
Troubleshoot IKE and IPsec



For supported software information, click [here](#).

This article describes how to troubleshoot IKE and IPsec issues.

View the IKE Session History

To troubleshoot an IKE session, you display information about the session history. To do this, issue the **show orgs org-services ipsec vpn-profile ike history** CLI command. The command output displays IKE session history information, including information about sessions that flapped and the reason for the flap. For example:

```
versa@PoP3-Ten1-Branch2-cli> show orgs org-services My-Organization ipsec vpn-profile branch-cntrl1
ike history
Local Gateway: 10.3.12.1   Remote Gateway: 10.1.1.121
Last Known State      : Active (Rekey)
Last State Timestamp  : 2015-12-21T06:25:5518.101768-00:00
Event History:
0. Event      : IKE Rekey
   Timestamp  : 2015-12-21T06:25:5526.560768-00:00
   Role       : initiator
   Inbound SPI : 0x3fd02bbfd83d0002
   Outbound SPI: 0xe28dedee106e0002
1. Event      : IKE Rekey
   Timestamp  : 2015-12-20T23:00:24534.391488-00:00
   Role       : initiator
   Inbound SPI : 0xaf42d13b41ae0002
   Outbound SPI: 0x32dd83255e370002
2. Event      : IKE Rekey
   Timestamp  : 2015-12-20T15:34:53165.19972-00:00
   Role       : initiator
   Inbound SPI : 0x598148d4b880002
   Outbound SPI: 0x8d396252e73a0002
3. Event      : IKE Rekey
   Timestamp  : 2015-12-20T08:09:21060.162088-00:00
   Role       : initiator
   Inbound SPI : 0xdd149fd165df0002
   Outbound SPI: 0xcd3cd3f7e85d0002
```

View the IKE Security Association

To display the IKE security association, issue the **show orgs org-services ipsec vpn-profile ike security-associations brief** CLI command. For example:

```
versa@PoP3-Ten1-Branch2-cli> show orgs org-services My-Organization ipsec vpn-profile branch-cntrl1
ike security-associations brief
REMOTE
GATEWAY  PROFILE NAME  LOCAL SPI      REMOTE SPI      TRANSFORM
-----
10.1.1.121 branch-cntrl1 0x3fd02bbfd83d0002 0xe28dedee106e0002 aes-cbc
```

View IPsec IKE Authentication Failure Event

When the authentication information sent by the peer does not match the configured peer authentication information in the local VPN profile, the `ipseclkeAuthFailure` event is generated. This failure event reports VPN connection failures that occurred because of invalid credentials or a mismatch of credentials.

The `ipseclkeAuthFailure` event has the following format:

```
Event: "ipseclkeAuthFailure",
Severity: indeterminate,
Key: peer-ip-address | tunnel-identifier,
Description: "IKE connection with peer peer-ip-address remote id remote-id (routing-instance vrf-name) failed."
```

Note that the `ipseclkeAuthFailure` event is not generated if the authentication information sent by the peer matches the configured peer authentication information, but the local authentication information does not match the peer configuration. In this case, the authentication failure is reported by the peer device. If the peer device is a VOS device, that device generates the `ipseclkeAuthFailure` event.

To display the generated alarms, issue the **show alarms** command. For example:

```
admin@host-app2-cli> show alarms last-n 5
Module      Alarm              Time              Text
=====
ipsec       ipsecTunnelUp      2020-05-28T05:05:17-0 org1: IPSEC tunnel with peer 10.10.10.1 (routing-
instance org1-vrf) is up
ipsec       ipsecTunnelDown    2020-05-28T05:13:32-0 org1: IPSEC tunnel with peer 10.10.10.1 (routing-
instance org1-vrf) is down
ipsec       ipseclkeAuthFailure 2020-05-28T05:13:32-0 org1: IKE authentication with peer 10.10.10.1
remote id app1@test.com (routing-instance org1-vrf) failed
ipsec       ipseclkeAuthFailure 2020-05-28T05:13:48-0 org1: IKE authentication with peer 10.10.10.1
remote id app1@test.com (routing-instance org1-vrf) failed
ipsec       ipsecTunnelUp      2020-05-28T05:13:53-0 org1: IPSEC tunnel with peer 10.10.10.1 (routing-
instance org1-vrf) is up
```

View IPsec Tunnel Information

To display information about the IPsec tunnel, issue the **show orgs org-services ipsec vpn-profile security-associations brief** CLI command. For example:

```
versa@PoP3-Ten1-Branch2-cli> show orgs org-services My-Organization ipsec vpn-profile branch-cntrl1 security-associations brief
```

Remote Gateway	Transform	Inbound SPI	Bytes/sec	Outbound SPI	Bytes/sec	Tunnel Status	Up Time
10.3.11.1	aes-cbc	0x20aebb9	0	0x20b5bba	0	UP	1071 sec

View Overall IPsec Statistics

To determine the total number of IKE and IPsec sessions, follow these steps. The commands in this procedure provide the number of Phase 1 failures and rekeys, and other related information.

1. Log in to vsmd from the shell:

```
admin# vsh connect vsmd
```

2. Check the IPsec statistics:

```
vsm-vcsn0> show ipsec stats
----- IPsec Control Plane Stats from PM -----
IKE SA Active      : 4
IPSec SA Active    : 4
P1 Done            : 30
P1 failed          : 4
P1 rekeyed         : 19
IKE SA             : 7
IKE SA Initiated   : 7
IKE SA Responded   : 0
IKE Attempts       : 11
IKE Attempts Initiated: 11
IKE Attempts Responded: 0
IKE Packets in     : 98
IKE Packets out    : 162
IKE Octets in      : 16296
IKE Octets out     : 31472
IKE Retransmits    : 57
IKE Discarded Packets : 0
IKE Init Failures  : 4
Init NO responses  : 4
resp failures      : 0
Engine Active Flows : 4
Transforms         : 4
Fast Path Packets In : 104
Fast Path Packets Fwd : 0
```

3. To display tenant-specific IPsec statistics, issue the **show ipsec stats tCLI** command. To display IPsec statistics for all tenants, issue the **show ipsec stats 0** CLI command.

Troubleshoot IPsec in Stage 1 and Stage 2

To diagnose IPsec problems in Stage 1 and Stage 2 communication:

1. To check whether the IPsec session between the branch and the Controller is up, issue the **show orgs org-services ipsec vpn-profile security-associations brief** CLI command. For example:

```
versa@PoP3-Ten1-Branch2-cli> show orgs org-services My-Organization ipsec vpn-profile branch-
cntrl1 security-associations brief

Remote Gateway  Transform  Inbound SPI  Bytes/sec  Outbound SPI  Bytes/sec  Tunnel Status  Up Time
-----
10.3.11.1       aes-cbc    0x20aebb9    0           0x20b5bba     0          UP              1071 sec
```

2. If the IPsec session between the branch and the Controller is not up:
 - a. Check the IPsec configuration to ensure that local and remote authentication parameters match and that the local and remote IP addresses are for VNI interfaces.
 - b. To check that the configuration has been applied and is present in the backend, issue the **show ipsec config 0 all** CLI command. Check that the output of the Loaded parameter displays Yes. For example:

```
vsm-vcsn0> show ipsec config 0 all
##### Tenant 2 config #####
-----
VPN Name - branch-cntrl1, OBJ ID 1, VPN ID 1
VPN Type - Branch-SD-WAN
VRF ID - mgmt1(18)
Tunnel VRF ID - mgmt1(18)
VSN ID - 0
Loaded - Yes
Local - 10.3.12.1
----- Local Identity -----
Auth Type - Pre Shared Key
ID Type - EMAIL
ID - br2_west_email@Provider.com
PSK - 1234
----- IPsec Datapath Configuration -----
Anti Replay : Enabled
Mode : Tunnel
PFS : 0
Transform : 1
Lifetime : 25000 seconds, 0 mbytes
----- IKE Control Path Configuration -----
DH Group : 19
Transform : 1
Lifetime : 27000
Version : 2
DPD Timeout : 10
----- ## Flows 0 -----
```

- If this step fails, the issue is with the data path. Use data plane diagnostics to debug the problem.

- ```
admin@PoP3-Ten2-Branch5-cli> show interfaces brief
```
- | NAME      | IP                | MAC               | OPER | ADMIN | TNT | VRF     |
|-----------|-------------------|-------------------|------|-------|-----|---------|
| tvi-0/3   |                   | n/a               | up   | up    |     |         |
| tvi-0/3.0 | [ 10.3.1.113/24 ] | n/a               | up   | up    | 1   | mgmt    |
| vni-0/0   |                   | 52:0a:30:be:05:02 | up   | up    |     |         |
| vni-0/0.0 | [ 113.1.1.5/24 ]  | 52:0a:30:be:05:02 | up   | up    | 1   | grt-vrf |
| vni-0/1   |                   | 52:0a:30:be:05:03 | down | down  |     |         |
| vni-0/2   |                   | 52:0a:30:be:ce:04 | down | down  |     |         |

- Issue the **vsh connect infmgr** shell command to connect to infmgr.
  - Issue the **show p2mp management-routing-instance** CLI command, and check for a valid VNF manager address, which is the Director IP address.
- If Step 3 is successful, ping from Versa Director to the branch device.
- If the ping fails, check whether the proper route for the Director IP address is installed in the branch device's route table
- Issue the **ssh** command to access branch device from Versa Director.

## Troubleshoot the Interface Manager Process

To determine whether packets are flowing on the control path, check the status of the Versa interface manager process (infmgr). This process is responsible for creating, configuring, and deleting interface elements, and it acts as a conduit for sending and receiving control path packets to other Versa processes.

- ### Connect to infmgr:

```
admin@SDWAN-Branch1:~$ vsh connect infmgr
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.
```

[illegible]

2. To check that the expected Director IP address is included in the addresses and subnets listed under the VNF manager (indicated by the vnf-mgr string in the command output), issue the **show p2mp-nbrs detail org provider-org self** command. For example:

```
infmgr> show p2mp-nbrs detail org provider-org self
network-id 20, branch-id 106B, site-id 0x6a00, rtt-index 32, tenant-id 12, site-name SDWAN-Branch1,
parent-nwid 0, mgmt-nw-id 20, flags: CFG SELF, location-id Unique-location-id, start-time 2019-07-
23T14:43:29;
site-type = SDWAN, chassis-id a96067ac-35f3-4764-93d8-8e25d530d1c4, hwdev-id br101.TechPub-
Testbed
mgmt_ip: 10.20.64.106
tunnel: (local: 10.20.0.106, remote: 10.20.0.106) [[encap-outer 0x5, encap-inner 0x1, nbrtun_cfgidx 0]]
tunnel: (local: 10.20.64.106, remote: 10.20.64.106) [[encap-outer 0x5, encap-inner 0x3, nbrtun_cfgidx 0]]
NBR:link id 1[EP], RTT WAN1-Transport-VR, seq 1, mtu 1500, transp-doms[2], inet(local-ip 192.168.11.
101, ckt-name WAN1)
NBR:link id 2[EP], RTT WAN2-Transport-VR, seq 1, mtu 1500, transp-doms[2], inet(local-ip 192.168.12.
101, ckt-name WAN2)
NBR:link id 3[EP], RTT WAN3-Transport-VR, seq 1, mtu 1500, transp-doms[3], inet(local-ip 192.168.13.
101, ckt-name WAN3)
dynamic-info: SA[117]
0x0801106a1840208008280630053a20718b2cc38c41ab789f0c1f78f7417115f9fbd3f150def60ea6356e6e3f98562d424
dynamic-info: SA(old)[70]
0x6a00130a0605c437793d5e07719c8424cfcb7f2f608e6522a9a079369891f0d9640ef8c2824e6cdd4e306b7695ae5d5e
link-id 1 (vni-0/0.0), , seq 1, nat{public-ip 101.101.101.1:56952, bindings: (10002.1 101.101.101.1:56952
@[2])}
link-id 2 (vni-0/1.0), , seq 1, nat{public-ip 101.101.102.1:62674, bindings: (10002.1 101.101.102.1:62674
@[2])}
local_conf: n_wanlinks 3
vni-0/0.0 IPv4: (ifindex 1148, ip 192.168.11.101, link-id 1, circuit-name WAN1, shaping_rate 0(min 0),
tunnels:encrypt,plaintext, IKE-link, path_meas_interval 0)
vni-0/1.0 IPv4: (ifindex 1150, ip 192.168.12.101, link-id 2, circuit-name WAN2, shaping_rate 0(min 0),
tunnels:encrypt,plaintext, IKE-link, path_meas_interval 0)
vni-0/2.0 IPv4: (ifindex 1152, ip 192.168.13.101, link-id 3, circuit-name WAN3, shaping_rate 0(min 0),
tunnels:encrypt,plaintext, IKE-link, path_meas_interval 0)
branch: mgmt_ifidx [71], vnf-mgr [192.168.75.2/32]
[[source: config; state: , ipc:config]]
```

3. To ensure that a route entry for the Director node is present, log in to the Director node, and issue the **ip route list table all** command. For example:

```
admin@SDWAN-VOAE1:~$ ip route list table all
default via 10.48.0.1 dev eth0
10.0.1.0/24 via 192.168.75.1 dev eth1.701
10.0.30.0/24 via 192.168.75.1 dev eth1.701
10.0.33.0/24 via 192.168.75.1 dev eth1.701
10.0.62.0/24 via 192.168.75.1 dev eth1.701
10.0.65.0/24 via 192.168.75.1 dev eth1.701
10.1.30.0/24 via 192.168.75.1 dev eth1.701
10.1.62.0/24 via 192.168.75.1 dev eth1.701
10.1.64.0/24 via 192.168.75.1 dev eth1.701
10.20.0.0/16 via 192.168.75.1 dev eth1.701
10.21.0.0/16 via 192.168.75.1 dev eth1.701
10.48.0.0/16 dev eth0 proto kernel scope link src 10.48.80.15
192.168.71.0/24 via 192.168.75.1 dev eth1.701
```

```

192.168.72.0/24 via 192.168.75.1 dev eth1.701
192.168.75.0/24 dev eth1.701 proto kernel scope link src 192.168.75.2
broadcast 10.48.0.0 dev eth0 table local proto kernel scope link src 10.48.80.15
local 10.48.80.15 dev eth0 table local proto kernel scope host src 10.48.80.15
broadcast 10.48.255.255 dev eth0 table local proto kernel scope link src 10.48.80.15
broadcast 127.0.0.0 dev lo table local proto kernel scope link src 127.0.0.1
local 127.0.0.0/8 dev lo table local proto kernel scope host src 127.0.0.1
local 127.0.0.1 dev lo table local proto kernel scope host src 127.0.0.1
broadcast 127.255.255.255 dev lo table local proto kernel scope link src 127.0.0.1
broadcast 192.168.75.0 dev eth1.701 table local proto kernel scope link src 192.168.75.2
local 192.168.75.2 dev eth1.701 table local proto kernel scope host src 192.168.75.2
broadcast 192.168.75.255 dev eth1.701 table local proto kernel scope link src 192.168.75.2
unreachable default dev lo table unspec proto kernel metric 4294967295 error -101
fe80::/64 dev eth0 proto kernel metric 256
fe80::/64 dev eth1 proto kernel metric 256
fe80::/64 dev eth1.701 proto kernel metric 256
unreachable default dev lo table unspec proto kernel metric 4294967295 error -101
local ::1 dev lo table local proto none metric 0
local fe80::500a:30ff:fe50:f01 dev lo table local proto none metric 0
local fe80::500a:30ff:fe50:f02 dev lo table local proto none metric 0
local fe80::500a:30ff:fe50:f02 dev lo table local proto none metric 0
ff00::/8 dev eth0 table local metric 256
ff00::/8 dev eth1 table local metric 256
ff00::/8 dev eth1.701 table local metric 256
unreachable default dev lo table unspec proto kernel metric 4294967295 error -101

```

4. If no route entry is present, the likely problem is an issue with the Versa routing process, versa-rtd. For debugging help, contact Versa Customer Support.
5. If the route entry is present, ping from the Director node to the IP address of the branch tvi interface. If the ping command is unsuccessful, it is likely that ICMP packets are being blocked at an intermediate network hop. Issue the **tcpdump** command at all intermediate nodes to determine which node is dropping packets.

## Troubleshoot IPsec Stage 3 Branch-to-Controller Issues

To diagnose problems in Stage 3 communication from the branch to the Controller:

1. To check whether the IPsec session between the branch and the Controller is up, issue the **show orgs org-services ipsec vpn-profile security-associations br** CLI command. For example:

```

versa@PoP3-Ten1-Branch2-cli> show orgs org-services My-Organization ipsec vpn-profile branch-
cntrl1 security-associations br

```

| Remote Gateway | Transform | Inbound SPI | Bytes/sec | Outbound SPI | Bytes/sec | Tunnel Status | Up Time  |
|----------------|-----------|-------------|-----------|--------------|-----------|---------------|----------|
| 10.3.11.1      | aes-cbc   | 0x20aebb9   | 0         | 0x20b5bba    | 0         | UP            | 1071 sec |
| 10.3.13.1      | aes-cbc   | 0x20adbbb   | 0         | 0x20adbba    | 0         | UP            | 1113 sec |
| 10.3.14.1      | aes-cbc   | 0x20adbba   | 0         | 0x20adbba    | 0         | UP            | 339 sec  |
| 10.1.1.121     | aes-cbc   | 0x20069de   | 0         | 0x2000a36    | 0         | UP            | 9728 sec |

2. Check the IPsec configuration to ensure that local and remote authentication parameters match and that the local and remote IP addresses belong to VXLAN TVI interfaces.
3. To check that the configuration has been applied and is present in the backend, issue the **show ipsec config 0 all** CLI command. Check that the output of the Loaded parameter displays Yes. For example:

```
vsm-vcsn0> show ipsec config 0 all
Tenant 2 config

VPN Name - branch-cntrl1, OBJ ID 1, VPN ID 1
VPN Type - Branch-SD-WAN
VRF ID - mgmt1(18)
Tunnel VRF ID - mgmt1(18)
VSN ID - 0
Loaded - Yes <<<< === It should be YES
Local - 10.3.12.1
----- Local Identity -----
Auth Type - Pre Shared Key
ID Type - EMAIL
ID - br2_west_email@Provider.com
PSK - 1234
----- IPsec Datapath Configuration -----
Anti Replay : Enabled
Mode : Tunnel
PFS : 0
Transform : 1
Lifetime : 25000 seconds, 0 mbytes
----- IKE Control Path Configuration -----
DH Group : 19
Transform : 1
Lifetime : 27000
Version : 2
DPD Timeout : 10
----- ## Flows 0 -----
Flow 0 SRC any DST any

```

4. If Step 3 is successful, ping from the local IP address to the remote IP address (these addresses are specified in the IPsec profile) to ensure that the remote IP address is reachable.  
If this step fails, the issue is with the data path. Use data plane diagnostics to debug the problem.
5. If the **vxlan-ping** command from the branch to the Controller succeeds, issue the **esp-ping** command from the branch to the Controller.

A branch that has a complete configuration after staging is referred to as a Stage 3 branch.

## Troubleshooting IPsec Stage 3 Branch-to-Branch Issues

To diagnose problems in Stage 3 communication between two branches:

1. To check whether the IPsec sessions between the branch and all other branches are up, issue the **show orgs org-services ipsec vpn-profile branch-2-branch security-associations br** CLI command. In the command output, the first entry is for the Controller and rest are for branches. The output below has four entries, for one



Controller and three branches. All the IPsec sessions must be up. For example:

```
versa@PoP3-Ten1-Branch2-cli> show orgs org-services Costco ipsec vpn-profile branch-cntrl1
branch-2-branch security-associations br
```

| Remote Gateway                   | Transform | Inbound SPI | Bytes/sec | Outbound SPI | Bytes/sec | Tunnel Status | Up Time                   |
|----------------------------------|-----------|-------------|-----------|--------------|-----------|---------------|---------------------------|
| 10.3.11.1                        | aes-cbc   | 0x20aebb9   | 0         | 0x20b5bba    | 0         | UP            | 1071 sec >>>> First entry |
| is between branch and Controller |           |             |           |              |           |               |                           |
| 10.3.13.1                        | aes-cbc   | 0x20adbba   | 0         | 0x20adbba    | 0         | UP            | 1113 sec >>>> Subsequent  |
| entries are for branch to branch |           |             |           |              |           |               |                           |
| 10.3.14.1                        | aes-cbc   | 0x20adbba   | 0         | 0x20adbba    | 0         | UP            | 339 sec                   |
| 10.1.1.121                       | aes-cbc   | 0x20069de   | 0         | 0x2000a36    | 0         | UP            | 9728 sec                  |

For every remote branch, one PTVI-ESP interface is created, and the DHKEY pair protocol generates and periodically refreshes the IPsec key pairs between any two branches. (Note that the DHKEY pair protocol is used to exchange the IPsec keys for branch-to-branch communication.) This SPI is associated with the PTVI-ESP interface corresponding to the remote branch.

2. Issue an **esp-ping** command between the two branches.
3. If Step 2 fails, enable IPsec debugging logs.  
If the packet is dropped because of an invalid SPI index, ensure that the correct SPI index is associated with PTVI index.

---

## Troubleshoot Certificate-Based Authentication

This section describes how to debug IPsec problems in an SD-WAN network.

---

### View Certificate Information

To display certification information, issue the **show orgs org-services security crypto pki** CLI command. For example:

```
admin@vm1-14-cli> show orgs org-services Provider security crypto pki
security crypto pki private-keys versa-ctrl1-key
algo RSA
modulus 1024
pub-key "AwEAAbSdwDYhEArVISErUJeNeZVWO/bY6DJYWCDLnCxm2tqYgRgk6WF9xs/
XakyVmh9eeHb/nZoCO2LaskPIrJQ+KiNuGGbe1SYnox16qLai9mabkoGWIB1lz+58h7tBzo+
GRODTL6eXN9dlw\
ninKIROUZ4sYZelXTMjyYEHZA2jy9pZuZ"

security crypto pki certificates versa-ctrl1-cert
priv-key versa-ctrl1-key
ca versa-ctrl1-cert
CA-CERT NO
not-before Mar-3-2016
not-after Nov-17-2016
pub-key "AwEAAbSdwDYhEArVISErUJeNeZVWO/bY6DJYWCDLnCxm2tqYgRgk6WF9xs/
XakyVmh9eeHb/nZoCO2LaskPIrJQ+KiNuGGbe1SYnox16qLai9mabkoGWIB1lz+58h7tBzo+
```

```
GRODTL6eXN9dlw\
ninKIROUZ4sYZelXTMjyYEHZA2jy9pZuZ"
cert-data
"MIIDMzCCAhugAwIBAgIIbQJwQtyCHZEwDQYJKoZIhvcNAQEFBQAwwFjEUMBIGA1UEAwwLVmVyl
nc2FUZXN0Q0EwHhcNMTYwMzAzMjAxMTA4WhcNMTYxMTE3MTgxMTM3WjBzMScwJQYDVQQDDDB52\
nZXJzYS1jdHJsMS52ZXJzYS1uZXR3b3Jrcy5jb20xETAPBgNVBAsMCHNvZnR3YXJIMQ4wDAYD\
nVQKDAV2ZXJzYTELMaGA1UEBwwCU0MxCzAJBgNVBAGMAKNBMQswCQYDVQQGEwJVUzCBnzAN\
nBgqhkiG9w0BAQEFAAOBjQAwgYkCgYEAzJ3ANiEQCtUhlStQl415IVY79tjoMlhYIMucLGba\
n2piBGCTpYX3Gz9dqTJWaH154dv9mgI7Ytqwo8islD4ql24YZt7VJiejHXqotqL2ZpuSgZaUH\
nUjP7nyHu0HOj4ZE4NMvp5c312XCkcoHE5Rnixhl4hdMyPjGqfMDaPL2lm5kCAwEAAaOBqzCB\
nqDAdBgNVHQ4EFgQUUGJzicSi+eD8NgdR8Em6YQYU9wfsWDAYDVR0TAAQH/BAlwADAfBgNVHSME\
nGDAWgBQA5Ca3UiqJzkJapVXtFD0Jf43BezAOBgNVHQ8BAf8EBAMCBeAwHQYDVROIBBYwFAYI\
nKwYBBQUHAWIGCCsGAQUFBwMEMCkGA1UdEQQiMCCBHnZlcnNhLWN0cmwxQHZlcnNhLW5ldHdv\
ncmtzLmNvbTANBgqhkiG9w0BAQUFAAOCAQEAljg59j9OdI7XOqDN2Y9KkNmFEcNrJvn+Cwp8\inxJxnW\
AtZQkQ9JFTY5gf9oYdmPnuzXOI8FzNZ+xestAwWC8nV0kIWf7jHA2ZKbsKhHN9JZ9S\
nza+/38A+KFMlyF3sF61Orgh9kLUF+SXR5F1wWLuST0IzfRJIhur4qGchVIPKpHla9fSKukt\
nEURkh14oQZlRQIBDWxv5eiYIKHa1TkGj6SlgiKRvSEcz+Se541ow2M7pr/OQpesw2yJWtOd\
nLlw5JHPHe4m71Bysyd9Ly3yBpukU5tsjKrZN+jma0lfuWLI/1HA4IIPwYvpK5OdMh88L/pt\ntp6eEhD1no8+
AJreKvg=="
```

```
security crypto pki ca-chains versa-ca
ca-chain-certificates 21437e7376b2747332bb51107198e436
ca-name "CommonName: VersaTestCA, orgUnit: , organization: "
ca-cert-data
"MIIDETCCAfmGAWIBAgIIYRn5dAOLT70wDQYJKoZIhvcNAQEFBQAwwFjEUMBIGA1UEAwwLVmVyl
nc2FUZXN0Q0EwHhcNMTUxMTE3MTgxMTM3WhcNMTYxMTE3MTgxMTM3WjBzMScwJQYDVQQDDDAw\
nZXJzYVRlc3RDQTCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJk59iQdxcFyQuLU\
na1sI2Pba7IUI1G0AGZ4NTLTx6lr7E3aVaYAb97y7a5kUMq2jf8ovg493Dm7UsHHIsILpNHG1\
nqLKbG7gPotUXb/D0mFqFcRp1KaKSp+4BA4BdgDhUG08YtwLTT3w8TCzaqrFE+if6+JkUT1W\
nkNMEeOnppDGCBj3Dh2TJcylCjDnWoxolqlozVv964mPYZUy+O1CM0Q5yJ4oZeyel1dTQMXw6\
nhta9qpeJ54vMxG91Yg1DWB/BWrs1p1v7uwBYU5bgEIE46h50ILXLIQe0d891N/i6PAWd9\
nhLGEg9TuwInDAks4OpZ32MI32ZGZLN5RgPNI7t8CAwEAAANjmGEwHQYDVRO0BBYEFADkJrdS\
nKonOQlqIve0UPQl/jcF7MA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgwFoAUAOQmt1lqic5C\
nWqVV7RQ9CX+NwXswDgYDVR0PAQH/BAQDAgGGMA0GCSqGSIb3DQEBBQUAA4IBAQBZFpBJwVQM\
niY2RylCADC5Vf3kkGzBXqaQirtE59bMQytzgF/28H7g8n+GTz0RDoBclgPbPunyWLuNK5Qx8\
nh55fi7Tm21k5Kckzh/xFQKYEn6011QhgXhvdv11qlnxCOJxd+Q7ELAWe1t+ml74mgDcB/L5Q\
ncURVAjJiSjDh0IOeFaj6fW69CP4F2KLpnl0OIGIsXylwgrLXD2+Oub4w4de2dou58GgVUu9S\
nkSKTxNRJXvosk3dGfg9tR+Ovhl4psiXg/8Axw5ZrgwtFRUIA7DfmTuDxzfqdvtCJ7U87jNGh\
ne6mawICTy0VxnhWHnCsKc3Akra6duJCilCe2q5F1FXd"
```

## View the IPsec Configuration

To display the IPsec configuration, issue the **show ipsec config 0 all** CLI command. For example:

```
vsm-vcsn0> show ipsec config 0 all
Tenant 1 config

VPN Name - gw1, OBJ ID 1, VPN ID 1
VPN Type - Controller-SD-WAN
DHKey: Profile = []
VRF ID - mgmt(10)
Tunnel VRF ID - mgmt(10)
```

[https://docs.versa-networks.com/Secure\\_SD-WAN/03\\_Troubleshooting/Troubleshoot\\_IKE\\_and\\_IPsec](https://docs.versa-networks.com/Secure_SD-WAN/03_Troubleshooting/Troubleshoot_IKE_and_IPsec)

Updated: Wed, 23 Oct 2024 08:07:09 GMT

Copyright © 2024, Versa Networks, Inc.

```

VSN ID - 0
Loaded - Yes
Crypto offload - Enabled (i.e. use if any hw-accel available)
Local - 10.10.1.1
----- Local Identity -----
Auth Type - Certificate
Certificate-Authority - versa-ca
Certificate present
Private key present
ID Type - EMAIL
ID - versa-ctrl1@versa-networks.com
----- IPsec Datapath Configuration -----
Anti Replay : Enabled
Mode : Tunnel
PFS : 0
Transform : 1
Lifetime : 25000 seconds, 0 mbytes
----- IKE Control Path Configuration -----
DH Group : 19
Transform : 1
Lifetime : 28000
Version : 2
DPD Timeout : 30
----- ## Flows 0 -----
-- General AddrRange NetMask #Subnets 0 VSN 0---
VSN 0 - Range
-- Mgmt AddrRange NetMask #Subnets 0 VSN 0---
VSN 0 - Range
--RAC AuthType 2, EAP Type 0, #Clients 0 --

```

## View the Certificate Management Protocol

To display a summary of the certification information, issue the **show certd csr summary** CLI command. For example:

```

certd> show certd csr summary 1
CSR-Name Request-State

provider-br1-cert Sign-Done

certd> show certd csr stats 1 provider-br1-cert
CERTD CSR (provider-br1-cert) stats for Tenant: 1

CERTD srvr: provider-ca
Cert check success (IR) : 1
Interface down (IR) : 0
Interface addr unavailable (IR) : 0
Auth-key fail (IR) : 0
Auth-cert fail (IR) : 0
Prv-key gen fail (IR) : 0
CSR gen fail (IR) : 0
CSR enroll sent (IR) : 0
Switch ns fail (IR) : 0

```

|                                  |     |
|----------------------------------|-----|
| Revert ns fail (IR)              | : 0 |
| Cert sign success (IR)           | : 0 |
| CA cert sign success (IR)        | : 0 |
| Cert sign rejected (IR)          | : 0 |
| Cert sign done (IR)              | : 0 |
| Cert sign failure (IR)           | : 0 |
| Cert check success (KUR)         | : 0 |
| Interface down (KUR)             | : 0 |
| Interface addr unavailable (KUR) | : 0 |
| Auth-key fail (KUR)              | : 0 |
| Auth-cert fail (KUR)             | : 0 |
| Prv-key gen fail (KUR)           | : 0 |
| CSR gen fail (KUR)               | : 0 |
| CSR enroll sent (KUR)            | : 0 |
| Switch ns fail (KUR)             | : 0 |
| Revert ns fail (KUR)             | : 0 |
| Cert sign success (KUR)          | : 0 |
| CA cert sign success (KUR)       | : 0 |
| Cert sign rejected (KUR)         | : 0 |
| Cert sign done (KUR)             | : 0 |
| Cert sign failure (KUR)          | : 0 |

---

## Supported Software Information

Releases 20.2 and later support all content described in this article.

---

## Additional Information

[Configure IPsec VPN Profiles](#)

[Troubleshoot the SD-WAN Data Path](#)