTOBD    - Failed to send
challenge to BoardID.
HWCERTREV   - Hardware vEdge Enterprise Cert Revoked.    UNAUTHEL    - Recd Hello from
Unauthenticated peer.
IP_TOS      - Socket Options failure.                    UNMSGBDRG   - Unknown Message
type or Bad Register msg.
LISFD       - Listener Socket FD Error.                  VBDEST      - vDaemon process
terminated.
MEMALCFL    - Memory Allocation Failure.                 VECRTREV    - vEdge Certification
 revoked.
MGRTBLCKD   - Migration blocked. Wait for local TMO.     VB_TMO      - Peer vBond Timed
out.
NEWVBNOVMNG - New vBond with no vMng connections.        VM_TMO      - Peer vManage Timed
 out.
NOACTVB     - No Active vBond found to connect.          VP_TMO      - Peer vEdge Timed
out.
NOERR       - No Error.                                  XTVMTRDN    - Teardown extra
vManage.
NOSLPRCRT   - Unable to get peer's certificate.


     PEER                          PEER
PEER      PEER      PEER             SITE         LOCAL                      PEER
     PRIVATE   PEER               PUBLIC                    LOCAL       REMOTE      REPEAT
TYPE      PROTOCOL  SYSTEM IP          ID           INTERFACE                  PRIVATE IP
     PORT      PUBLIC IP         PORT     STATE            ERROR       ERROR       COUNT
DOWNTIME
------------------------------------------------------------------------------------------------------------------------------------
vbond     dtls      0.0.0.0           0            TenGigabitEthernet0/0/2   10.0.12.26
     12346     10.0.12.26        12346    tear_down        DISCVBD     NOERR       0
2023-11-07T14:19:54+0000
vbond     dtls      0.0.0.0           0            TenGigabitEthernet0/0/2_  2001:a0:c::1a
     12346     2001:a0:c::1a     12346    tear_down        PSEV6DISC   NOERR       0
2023-11-07T14:19:30+0000
vbond     dtls      0.0.0.0           0            TenGigabitEthernet0/0/2   10.0.12.26
     12346     10.0.12.26        12346    up               LISFD       NOERR       0
2023-11-07T14:19:30+0000
vbond     dtls      0.0.0.0           0            TenGigabitEthernet0/0/2   10.0.12.26
     12346     10.0.12.26        12346    tear_down        DISTLOC     NOERR       0
2023-11-07T14:19:26+0000
```

show sd-routing control connections summary

To display information about the active control-plane connections on a device operating in the SD-Routing mode, use the show **sd-routing control connections summary** command in privileged EXEC mode.

show sd-routing control connections summary

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, and Cisco 1000 Series Integrated Services Routers.

Usage Guidelines

When compared to the output of the **show sd-routing control connections details** command, the output of **show sd-routing control connections summary** command excludes detailed Tx and Rx statistics related to each control connection.

The following is sample output of the **show sd-routing control connections summary** command:

```
Device# show sd-routing control connections summary

                     PEER                                                PEER
PEER     PEER  PEER             SITE        LOCAL                        PEER
                     PRIV   PEER                                        PUB
TYPE     PROT  SYSTEM IP        ID          INTERFACE                    PRIVATE IP
                     PORT   PUBLIC IP                                   PORT   STATE   UPTIME

-----------------------------------------------------------------------------------------------------------
vmanage  dtls  172.16.255.22    200         TenGigabitEthernet0/0/2   10.0.12.22
                    12546  10.0.12.22                              12546  up      2:01:26:16
```

show sd-routing control local-properties summary

To display the summary of the status of a device and root certificate installation in the SD routing mode, use the **show sd-routing control local-properties summary** command in privileged EXEC mode.

show sd-routing control local-properties summary

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router .

Usage Guidelines

You can use this command when you are onboarding a device. The output helps you verify the status of a device and root certificate installation of WAN interfaces.

Example

The following is sample output of the **show sd-routing control local-properties summary** command:

```
Device#show sd-routing control local-properties summary
 personality                      vedge
sp-organization-name              vIPtela Inc Regression
organization-name                 vIPtela Inc Regression
root-ca-chain-status              Installed
root-ca-crl-status                Not-Installed

certificate-status                Installed
certificate-validity              Valid
certificate-not-valid-before      Nov 27 08:53:44 2023 GMT
certificate-not-valid-after       Nov 26 08:53:44 2024 GMT

enterprise-cert-status            Not Applicable
enterprise-cert-validity          Not Applicable
enterprise-cert-not-valid-before  Not Applicable
enterprise-cert-not-valid-after   Not Applicable

dns-name                          vbond
site-id                           100
protocol                          dtls
tls-port                          0
system-ip                         172.16.255.21
chassis-num/unique-id             C8K-9bdc48d2-4987-4d49-8f28-e62e72900628
serial-num                        1234570D
subject-serial-num                N/A
enterprise-serial-num             Not Applicable
token                             Invalid
keygen-interval                   0:02:00:00
retry-interval                    0:00:00:18
no-activity-exp-interval          0:00:00:20
dns-cache-ttl                     0:00:02:00
port-hopped                       FALSE
time-since-last-port-hop          0:00:00:00
```

```
embargo-check                    success
number-vbond-peers               2
number-active-wan-interfaces     1
```

show sd-routing control local-properties vbond

To display vBond-related information about local control properties of WAN interfaces in the SD routing mode, use the **show sd-routing control local-properties vbond** command in privileged EXEC mode.

show sd-routing control local-properties vbond

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router .

Usage Guidelines

You can use this command when you are onboarding a device. The output helps you verify the vBond information about local control properties of WAN interfaces.

Example

The following is sample output of the **show sd-routing control local-properties vbond** command:

```
Device#show sd-routing control local-properties vbond
 INDEX    IP                                        PORT
-----------------------------------------------------------
0        10.0.12.26                                12346
1        2001:a0:c::1a                             12346
```

show sd-routing control local-properties wan detail

To display detailed information about local control properties of WAN interfaces in the SD routing mode use the **show sd-routing control local-properties wan detail** command in privileged EXEC mode.

show sd-routing control local-properties wan detail

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router .

Usage Guidelines

The NAT type information is displayed only when two or more vBonds are configured.

Example

The following is sample output of the **show sd-routing control local-properties wan detail** command:

```
Device#show sd-routing control local-properties wan detail
NAT Type: E -- indicates End-point independent mapping
          A -- indicates Address-port dependent mapping
          N -- indicates Not learned
          Note: Requires minimum two vbonds to learn the NAT type

Interface GigabitEthernet1
  Public  IPv4       : 50.0.1.14
  Public  Port       : 65104
  Private IPv4       : 50.0.1.14
  Private IPv6       : 2001:320:1::e
  Private Port       : 65104
  State              : up
  Number of vManages : 1
  Control            : yes
  STUN               : no
  Low Bandwidth Link : no
  Last Connection    : 0:05:23:05
  SPI Remaining Time : 0:00:00:00
  NAT Type           : N
  vManage Connection : 5
  Region IDs         : 0
```

show sd-routing control local-properties wan ipv4

To display IPv4 related information about local control properties of WAN interfaces in the SD routing mode use the **show sd-routing control local-properties wan ipv4** command in privileged EXEC mode.

show sd-routing control local-properties wan ipv6

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router .

Usage Guidelines

Example

The following is sample output of the **show sd-routing control local-properties wan ipv4** command:

```
Device#show sd-routing control local-properties wan ipv6
 PUBLIC           PUBLIC  PRIVATE          PRIVATE
INTERFACE                      IPv4             PORT    IPv4             PORT     STATE
-------------------------------------------------------------------------------------
GigabitEthernet1               50.0.1.14        65314   50.0.1.14        65314    up
```

show sd-routing control local-properties wan ipv6

To display IPv6 related information about local control properties of WAN interfaces in the SD routing mode use the **show sd-routing control local-properties wan ipv6** command in privileged EXEC mode.

show sd-routing control local-properties wan ipv6

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router .

Usage Guidelines

Example

The following is sample output of the **show sd-routing control local-properties wan ipv6** command:

```
Device#show sd-routing control local-properties wan ipv6
                                PUBLIC  PRIVATE                                 PRIVATE
INTERFACE                       PORT    IPv6                                    PORT
STATE
-------------------------------------------------------------------------------------------
GigabitEthernet1                65314   2001:320:1::e                           65314
up
```

show sd-routing system status

To display the system status information of WAN interfaces in the SD routing mode, use the **show sd-routing system status** command in privileged EXEC mode.

show sd-routing system status

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.12.1a	This command was introduced on Cisco Catalyst 8200, 8300, and 8500 Series Edge Platforms, Cisco Catalyst 8000V Edge Software, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, and Cisco ASR 1000 Series Aggregation Services Router .

Usage Guidelines

You can use this command when you are onboarding a device. The output helps you verify the status of a device.

Example

The following is sample output of the **show sd-routing system status** command:

```
Device#show sd-routing system status
 Cisco IOS XE Software
Copyright (c) 2023-2023 by Cisco Systems, Inc.
Controller Compatibility: 20.14
Version: 17.14.01.0.190568

System logging to host  is disabled
System logging to disk is enabled

System state:            GREEN. All daemons up
System FIPS state:       Disabled

Last reboot:             factory-reset
CPU-reported reboot:     Initiated by other
System uptime:           1 days 04 hrs 18 min 48 sec
Current time:            Tue Nov 28 13:05:25 UTC 2023

Hypervisor Type:         KVM
Cloud Hosted Instance:   false

Load average:            1 minute: 0.61, 5 minutes: 0.54, 15 minutes: 0.50
Processes:               323 total
CPU allocation:          4 total,   1 control,   3 data
CPU states:              4.37% user, 3.47% system, 92.14% idle
Memory usage:            6016884K total,    3153512K used,   2863372K free
                         7464K buffers,  2404412K cache

Disk usage:             Filesystem                      Size   Used  Avail   Use %  Mounted
 on
                         /dev/disk/by-label/fs-bootflash   4933M  968M   3693M   21%
/bootflash

Personality:             vEdge
```

```
Model name:              C8000V
Device role              Autonomous
Services:                None
vManaged:                false
Commit pending:          false
Configuration template:
Chassis serial number:   SSI130300YK
```