SECURE CONNECT

IBM Cloud

Configuration Guide for The Classic Infrastructure on IBM Cloud

June 2024

JUNIPER NETWORKS | Driven by Experience

Contents

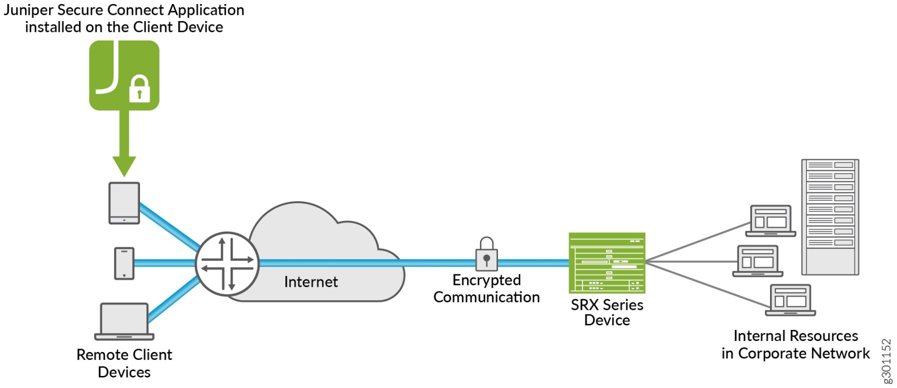
What Is Juniper Secure Connect?

Juniper Secure Connect is a client-based SSL-VPN application that allows you to securely connect and access protected resources on your network. This application, when combined with the vSRX, helps organizations quickly achieve dynamic, flexible, and adaptable connectivity from devices anywhere across the globe. Juniper Secure Connect extends visibility and enforcement from client to cloud using secure VPN connections.

Juniper Secure Connect solution includes:

vSRX Firewall—Serves as an entry and exit point for communication between users with Juniper Secure Connect and the protected resources on the corporate network or in the cloud.

Juniper Secure Connect application—Secures connectivity between the protected resources and the host clients running Microsoft Windows, Apple macOS and iOS/iPadOS, and Android operating systems. The Juniper Secure Connect application connects through a VPN tunnel to the vSRX Series firewall to gain access to the protected resources in the network.



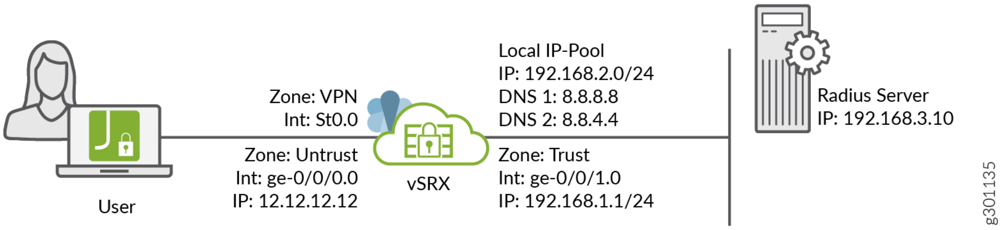
BENEFITS OF JUNIPER SECURE CONNECT

- Secure remote access from anywhere with VPN
- Simple user experience
- Easy management of remote clients, policies, and VPN events from a single console

(using J-Web or Security Director Cloud)

DEPLOYMENT SCENARIO FOR JUNIPER SECURE CONNECT

For traffic to flow correctly, you can either include a route in the protected network for the IP address that you assign to the clients directs to the vSRX or NAT all client traffic coming into the protected networks.



Click here for more deployment scenarios.

Preparing the vSRX for Juniper Secure Connect Configuration using J-Web

This section is intended to guide users on configuring Juniper Secure Connect on the vSRX in the IBM Cloud Classic Infrastructure using the Graphical User interface (J-Web)

Listed below is the step-by-step procedure on how to prepare the vSRX, and helpful links that will answer the most common questions when configuring Juniper Secure Connect.

NOTE: *All vSRX versions* ***23.2R2-S1*** *and under have been provisioned with J-Web access disabled due to security vulnerabilities explained in detail under the following article* ***JSA72300***

Starting in ***23.4R1-S2*** *the above JSA has been fixed and the vSRX will not face vulnerabilities while enabling web access to proceed with setting up Secure Connect as it is required for remote session connection to get established.*

Before you proceed with enabling web-management access to the vSRX device make sure you are aware of your code version and the vulnerabilities mentioned above.

Using the command line prompt connected utilizing the root user via SHH or Telnet, execute the following command enable web-management:

```
root@vSRX:~ # cli
root@vSRX > edit
Entering configuration mode
The configuration has been changed but not committed

[edit]
root@vSRX# activate system services web-management

[edit]
root@vSRX# commit and-quit
commit complete
Exiting configuration mode
```

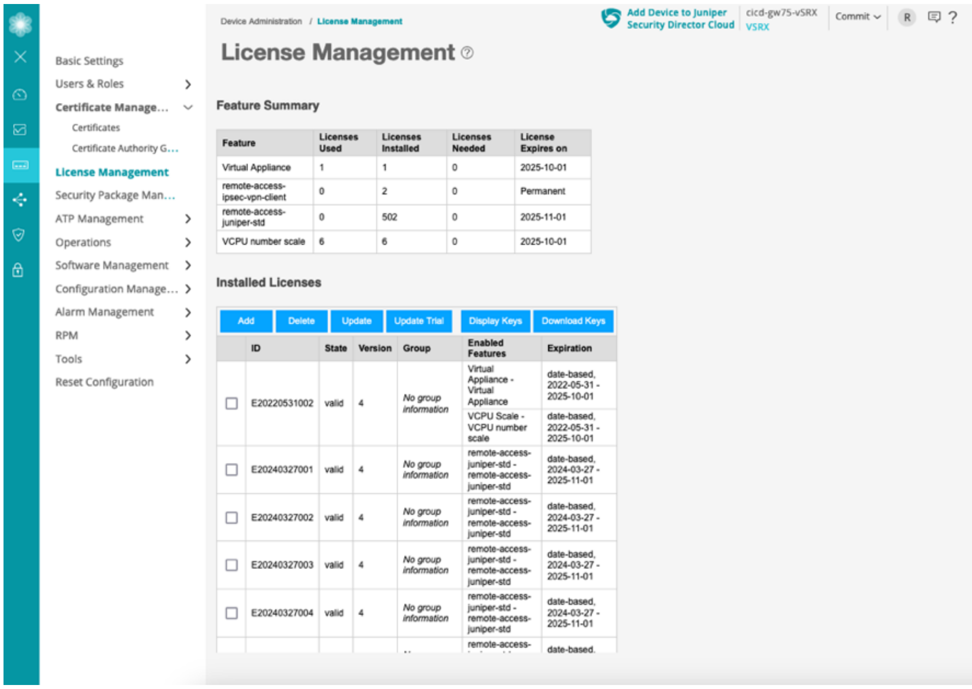
1. Check Secure Connect License Using J-Web
2. Enable Port Traffic for IKE And ESP Protocols Using J-Web
3. Generate a Device Certificate Using J-Web
4. Enable Device Certificate for Web Management Access Using J-Web
5. Configure Dedicated HTTPS Access Using J-Web

1. Configure Juniper Secure Connect With Local Authentication Using J-Web

CHECK SECURE CONNECT LICENSES USING J-WEB

This guide was created using a vSRX with version code **23.2R2.**

In the J-Web side pane, navigate to Device **Administration > License Management**



License Management

Feature Summary

Feature	Licenses Used	Licenses Installed	Licenses Needed	License Expires on
Virtual Appliance	1	1	0	2025-10-01
remote-access-ipsec-vpn-client	0	2	0	Permanent
remote-access-juniper-std	0	502	0	2025-11-01
VCPU number scale	6	6	0	2025-10-01

Installed Licenses

Add | Delete | Update | Update Trial | Display Keys | Download Keys

	ID	State	Version	Group	Enabled Features	Expiration
□	E20220531002	valid	4	*No group information*	Virtual Appliance - Virtual Appliance	date-based, 2022-05-31 - 2025-10-01
					VCPU Scale - VCPU number scale	date-based, 2022-05-31 - 2025-10-01
□	E20240327001	valid	4	*No group information*	remote-access-juniper-std - remote-access-juniper-std	date-based, 2024-03-27 - 2025-11-01
□	E20240327002	valid	4	*No group information*	remote-access-juniper-std - remote-access-juniper-std	date-based, 2024-03-27 - 2025-11-01
□	E20240327003	valid	4	*No group information*	remote-access-juniper-std - remote-access-juniper-std	date-based, 2024-03-27 - 2025-11-01
□	E20240327004	valid	4	*No group information*	remote-access-juniper-std - remote-access-juniper-std	date-based, 2024-03-27 - 2025-11-01
					remote-access-	date-based,

***Note**: All vSRX firewalls will come with two built-in remote-access concurrent connections.*

If you need to order additional remote access VPN user licenses for the Juniper vSRX you may purchase either as part of your IBM Cloud Gateway order or by adding to an existing IBM Cloud Juniper Gateway. The licenses support 50 users per license, and you can order up to 10 licenses. They will be automatically added to the existing vSRX instance when the purchase is complete.

To order your new licenses from your IBM Cloud Portal, visit the following link for more details.

https://cloud.ibm.com/docs/vsrx?topic=vsrx-getting-started#choosing-license

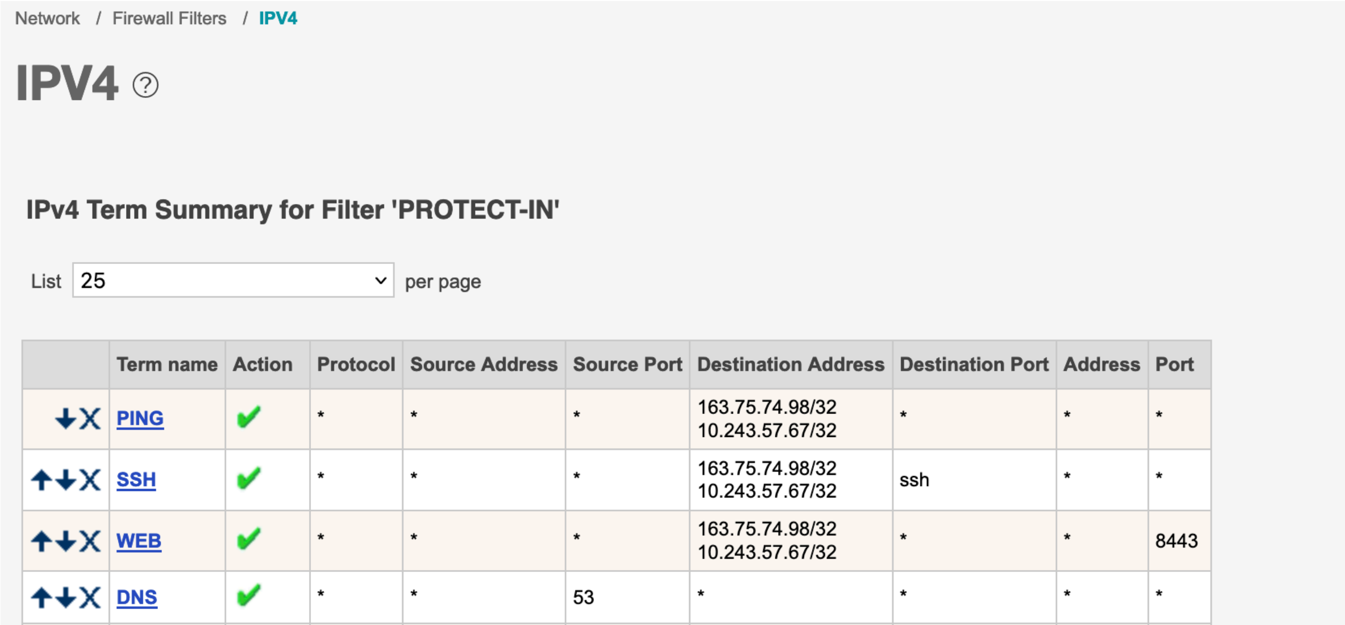
To check your existing purchased licenses, visit the following link for more details.

https://cloud.ibm.com/docs/vsrx?topic=vsrx-vsrx-licenses

ENABLE PORT TRAFFIC FOR IKE AND ESP PROTOCOLS USING J-WEB

After configuring the following firewall filters, the specified ports will be allowed to communicate to the external interface of the vSRX, in our case will be the remote users connecting over SSL-VPN.

In the J-Web side pane, navigate to **Network > Firewall Filters / IPV4** and click on 'PROTECT-IN' filter.



Network / Firewall Filters / IPV4

IPV4 ?

IPv4 Term Summary for Filter 'PROTECT-IN'

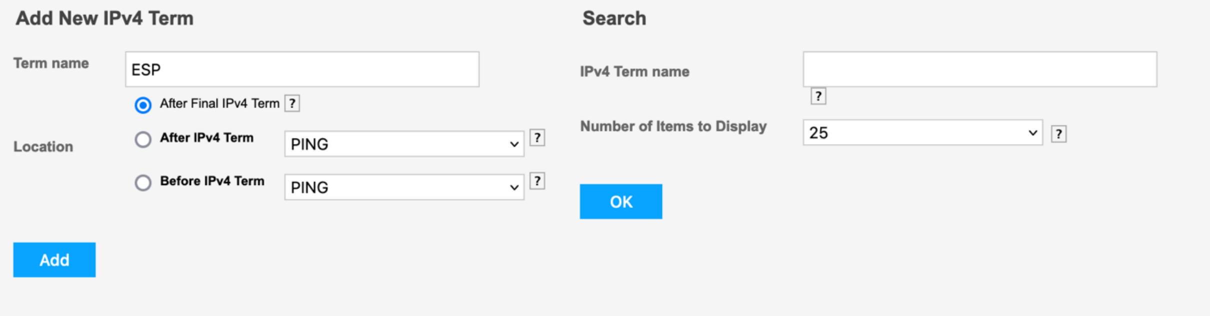
List 25 per page

	Term name	Action	Protocol	Source Address	Source Port	Destination Address	Destination Port	Address	Port
↓ X	PING	✓	*	*	*	163.75.74.98/32 10.243.57.67/32	*	*	*
↑ ↓ X	SSH	✓	*	*	*	163.75.74.98/32 10.243.57.67/32	ssh	*	*
↑ ↓ X	WEB	✓	*	*	*	163.75.74.98/32 10.243.57.67/32	*	*	8443
↑ ↓ X	DNS	✓	*	*	53	*	*	*	*

At the bottom of the screen, you will find an area where you can add new IPv4 terms to the 'PROTECT-IN' filter.

1. Create filter for ESP

Type ESP under the term mane and hit the **Add** button.



Add New IPv4 Term

Term name: ESP

Location:
● After Final IPv4 Term ?
○ After IPv4 Term PING ?
○ Before IPv4 Term PING ?

Add

Search

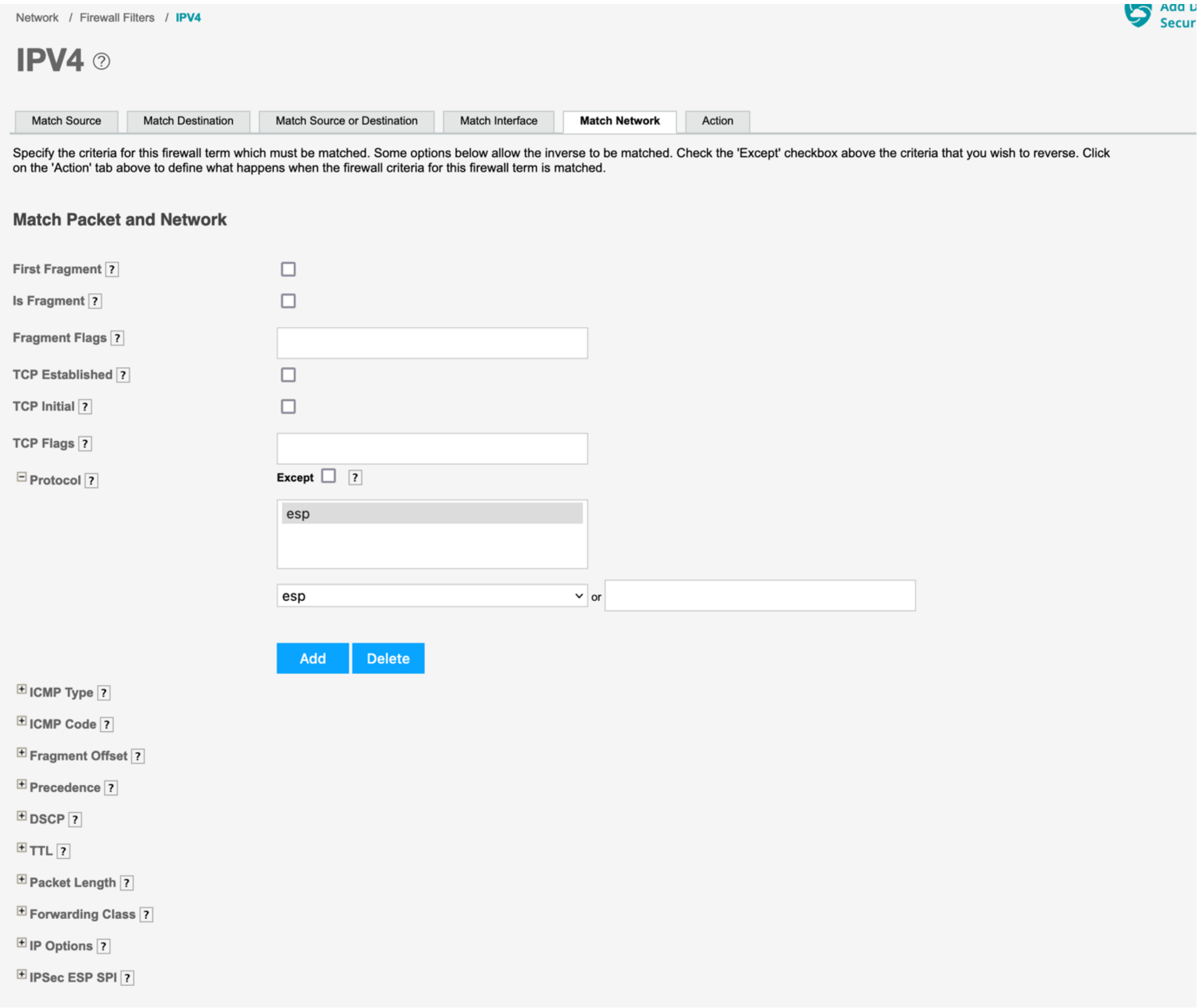
IPv4 Term name: ?

Number of Items to Display: 25 ?

OK

Once you add the new term to the filter you will see it under the table. Click the new tern ESP and define the acceptance criteria.

Select **Match Network** at the upper tab menu and select **esp** protocol by expanding the predefined protocol dropdown.



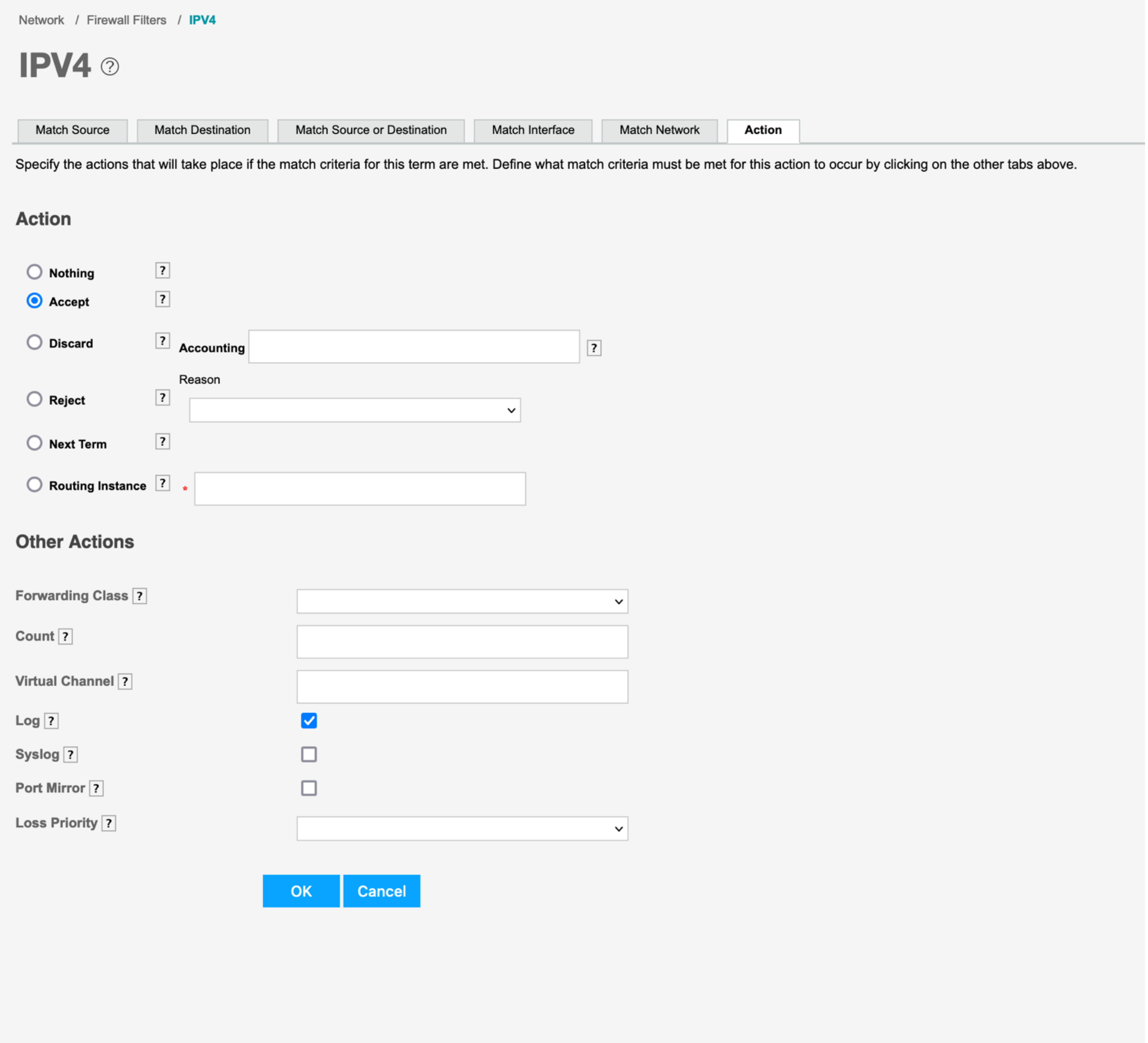
Specify the criteria for this firewall term which must be matched. Some options below allow the inverse to be matched. Check the 'Except' checkbox above the criteria that you wish to reverse. Click on the 'Action' tab above to define what happens when the firewall criteria for this firewall term is matched.

Match Packet and Network

- First Fragment ? □
- Is Fragment ? □
- Fragment Flags ?
- TCP Established ? □
- TCP Initial ? □
- TCP Flags ?
- ⊟ Protocol ? Except □ ?
  - esp
  - esp or
- ⊞ ICMP Type ?
- ⊞ ICMP Code ?
- ⊞ Fragment Offset ?
- ⊞ Precedence ?
- ⊞ DSCP ?
- ⊞ TTL ?
- ⊞ Packet Length ?
- ⊞ Forwarding Class ?
- ⊞ IP Options ?
- ⊞ IPSec ESP SPI ?

Click the **Add** button and then click on **Action** at the upper tab menu.

Define Action to accept traffic and then enable the log knob to save all protocol handshake activity.



Network / Firewall Filters / IPV4

IPV4

Specify the actions that will take place if the match criteria for this term are met. Define what match criteria must be met for this action to occur by clicking on the other tabs above.

Action

○ Nothing

● Accept

○ Discard

Accounting Reason

○ Reject

○ Next Term

○ Routing Instance *

Other Actions

Forwarding Class

Count

Virtual Channel

Log ☑

Syslog □

Port Mirror □

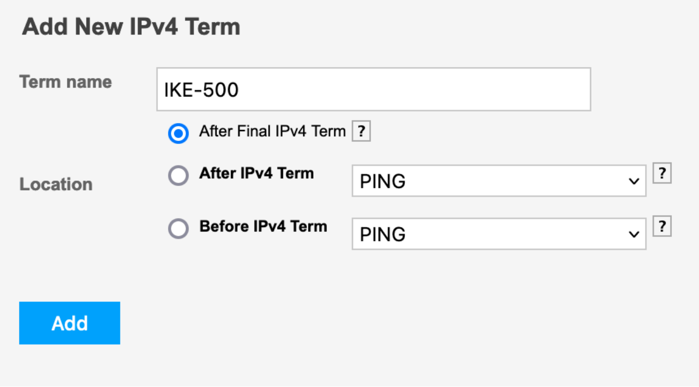
Loss Priority

Hit **OK** and then commit the Configuration.

2. Create filter for IKE-500

Navigate back to Network > Firewall Filters / IPV4 **and click on 'PROTECT-IN' filter.**

Type **IKE-500** under the term mane and hit the **Add** button.



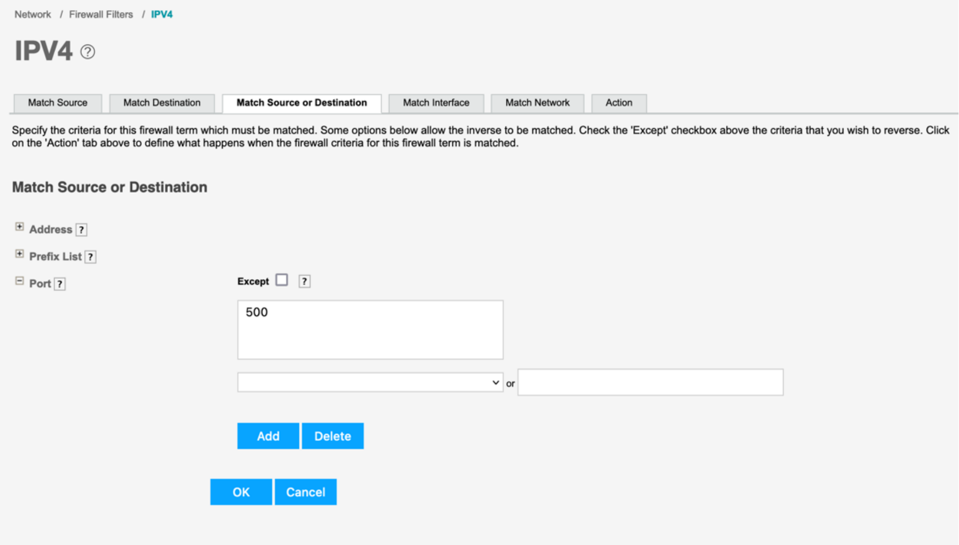
Add New IPv4 Term

Term name: IKE-500

Location:
- ● After Final IPv4 Term ?
- ○ **After IPv4 Term** PING ?
- ○ **Before IPv4 Term** PING ?

Once you add the new term to the filter you will see it under the table. Click the new term IKE-500 and define the acceptance criteria.

Select **Match Source or Destination** at the upper tab menu and expand port and type 500 and hit **OK.**



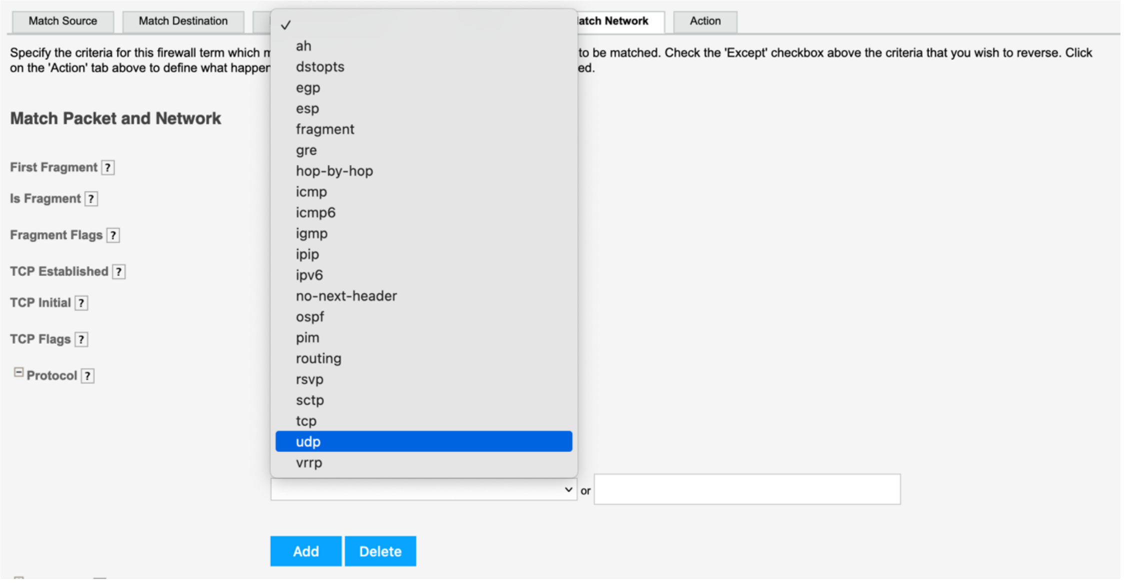
Specify the criteria for this firewall term which must be matched. Some options below allow the inverse to be matched. Check the 'Except' checkbox above the criteria that you wish to reverse. Click on the 'Action' tab above to define what happens when the firewall criteria for this firewall term is matched.

Match Source or Destination

- ⊞ Address ?
- ⊞ Prefix List ?
- ⊟ Port ? — Except □ ? — 500

Select **Match Network** at the upper tab menu and select **UDP** protocol by expanding the predefined protocol dropdown.

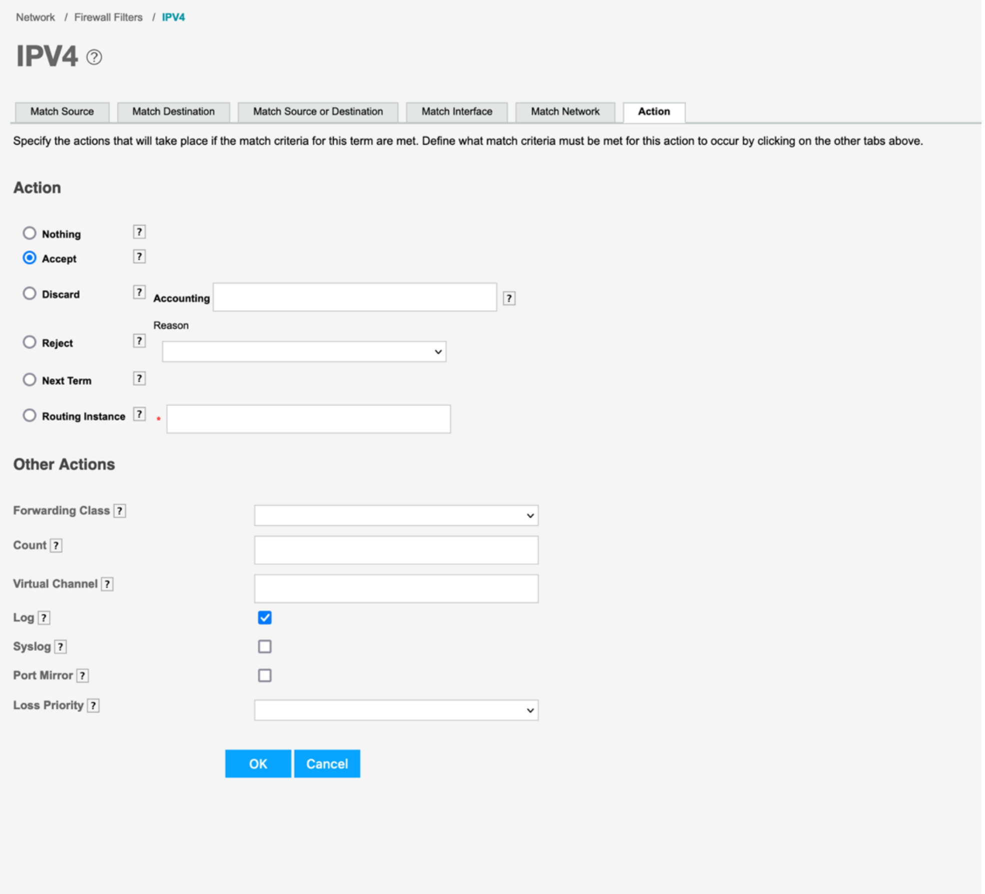
Click the **Add** button and then click on **Action** at the upper tab menu.



Specify the criteria for this firewall term which m to be matched. Check the 'Except' checkbox above the criteria that you wish to reverse. Click on the 'Action' tab above to define what happer ed.

Match Packet and Network

Define Action to accept traffic and then enable the log knob to save all protocol handshake activity.



Specify the actions that will take place if the match criteria for this term are met. Define what match criteria must be met for this action to occur by clicking on the other tabs above.

Action

○ Nothing

● Accept

○ Discard Accounting

Reason

○ Reject

○ Next Term

○ Routing Instance *

Other Actions

Forwarding Class

Count

Virtual Channel

Log ☑

Syslog □

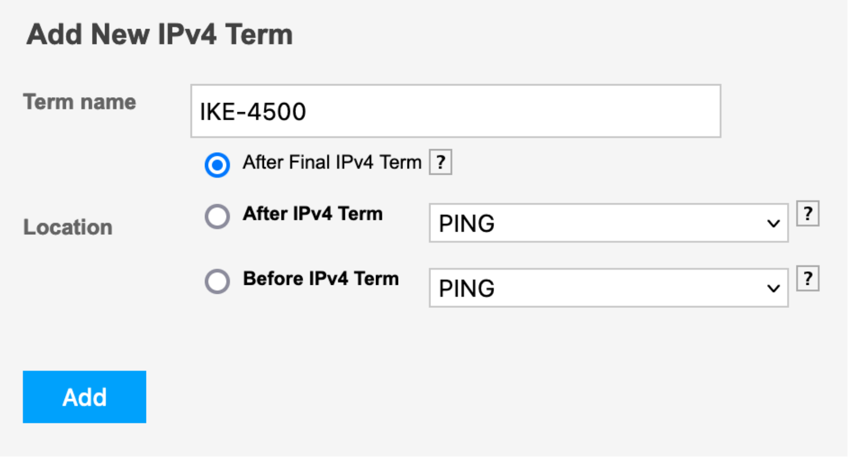
Port Mirror □

Loss Priority

Hit **OK** and then commit the Configuration.

3. **Create filter for IKE-4500**

4. Type IKE-4500 under the term mane and hit the **Add** button.



Add New IPv4 Term

Term name: IKE-4500

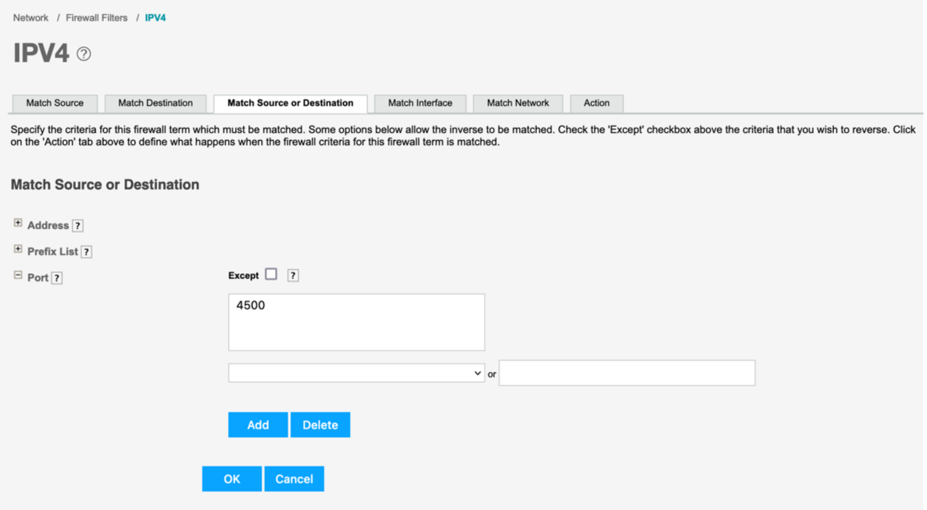
Location: ● After Final IPv4 Term

○ After IPv4 Term: PING

○ Before IPv4 Term: PING

5. Once you add the new term to the filter you will see it under the table. Click the new term IKE-4500 and define the acceptance criteria.

6. Select **Match Source or Destination** at the upper tab menu and expand Port and type 4500 and hit **OK.**



Network / Firewall Filters / IPV4

IPV4

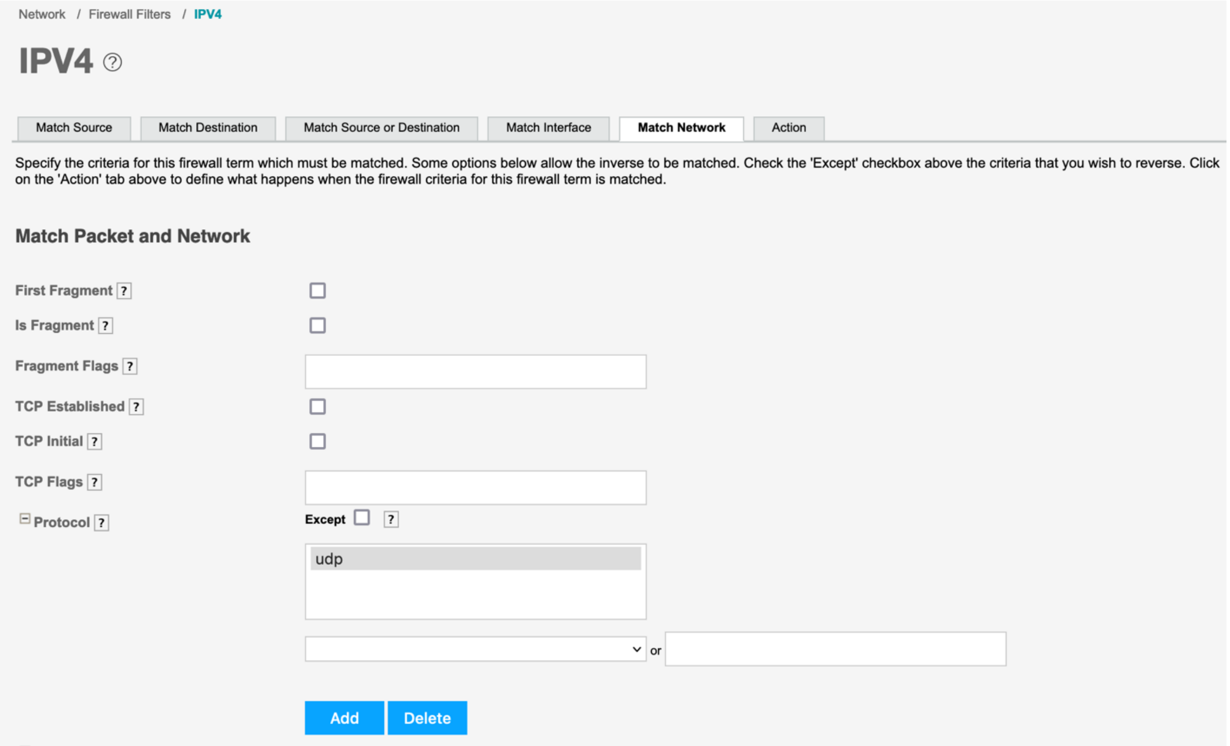
Specify the criteria for this firewall term which must be matched. Some options below allow the inverse to be matched. Check the 'Except' checkbox above the criteria that you wish to reverse. Click on the 'Action' tab above to define what happens when the firewall criteria for this firewall term is matched.

Match Source or Destination

Port: Except □

4500

7. Select **Match Network** at the upper tab menu and select **udp** protocol by expanding the predefined protocol dropdown.

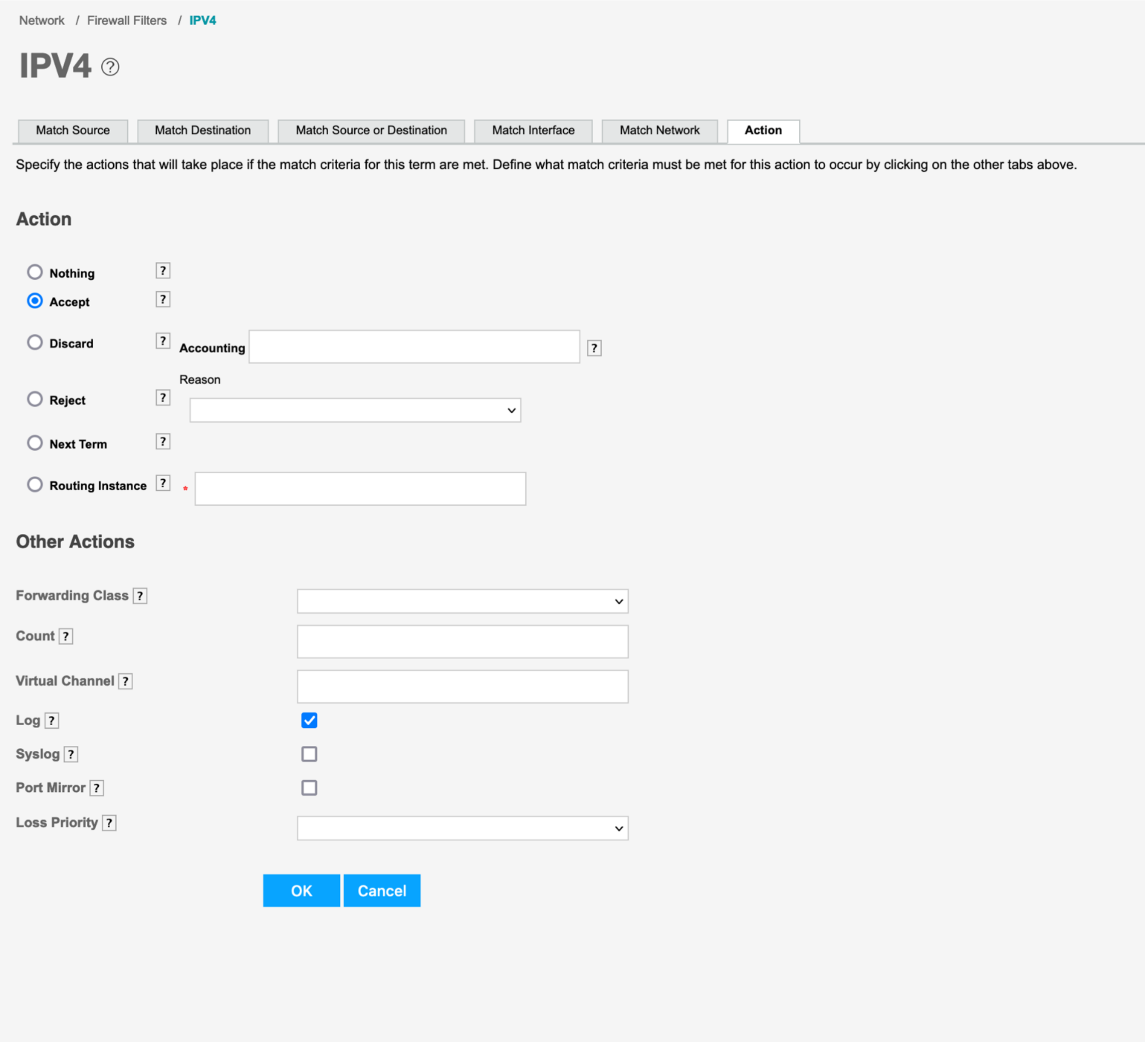


Specify the criteria for this firewall term which must be matched. Some options below allow the inverse to be matched. Check the 'Except' checkbox above the criteria that you wish to reverse. Click on the 'Action' tab above to define what happens when the firewall criteria for this firewall term is matched.

Match Packet and Network

First Fragment ?	□
Is Fragment ?	□
Fragment Flags ?	
TCP Established ?	□
TCP Initial ?	□
TCP Flags ?	
⊟ Protocol ?	Except □ ? udp

8. Click the **Add** button and then click on **Action** at the upper tab menu.



Network / Firewall Filters / IPV4

IPV4

Specify the actions that will take place if the match criteria for this term are met. Define what match criteria must be met for this action to occur by clicking on the other tabs above.

Action

○ Nothing
● Accept
○ Discard — Accounting
Reason
○ Reject
○ Next Term
○ Routing Instance *

Other Actions

Forwarding Class
Count
Virtual Channel
Log ☑
Syslog □
Port Mirror □
Loss Priority

9. Define Action to accept traffic and then enable the log knob to save all protocol handshake activity.

10. Hit **OK** and then commit the Configuration.

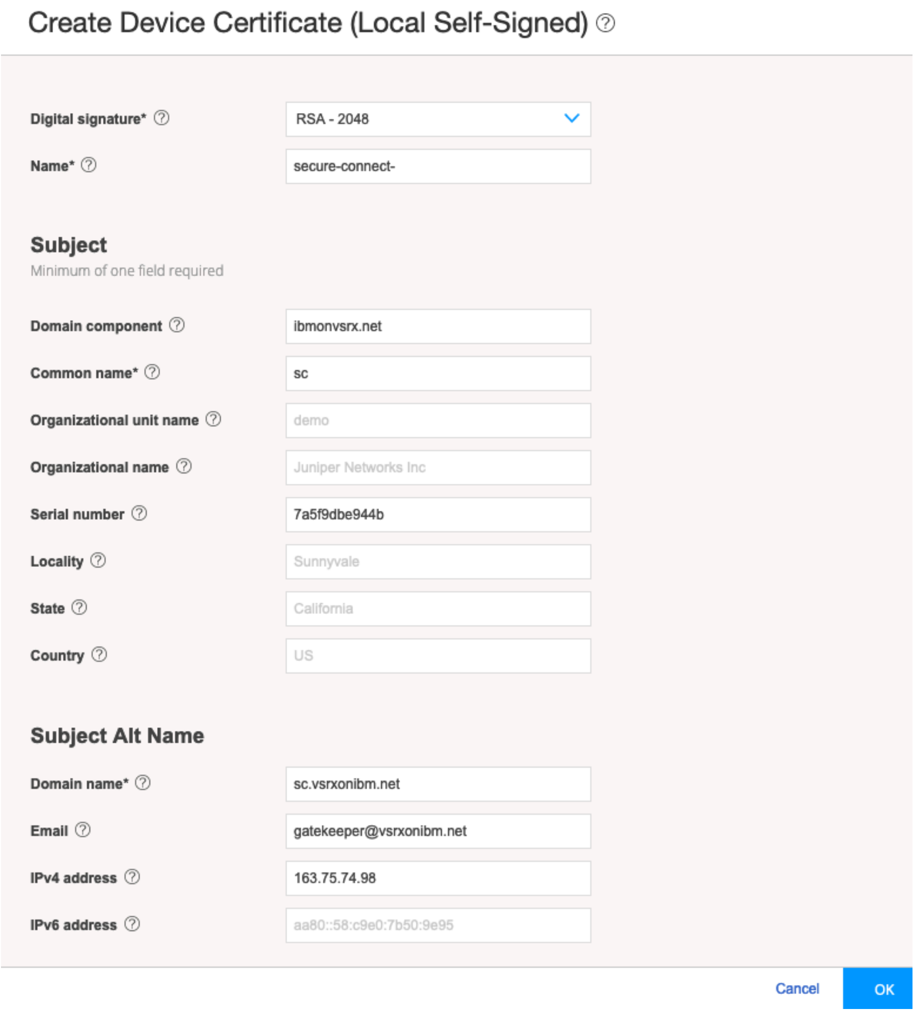
GENERATE A DEVICE CERTIFICATE USING J-WEB

Ensure that the vSRX uses either a signed certificate or a self-signed certificate instead of the default system-generated certificate. Log in to your vSRX using J-Web interface using your preferred browser.

https://<your-ip_address>:8443/

After logging in successfully, you land on the Basic Settings page, In the J-Web side pane, navigate to **Device Administration > Certificate Management > Certificates**

Then click the **Create** button and select **Device Certificate > Local Self-Signed**



Create Device Certificate (Local Self-Signed)

Digital signature*	RSA - 2048
Name*	secure-connect-

Subject

Minimum of one field required

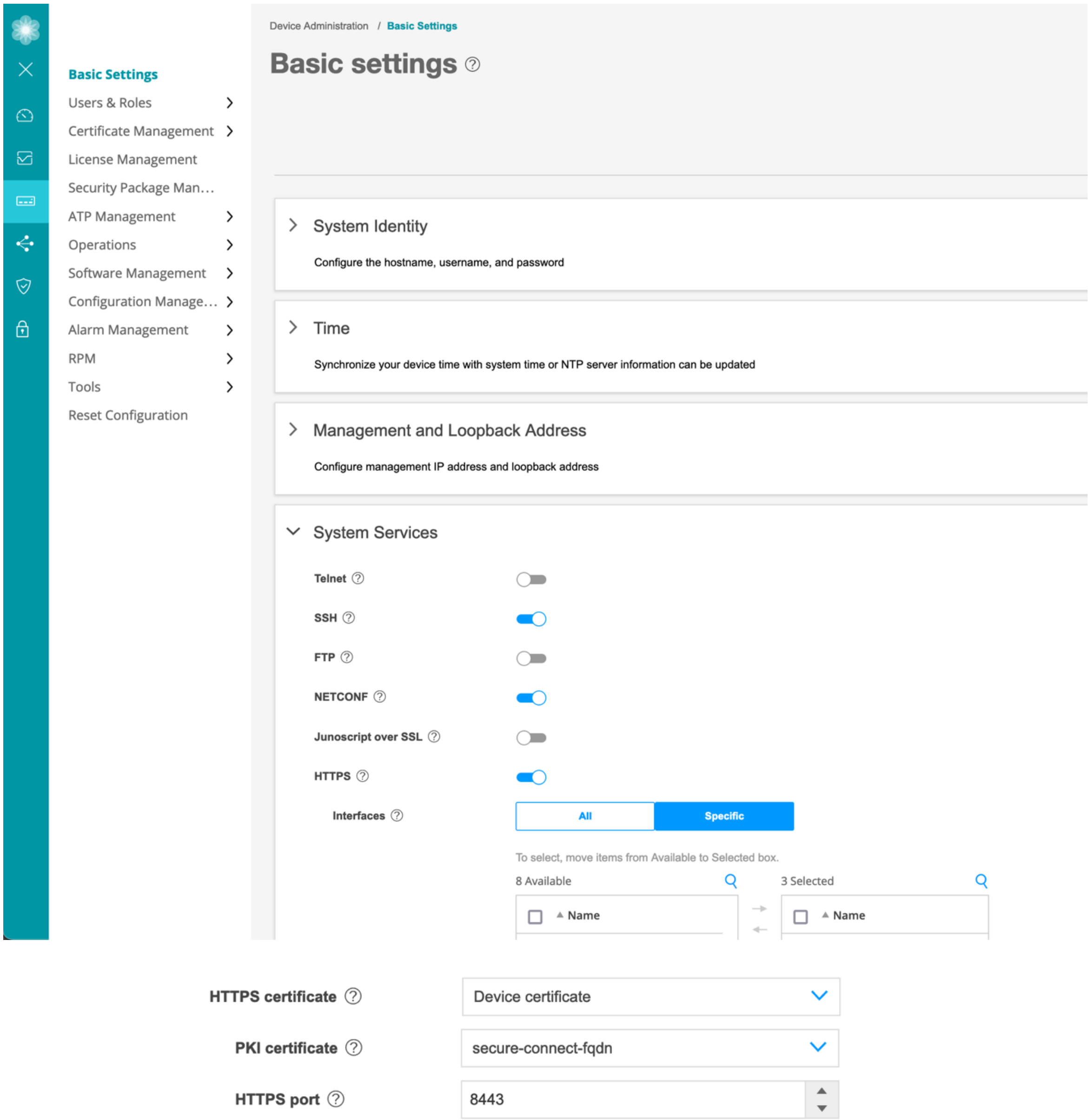
Domain component	ibmonvsrx.net
Common name*	sc
Organizational unit name	demo
Organizational name	Juniper Networks Inc
Serial number	7a5f9dbe944b
Locality	Sunnyvale
State	California
Country	US

Subject Alt Name

Domain name*	sc.vsrxonibm.net
Email	gatekeeper@vsrxonibm.net
IPv4 address	163.75.74.98
IPv6 address	aa80::58:c9e0:7b50:9e95

ENABLE DEVICE CERTIFICATE FOR WEB MANAGEMENT ACCESS USING J-WEB

After creating a self-signed or loading a signed certificate, you must bind the certificate to the vSRX by navigating to **Device Administration > Basic Settings > System Services > HTTPS > HTTPS certificate** and select Device Certificate, then select the one you created in the previous step.



System Identity

Configure the hostname, username, and password

Time

Synchronize your device time with system time or NTP server information can be updated

Management and Loopback Address

Configure management IP address and loopback address

System Services

Telnet: off

SSH: on

FTP: off

NETCONF: on

Junoscript over SSL: off

HTTPS: on

Interfaces: All / **Specific**

To select, move items from Available to Selected box.

8 Available — Name

3 Selected — Name

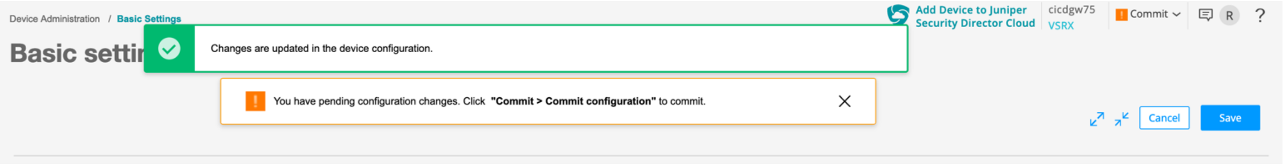
HTTPS certificate: Device certificate

PKI certificate: secure-connect-fqdn

HTTPS port: 8443

Click **Save** to complete the Basic Settings configuration.

Click the highlighted **Commit** button (at the top right of the page next to Feedback Button) to commit the configuration.


Device Administration / Basic Settings
Basic settir
Add Device to Juniper Security Director Cloud
cicdgw75
VSRX
Commit
R
?
Cancel
Save

Changes are updated in the device configuration.

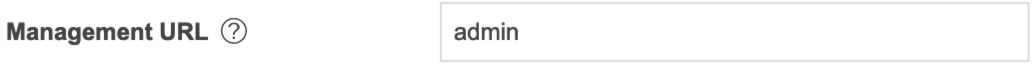
You have pending configuration changes. Click **"Commit > Commit configuration"** to commit.

When the certificate has been loaded to the vSRX, you can validate the certificate by viewing the certificate information in your browser bar. The steps involved in viewing the certificate information depend on your browser and browser version.

CONFIGURE DEDICATED HTTPS ACCESS USING J-WEB

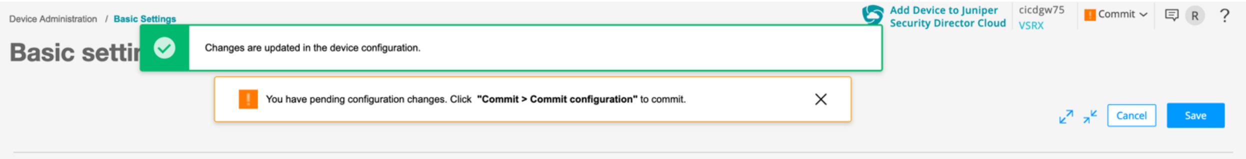
At the Basic Settings page, In the J-Web, Expand the **System Services** and scroll down to where **Management URL** can be defined and type your desired realm.

NOTE: *For this example, we will be defining our access as "***admin***", but network admins may set their preferred name for this path.*



Management URL: admin

Click **Save** to complete the Basic Settings configuration. Click the highlighted **Commit** button (at the top right of the page next to Feedback Button) to commit the configuration.

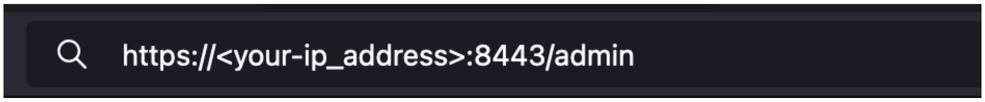


Device Administration / Basic Settings
Basic settir
Add Device to Juniper Security Director Cloud
cicdgw75
VSRX
Commit
R
?
Cancel
Save

Changes are updated in the device configuration.

You have pending configuration changes. Click **"Commit > Commit configuration"** to commit.

Now your J-Web portal can be accessed by appending the word `admin` after the port number.



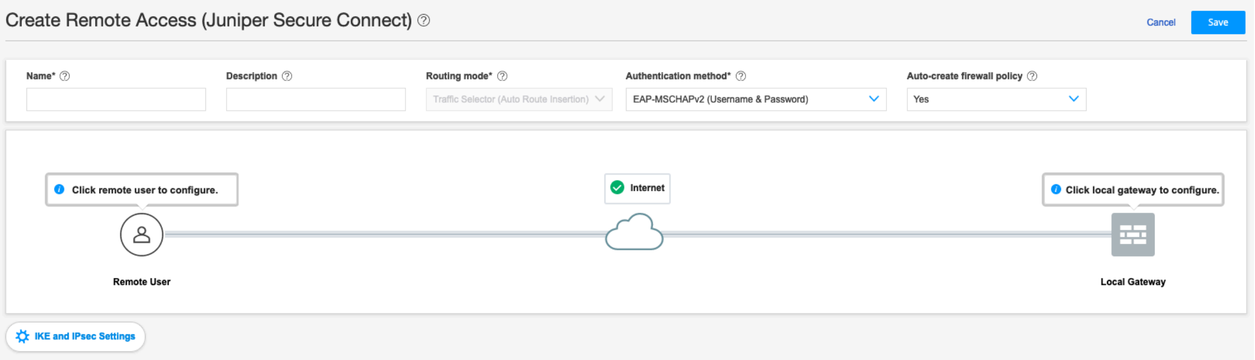
https://<your-ip_address>:8443/admin

CONFIGURE JUNIPER SECURE CONNECT WITH LOCAL AUTHENTICATION USING J-WEB

During the following steps, we will be defining a local authentication example for deployment. Click here for more deployment scenarios.

In the J-Web side pane, navigate to **Network > VPN > IPsec VPN**

At the right corner of the page, select **Create VPN > Remote Access > Juniper Secure Connect** to create the IPsec VPN setting for Juniper Secure Connect.



Create Remote Access (Juniper Secure Connect) ⓘ

Name* ⓘ:

Description ⓘ:

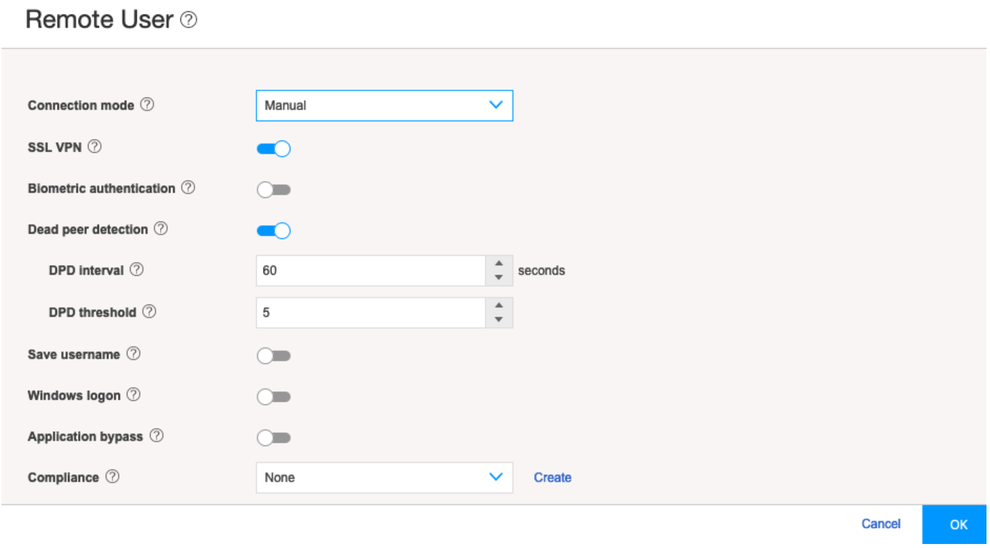
Routing mode* ⓘ: Traffic Selector (Auto Route Insertion)

Authentication method* ⓘ: EAP-MSCHAPv2 (Username & Password)

Auto-create firewall policy ⓘ: Yes

Cancel
Save
Click remote user to configure.
Internet
Click local gateway to configure.
Remote User
Local Gateway
IKE and IPsec Settings

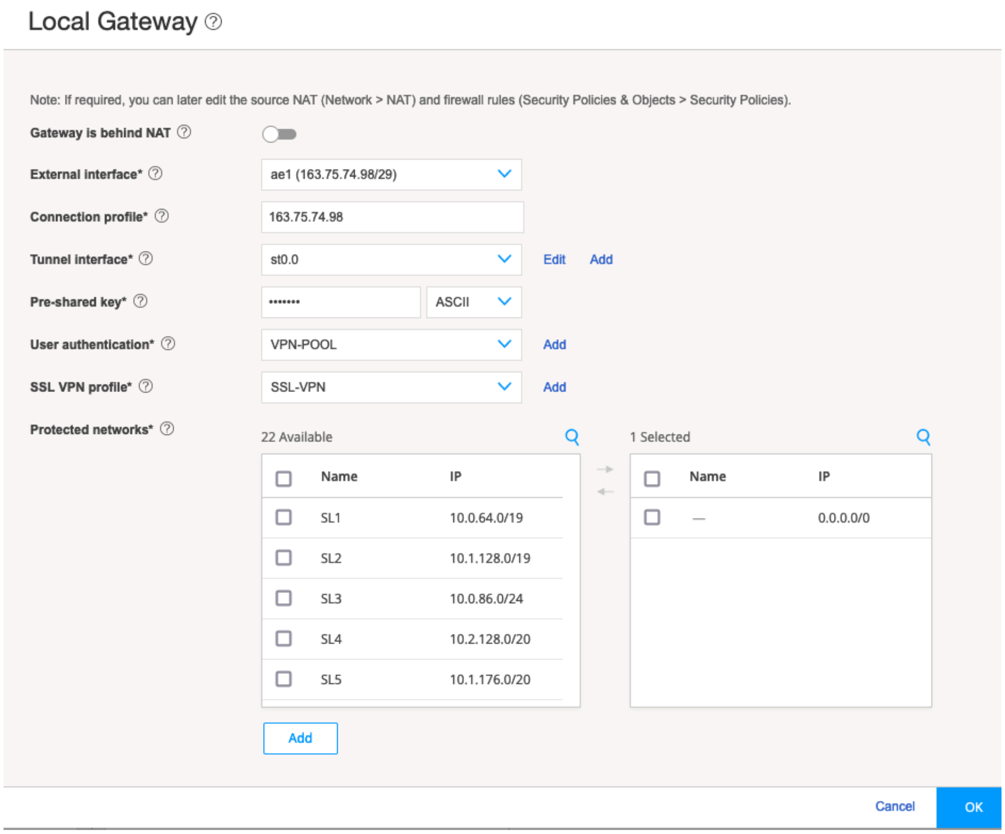
- Enter the name for the Remote Access Connection (this is, the name that will be displayed on the End Users Realm Name in Juniper Secure Connect application and a description.
- The routing mode is set to **Traffic Selector (Auto Route Insertion)** by default.
- Select the authentication method. For this example, let's select **Pre-shared Key** from the drop-down list.
- Select **Yes** to create the firewall policy automatically using the **Auto-create Firewall Policy** option.
- Click **Remote User** icon to configure the Juniper Secure Connect application settings.



Remote User

Connection mode	Manual
SSL VPN	☑
Biometric authentication	☐
Dead peer detection	☑
DPD interval	60 seconds
DPD threshold	5
Save username	☐
Windows logon	☐
Application bypass	☐
Compliance	None

- Click **OK** after reviewing all default options. For more details of the Remote User settings window click here.
- Click **Local Gateway** to configure the Local Gateway settings.



Local Gateway

Note: If required, you can later edit the source NAT (Network > NAT) and firewall rules (Security Policies & Objects > Security Policies).

Gateway is behind NAT	☐
External interface*	ae1 (163.75.74.98/29)
Connection profile*	163.75.74.98
Tunnel interface*	st0.0
Pre-shared key*	••••••• ASCII
User authentication*	VPN-POOL
SSL VPN profile*	SSL-VPN

Protected networks*

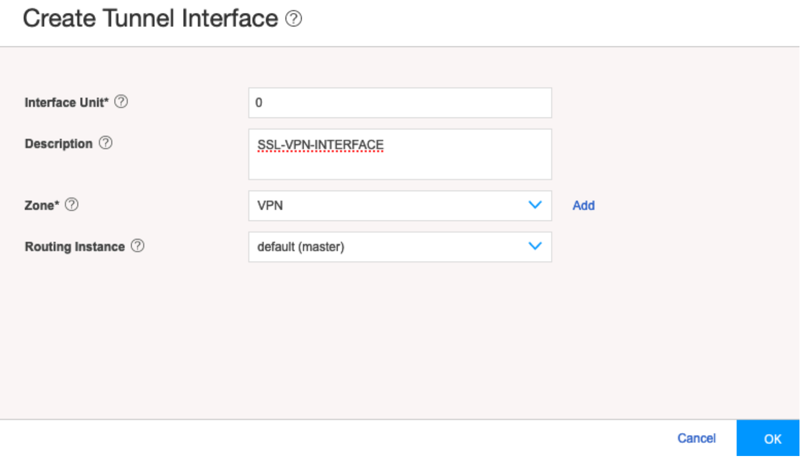
22 Available

□	Name	IP
□	SL1	10.0.64.0/19
□	SL2	10.1.128.0/19
□	SL3	10.0.86.0/24
□	SL4	10.2.128.0/20
□	SL5	10.1.176.0/20

1 Selected

□	Name	IP
□	—	0.0.0.0/0

- If you enable **Gateway is behind NAT**, a text box appears. In the text box, enter the NAT IP address. We support only IPv4 addresses. NAT address is the external address.
- Enter an IKE ID in **user@hostname.com** format.
- In the **External Interface** field, select the IP address for the clients to connect. You must enter this same IP address the Gateway Address field in the Juniper Secure Connect Client application.
- If you enable **Gateway is behind NAT**, then the NAT IP address becomes the gateway address.
- From the **Tunnel Interface** drop-down list, select an interface to bind it to the route-based VPN. Alternatively click **Add**. If you click **Add**, the **Create Tunnel Interface** page appears.



Create Tunnel Interface

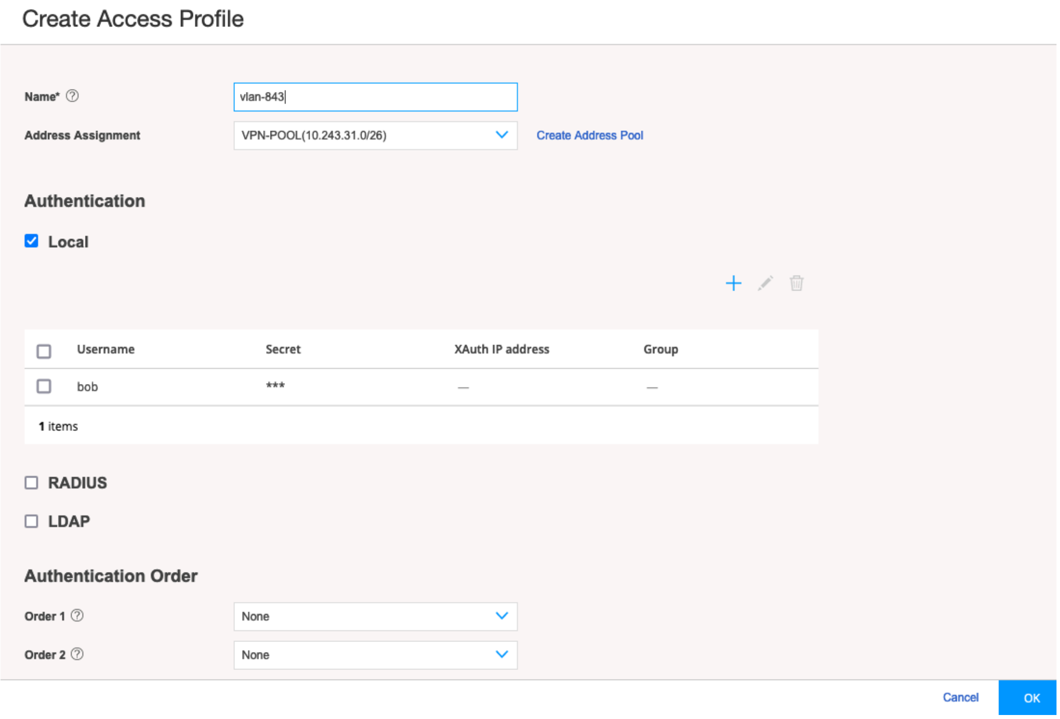
Interface Unit*: 0

Description: SSL-VPN-INTERFACE

Zone*: VPN

Routing Instance: default (master)

- The next available st0 logical interface number is displayed in the Interface Unit field and you can enter a description for this interface. Select the zone to add this tunnel interface to. If **Auto-create Firewall Policy** (in Create Remote Access page) is set to **Yes**, the firewall policy uses this zone. Click **OK**.
- Enter the preshared key in ASCII format. We do not support hexadecimal format for remote-access VPN.
- From the User Authentication drop-down list, select an existing access profile or click Add to create a new access profile. If you click **Add**, the Create Access Profile page appears.



Create Access Profile

Name* ⓘ vlan-843

Address Assignment VPN-POOL(10.243.31.0/26)

Authentication

☑ **Local**

	Username	Secret	XAuth IP address	Group
□	bob	***	—	—

1 items

□ **RADIUS**

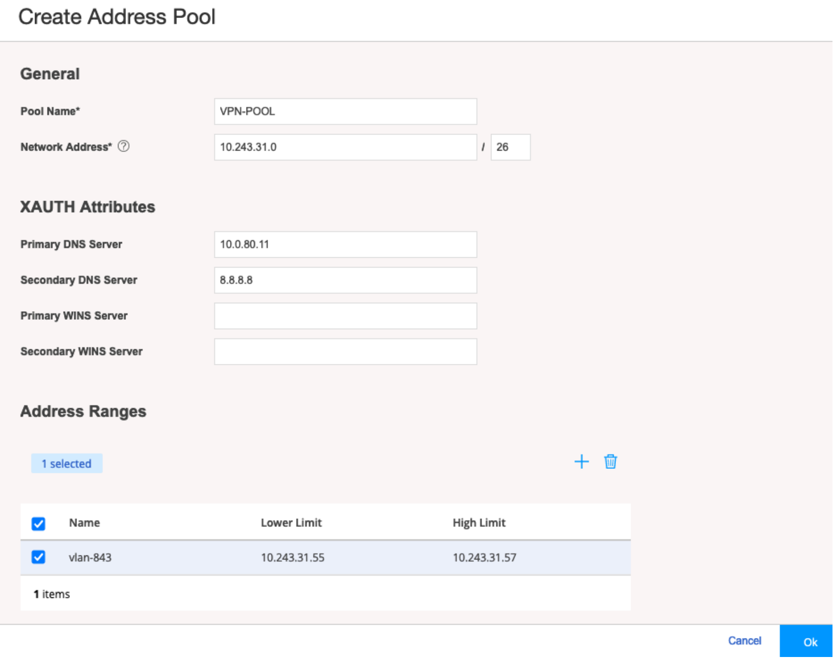
□ **LDAP**

Authentication Order

Order 1 ⓘ None

Order 2 ⓘ None

- Enter the access profile name. From the **Address Assignment** drop-down list, select an address pool or click **Create Address Pool**. If you click **Create Address Pool**, the Create Address Pool page appears.



Create Address Pool

General

Pool Name* VPN-POOL

Network Address* ⓘ 10.243.31.0 / 26

XAUTH Attributes

Primary DNS Server 10.0.80.11

Secondary DNS Server 8.8.8.8

Primary WINS Server

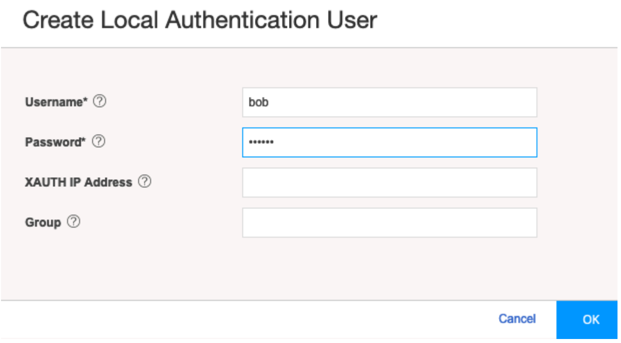
Secondary WINS Server

Address Ranges

	Name	Lower Limit	High Limit
☑	vlan-843	10.243.31.55	10.243.31.57

1 items

- Enter the details for the local IP pool that is in the VPN policy for the clients. Enter a name for the IP address pool.
- Enter the network address that you use for the address assignment.
- Enter your DNS server address. Enter WINS server details, if required. Now click the add icon (+) to create the address range to assign IP addresses to the clients.
- Enter the name, and the lower and higher limits. After entering the details, click **OK**.
- Select the Local check box to create local authentication user, where all the authentication details are stored on the SRX Series Firewalls. If you click the add icon (+), the Create Local Authentication User window appears.



Create Local Authentication User

Username* bob

Password* ••••••

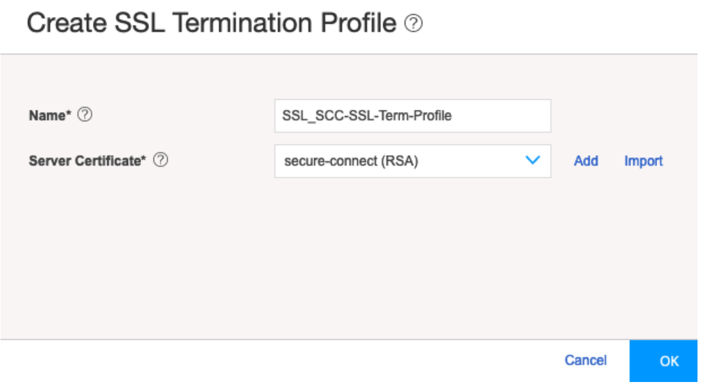
XAUTH IP Address

Group

- Enter a username and password, and then click **OK**. Click **OK** again to complete the access profile configuration.

- From the **SSL VPN Profile** drop-down list, select an existing profile or click **Add** to create a new SSL VPN profile. If you click **Add**, the **Add SSL VPN Profile** page appears.

- On the **Add SSL VPN Profile** page, you can configure the SSL VPN profile. Enter the SSL VPN profile name in the **Name** field, and enable logging using the toggle, if required. In the **SSL Termination Profile** field, select the SSL termination profile from the drop-down list. SSL termination is a process where the SRX Series Firewalls acts as an SSL proxy server and terminates the SSL session from the client. If you want to create a new SSL termination profile, click **Add**. The **Create SSL Termination Profile** page appears.


Create SSL Termination Profile

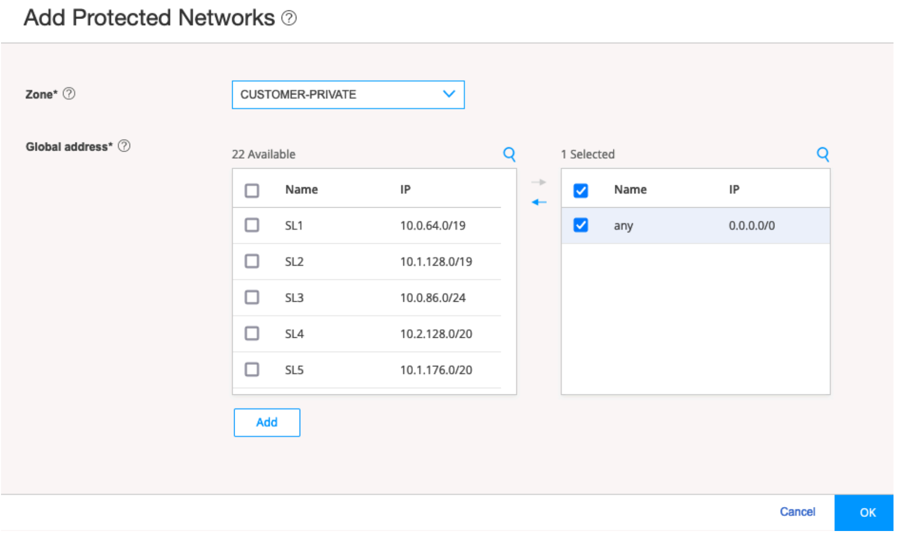
Name*: SSL_SCC-SSL-Term-Profile

Server Certificate*: secure-connect (RSA)

- Enter the name for the SSL termination profile and select the server certificate that you use for the SSL termination on the SRX Series Firewalls. Click **Add** to add a new server certificate or click **Import** to import the server certificate. The server certificate is a local certificate identifier. Server certificates are used to authenticate the identity of a server. Click **OK**.

The **Source NAT Traffic** option is enabled by default. When **Source NAT Traffic** is enabled, all traffic from the Juniper Secure Connect application is NATed to the selected interface by default. Click the toggle button to disable the **Source NAT Traffic** option. If the option is disabled, you must ensure that you have a route from your network pointing to the SRX Series Firewalls for handling the return traffic correctly.

- Under **Protected Networks**, click add icon (+) to select the networks that the Juniper Secure Connect application can connect to.



Add Protected Networks ⓘ

Zone* ⓘ CUSTOMER-PRIVATE

Global address* ⓘ

22 Available

☐	Name	IP
☐	SL1	10.0.64.0/19
☐	SL2	10.1.128.0/19
☐	SL3	10.0.86.0/24
☐	SL4	10.2.128.0/20
☐	SL5	10.1.176.0/20

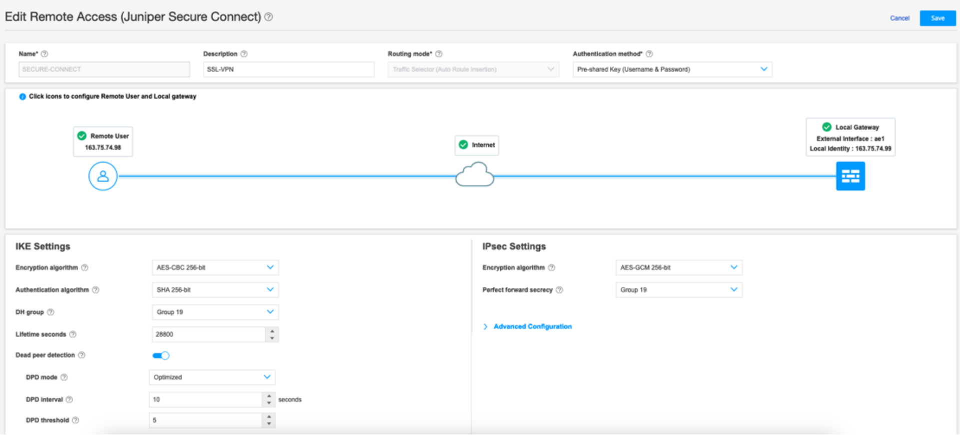
1 Selected

☑	Name	IP
☑	any	0.0.0.0/0

By default, any network 0.0.0.0/0 is allowed. If you configure a specific network, split tunneling for Juniper Secure Connect application is enabled. If you retain the default value, you can restrict access to your defined networks by adjusting the firewall policy from the client network.

- Click **OK**, and the selected networks are now in the list of protected networks. Click **OK** to complete the local gateway configuration.

IKE Settings and **IPsec Settings** are advanced options. J-Web is already configured with default values for the IKE and IPsec parameters. It is not mandatory to configure these settings.



Edit Remote Access (Juniper Secure Connect) ⓘ

Name* ⓘ	Description ⓘ	Routing mode* ⓘ	Authentication method* ⓘ
SECURE-CONNECT	SSL-VPN	Traffic Selector (Auto Route Insertion)	Pre-shared Key (Username & Password)

Click icons to configure Remote User and Local gateway

Remote User 163.75.74.98

Internet

Local Gateway
External Interface : ae1
Local Identity : 163.75.74.99

IKE Settings

Encryption algorithm ⓘ	AES-CBC 256-bit
Authentication algorithm ⓘ	SHA 256-bit
DH group ⓘ	Group 19
Lifetime seconds ⓘ	28800
Dead peer detection ⓘ	On
DPD mode ⓘ	Optimized
DPD interval ⓘ	10 seconds
DPD threshold ⓘ	5

IPsec Settings

Encryption algorithm ⓘ	AES-GCM 256-bit
Perfect forward secrecy ⓘ	Group 19

- Click **Save** to complete the Juniper Secure Connect VPN configuration and associated policy if you have selected the auto policy creation option.
- Click the highlighted **Commit** button (at the top right of the page next to Feedback Button) to commit the configuration.

You have successfully completed the remote access configuration.

Download and install Juniper Secure Connect application on the client machine. Launch Juniper Secure Connect and connect to the gateway address of the vSRX. See Juniper Secure Connect User Guide for more details.

Preparing the vSRX for Juniper Secure Connect Configuration using CLI

This section is intended to guide users on configuring Juniper Secure Connect on the vSRX in the IBM Cloud Classic Infrastructure using the Command Line Interface (CLI)

Listed below is the step-by-step procedure on how to prepare the vSRX, and helpful links that will answer the most common questions when configuring Juniper Secure Connect.

NOTE**: All vSRX versions **23.2R2-S1** and under have been provisioned with J-Web access disabled due to security vulnerabilities explained in detail under the following article **JSA72300

*Starting in **23.4R1-S2** the above JSA has been fixed and the vSRX will not face vulnerabilities while enabling web access to proceed with setting up Secure Connect as it is required for remote session connection to get established.*

Before you proceed with enabling web-management access to the vSRX device make sure you are aware of your code version and the vulnerabilities mentioned above.

Using the command line prompt connected utilizing the root user via SHH or Telnet, execute the following command enable web-management:

```
root@vSRX:~ # cli
root@vSRX > edit
Entering configuration mode
The configuration has been changed but not committed

[edit]
root@vSRX# activate system services web-management

[edit]
root@vSRX# commit and-quit
commit complete
Exiting configuration mode
```

1. Check Secure Connect License Using CLI
2. Enable Port Traffic for IKE And ESP Protocols Using CLI
3. Generate a Device Certificate Using CLI
4. Enable Device Certificate for Web Management Access Using CLI
5. Configure Dedicated HTTPS Access Using CLI
6. Configure Juniper Secure Connect With Local Authentication Using CLI

CHECK SECURE CONNECT LICENSES USING CLI

This guide was created using a vSRX with version code **23.2R2.**

Using the command line prompt connected utilizing the root user via SHH or Telnet, execute the following command to check the number of licenses installed for (**`remote-access-juniper-std`**) in your system.

```
root@vSRX:~ # cli
root@vSRX > show system license usage
                                 Licensed     Licensed    Licensed

                                  Feature      Feature     Feature

  Feature name                       used    installed      needed    Expiry

  Virtual Appliance                     1            1           0    2025-10-01 00:00:00 UTC

  remote-access-ipsec-vpn-client        0            2           0    permanent

  remote-access-juniper-std             0          502           0    2025-11-01 00:00:00 UTC

  VCPU Scale                            6            6           0    2025-10-01 00:00:00 UTC
```

***Note**: All vSRX firewalls will come with two built-in remote-access concurrent connections.*

If you need to order additional remote access VPN user licenses for the Juniper vSRX you may purchase either as part of your IBM Cloud Gateway order or by adding to an existing IBM Cloud Juniper Gateway. The licenses support 50 users per license, and you can order up to 10 licenses. They will be automatically added to the existing vSRX instance when the purchase is complete.

To order your new licenses from your IBM Cloud Portal, visit the following link for more details.

https://cloud.ibm.com/docs/vsrx?topic=vsrx-getting-started#choosing-license

To check your existing purchased licenses, visit the following link for more details.

https://cloud.ibm.com/docs/vsrx?topic=vsrx-vsrx-licenses

ENABLE PORT TRAFFIC FOR IKE AND ESP PROTOCOLS USING CLI

After configuring the following firewall filers, the specified ports will be allowed to communicate to the external interface of the vSRX, in our case will be the remote users connecting over SSL-VPN.

```
root@vSRX:~ # cli
root@vSRX > edit
Entering configuration mode
The configuration has been changed but not committed

[edit]
root@vSRX# load set terminal
[Type ^D at a new line to end input]

set firewall filter PROTECT-IN term IKE-500 from protocol udp
set firewall filter PROTECT-IN term IKE-500 from port 500
set firewall filter PROTECT-IN term IKE-500 then accept
set firewall filter PROTECT-IN term IKE-4500 from protocol udp
set firewall filter PROTECT-IN term IKE-4500 from port 4500
set firewall filter PROTECT-IN term IKE-4500 then accept
set firewall filter PROTECT-IN term ESP from protocol esp
set firewall filter PROTECT-IN term ESP then log
set firewall filter PROTECT-IN term ESP then accept

load complete

[edit]
root@vSRX# commit and-quit
commit complete
Exiting configuration mode
```

GENERATE A DEVICE CERTIFICATE USING CLI

Generating a self-signed certificate for Secure connect over HTTPS for users who will be establishing a remote connection to the vSRX.

*For this example, we will be calling our certificate ID "**test**", but network admins may set their preferred name for this certificate.*

```
root@vSRX> request security pki generate-key-pair size 2048 certificate-id test
Generated key pair test, key size 2048 bits
root@vSRX> request security pki local-certificate generate-self-signed certificate-id test
subject SN=7a5f9dbe944b domain-name vsrxonibm.net ip-address 163.75.74.98 email
admin@vsrxonibm.net
Self-signed certificate generated and loaded successfully
```

Preview Certificate

```
root@vSRX> show security pki local-certificate certificate-id test detail
LSYS: root-logical-system
Certificate identifier: test
  Certificate version: 3

  Serial number:
    hexadecimal: 0x29e0a315e2850557fc2ec1f9eef8062b
    decimal: 55664730090154584788180668314302285355
  Issuer:
    Serial number: 7a5f9dbe944b
  Subject:
    Serial number: 7a5f9dbe944b
  Subject string:
    serialNumber=7a5f9dbe944b
  Alternate subject: vsrxonibm.net, "admin@vsrxonibm.net", 163.75.74.98, ipv6 empty
  Cert-Chain: Issuer CA Certificate Missing
  Validity:
    Not before: 05- 8-2024 20:24 UTC
    Not after: 05- 7-2029 20:24 UTC
  Public key algorithm: rsaEncryption(2048 bits)
    30:82:01:0a:02:82:01:01:00:c4:f3:21:7c:86:2e:74:69:9a:be:6b
    47:4d:77:7d:17:f2:3c:ed:5c:c1:b6:10:79:5a:31:42:e9:e7:48:46
    0e:3b:cd:1b:30:46:67:55:2b:d2:aa:3c:f9:f5:2f:59:0c:e3:e9:9d
    72:73:68:56:d1:b1:5d:fd:ed:ad:91:05:c5:00:47:3e:b3:a8:04:e1
    b2:0d:28:df:a8:d9:85:0b:7f:02:4b:36:fb:22:5e:9a:06:4a:e9:a6
    22:96:0c:48:03:bf:91:76:7c:78:25:42:46:0e:fb:3a:5b:d5:05:5f
    0c:25:5c:4b:69:2e:c1:6c:62:de:d3:2a:4b:f5:30:3c:d2:76:00:3f
    1b:b5:1e:f1:12:67:57:0e:a0:a8:9f:0b:76:e1:2b:9c:3d:3d:25:33
    29:dd:c8:0d:b5:3d:90:7d:41:76:04:08:af:52:83:4a:b7:54:4c:67
    94:29:74:ea:1c:5f:67:03:0b:59:88:5f:e6:90:cd:6d:46:f6:bb:c3
    ab:33:96:80:67:bc:d2:76:8a:82:9b:91:83:84:24:38:ce:33:81:9a
    9d:53:92:2a:4b:96:bd:77:44:bf:13:01:b3:07:90:d8:10:55:ab:8d
    fd:42:e9:29:64:f8:6b:69:95:13:89:3e:b5:0b:25:6b:e3:15:da:a8
    51:f4:5c:1b:e1:02:03:01:00:01
  Signature algorithm: sha256WithRSAEncryption
  Fingerprint:
    58:6a:21:ba:c5:ad:46:79:db:9c:3f:19:f4:e9:57:7f:0a:85:3c:fe (sha1)
    ae:c0:1e:21:c8:e3:58:7a:3e:e2:c7:b1:8a:18:17:ff (md5)
```

```
eb:4e:89:1f:a5:fe:dc:0b:70:36:9b:6a:e3:ef:31:b5:17:93:8d:aa:1f:ad:c3:f7:d5:58:3a:c4:83:9d:9b:
10 (sha256)
  Auto-re-enrollment:
    Status: Disabled
    Next trigger time: Timer not started
```

ENABLE DEVICE CERTIFICATE FOR WEB MANAGEMENT ACCESS USING CLI

After creating a self-signed or loading a signed certificate, you must bind the certificate to the vSRX. To enable the new device certificate for web management, configure the following command:

```
root@vSRX:~ # cli
root@vSRX > edit
Entering configuration mode
The configuration has been changed but not committed

[edit]
root@vSRX# set system services web-management https pki-local-certificate test

[edit]
root@vSRX# commit and-quit
commit complete
Exiting configuration mode
```

When the certificate has been loaded to the vSRX, you can validate the certificate by viewing the certificate information in your browser bar. The steps involved in viewing the certificate information depend on your browser and browser version.

CONFIGURE DEDICATED HTTPS ACCESS USING CLI

Using the command line prompt connected utilizing the root user via SHH or Telnet, execute the following command enable a dedicated path.

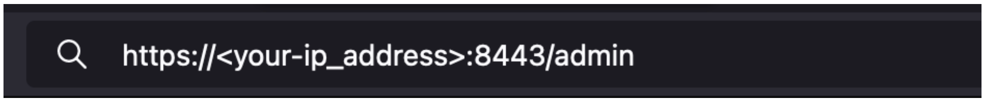
NOTE: *For this example, we will be defining our access as "***admin***", but network admins may set their preferred name for this path.*

```
root@vSRX:~ # cli
root@vSRX > edit
Entering configuration mode
The configuration has been changed but not committed

[edit]
root@vSRX# set system services web-management management-url admin


[edit]
root@vSRX# commit and-quit
commit complete
Exiting configuration mode
```

Now your J-Web portal can be accessed by appending the word `admin` after the port number


https://<your-ip_address>:8443/admin

CONFIGURE JUNIPER SECURE CONNECT WITH LOCAL AUTHENTICATION USING CLI

Using the command line prompt connected utilizing the root user via SHH or Telnet, copy the following set commands and paste them in the terminal after executing the `load set terminal` command and when complete, press **Ctrl + D** keys to append the configuration.

Then followed by `commit and-quit` to load the changes to an active state.

NOTE: For this example, we will be defining a local authentication for a remote username named ”bob” with password “bob123”, IPv4 pool address” 10.243.31.55- 57. Network admins should replace these parameters to match their network.

```
root@vSRX:~ # cli
root@vSRX > edit
Entering configuration mode
The configuration has been changed but not committed

[edit]
root@vSRX# load set terminal
[Type ^D at a new line to end input]

set security ike proposal SECURE-CONNECT description SSL-VPN
set security ike proposal SECURE-CONNECT authentication-method pre-shared-keys
set security ike proposal SECURE-CONNECT dh-group group19
set security ike proposal SECURE-CONNECT authentication-algorithm sha-256
set security ike proposal SECURE-CONNECT encryption-algorithm aes-256-cbc
set security ike proposal SECURE-CONNECT lifetime-seconds 28800
set security ike policy SECURE-CONNECT mode aggressive
set security ike policy SECURE-CONNECT description SSL-VPN
set security ike policy SECURE-CONNECT proposals SECURE-CONNECT
set security ike policy SECURE-CONNECT pre-shared-key ascii-text
"$9$pq47OIhevLVwgSrwgoJHkp0BISrKM87dbAt"
set security ike gateway SECURE-CONNECT ike-policy SECURE-CONNECT
set security ike gateway SECURE-CONNECT dynamic user-at-hostname "cicd-gw75-
vSRX@163.75.74.98.SECURE-CONNECT"
set security ike gateway SECURE-CONNECT dynamic ike-user-type shared-ike-id
set security ike gateway SECURE-CONNECT dead-peer-detection optimized
set security ike gateway SECURE-CONNECT dead-peer-detection interval 10
set security ike gateway SECURE-CONNECT dead-peer-detection threshold 5
set security ike gateway SECURE-CONNECT external-interface ae1
set security ike gateway SECURE-CONNECT local-address 163.75.74.98
set security ike gateway SECURE-CONNECT aaa access-profile VPN-POOL
set security ike gateway SECURE-CONNECT version v1-only
set security ike gateway SECURE-CONNECT tcp-encap-profile SSL-VPN
set security ipsec proposal SECURE-CONNECT description SSL-VPN
set security ipsec proposal SECURE-CONNECT protocol esp
set security ipsec proposal SECURE-CONNECT encryption-algorithm aes-256-gcm
set security ipsec proposal SECURE-CONNECT lifetime-seconds 3600
set security ipsec policy SECURE-CONNECT description SSL-VPN
set security ipsec policy SECURE-CONNECT perfect-forward-secrecy keys group19
set security ipsec policy SECURE-CONNECT proposals SECURE-CONNECT
set security ipsec vpn SECURE-CONNECT bind-interface st0.0
set security ipsec vpn SECURE-CONNECT df-bit clear
set security ipsec vpn SECURE-CONNECT copy-outer-dscp
set security ipsec vpn SECURE-CONNECT ike gateway SECURE-CONNECT
set security ipsec vpn SECURE-CONNECT ike ipsec-policy SECURE-CONNECT
set security ipsec vpn SECURE-CONNECT traffic-selector ts-1 local-ip 0.0.0.0/0
set security ipsec vpn SECURE-CONNECT traffic-selector ts-1 remote-ip 0.0.0.0/0
set security remote-access profile 163.75.74.98/SECURE-CONNECT description SSL-VPN
set security remote-access profile 163.75.74.98/SECURE-CONNECT ipsec-vpn SECURE-CONNECT
set security remote-access profile 163.75.74.98/SECURE-CONNECT access-profile VPN-POOL
set security remote-access profile 163.75.74.98/SECURE-CONNECT client-config SECURE-CONNECT
set security remote-access client-config SECURE-CONNECT connection-mode manual
set security remote-access client-config SECURE-CONNECT dead-peer-detection interval 60
set security remote-access client-config SECURE-CONNECT dead-peer-detection threshold 5
set security tcp-encap profile SSL-VPN ssl-profile SSL_SCC-SSL-Term-Profile
set access address-assignment pool SSL-POOL family inet network 10.243.31.0/26
set access address-assignment pool SSL-POOL family inet range vlan-pool low 10.243.31.55
set access address-assignment pool SSL-POOL family inet range vlan-pool high 10.243.31.57
set access address-assignment pool SSL-POOL family inet xauth-attributes primary-dns
10.0.80.11/32
set access address-assignment pool SSL-POOL family inet xauth-attributes secondary-dns
8.8.8.8/32
set access profile ACCESS-PROFILE-SC client bob firewall-user password
"$9$3bSf/9pKvL7NblegoGUHk"
set access profile ACCESS-PROFILE-SC address-assignment pool SSL-POOL
set access profile ACCESS-VPN client bob firewall-user password "$9$qPfzIRSleWB17-ws4o"
set access profile ACCESS-VPN address-assignment pool SSL-POOL
set access profile VPN-POOL client bob firewall-user password "$9$GQji.tpBREyCAvWx7Vb"
set access profile VPN-POOL address-assignment pool SSL-POOL
set access firewall-authentication web-authentication default-profile VPN-POOL
set security policies from-zone SL-PRIVATE to-zone VPN policy SECURE-CONNECT-1 match source-
address any
set security policies from-zone SL-PRIVATE to-zone VPN policy SECURE-CONNECT-1 match
destination-address any
set security policies from-zone SL-PRIVATE to-zone VPN policy SECURE-CONNECT-1 match
application any
set security policies from-zone SL-PRIVATE to-zone VPN policy SECURE-CONNECT-1 then permit
set security policies from-zone SL-PRIVATE to-zone VPN policy SECURE-CONNECT-1 then log
session-close
set security policies from-zone VPN to-zone SL-PRIVATE policy SECURE-CONNECT-2 match source-
address any
set security policies from-zone VPN to-zone SL-PRIVATE policy SECURE-CONNECT-2 match
destination-address any
set security policies from-zone VPN to-zone SL-PRIVATE policy SECURE-CONNECT-2 match
application any
set security policies from-zone VPN to-zone SL-PRIVATE policy SECURE-CONNECT-2 then permit
set security policies from-zone VPN to-zone SL-PRIVATE policy SECURE-CONNECT-2 then log
session-close
set security zones security-zone VPN interfaces st0.0 host-inbound-traffic system-services
all
set interfaces st0 unit 0 description SSL-VPN-INTERFACE
set interfaces st0 unit 0 family inet
set services ssl termination profile SSL_SCC-SSL-Term-Profile server-certificate test

load complete

[edit]
root@vSRX# commit and-quit
commit complete
Exiting configuration mode
```

Installing Juniper Secure Connect Client (MacOS)

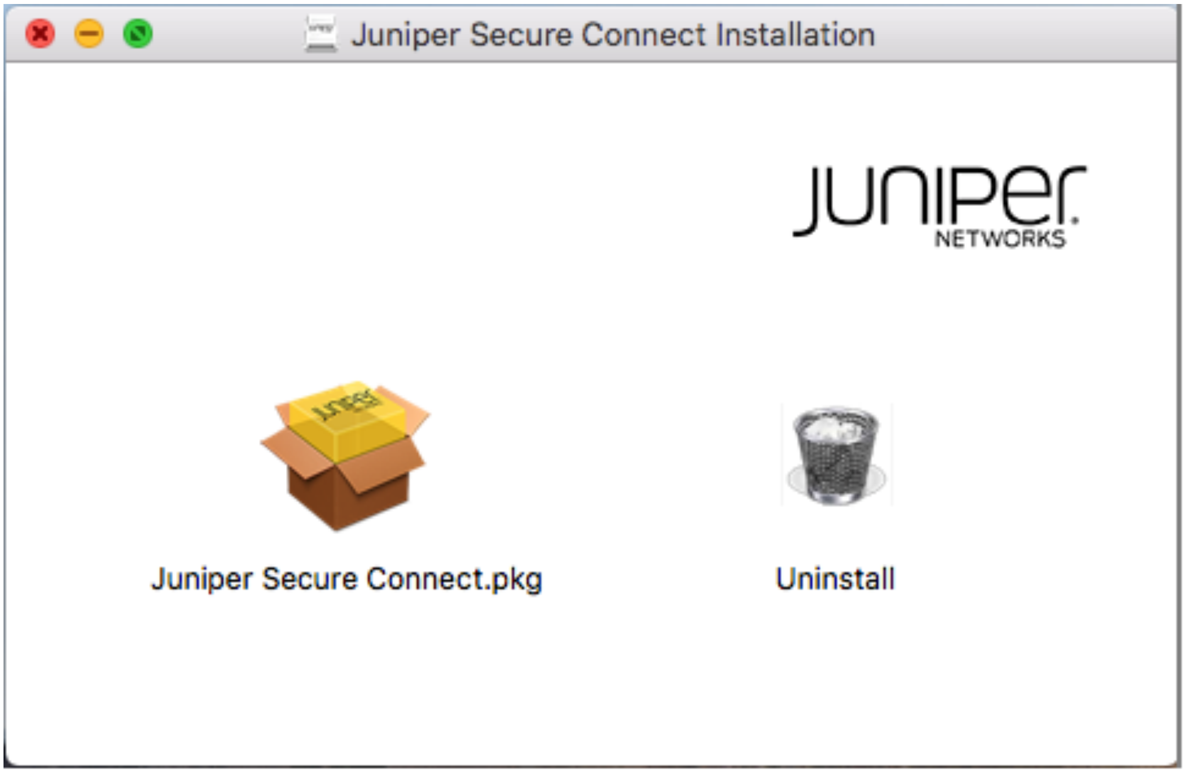
Following are the steps to install the Juniper Secure Connect on your macOS machine.

Download Juniper Secure Connect Client from juniper.net

https://support.juniper.net/support/downloads/?p=jsc-mac

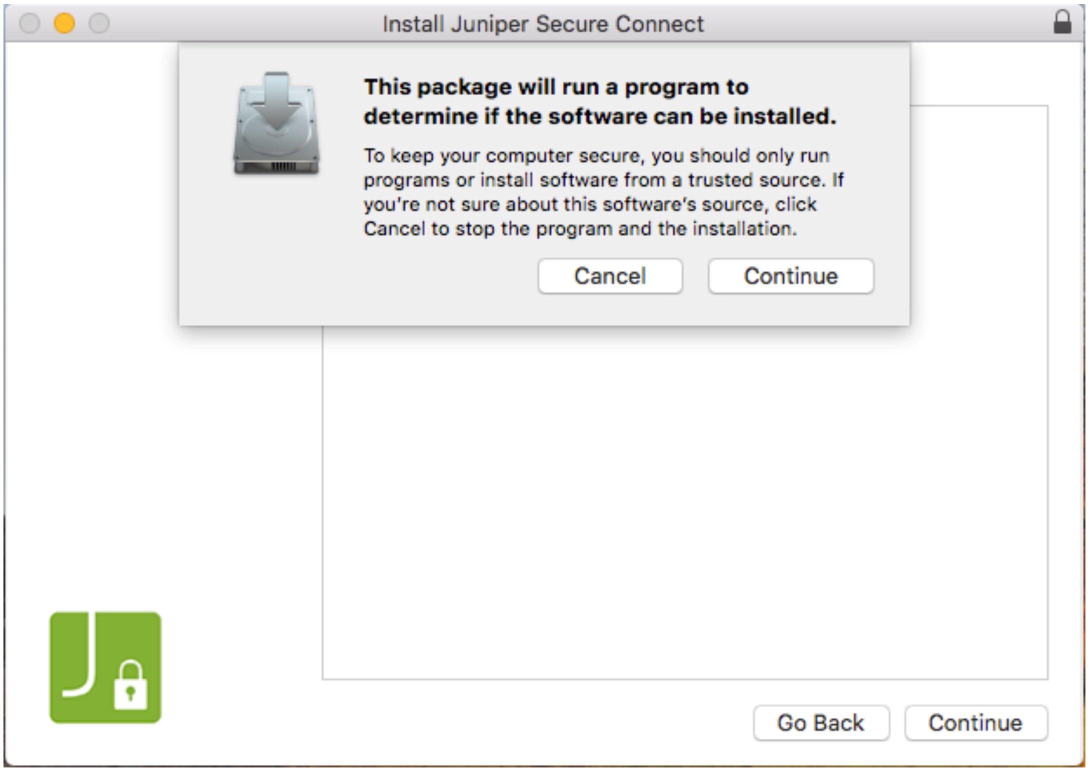
1. Run the Juniper Secure Connect installer (.dmg file). To start the installation, click on `Juniper Secure Connect.pkg`. See Figure 1.

Figure 1: Juniper Secure Connect Installer


Juniper Secure Connect Installation
JUNIPer NETWORKS
Juniper Secure Connect.pkg
Uninstall

2. A pop-up window appears as shown in Figure 2 with a message that a program will run to check whether Juniper Secure Connect application can be installed. Click **Continue** to run the program.

Figure 2: Trusted Resource Verification Pop-up Window

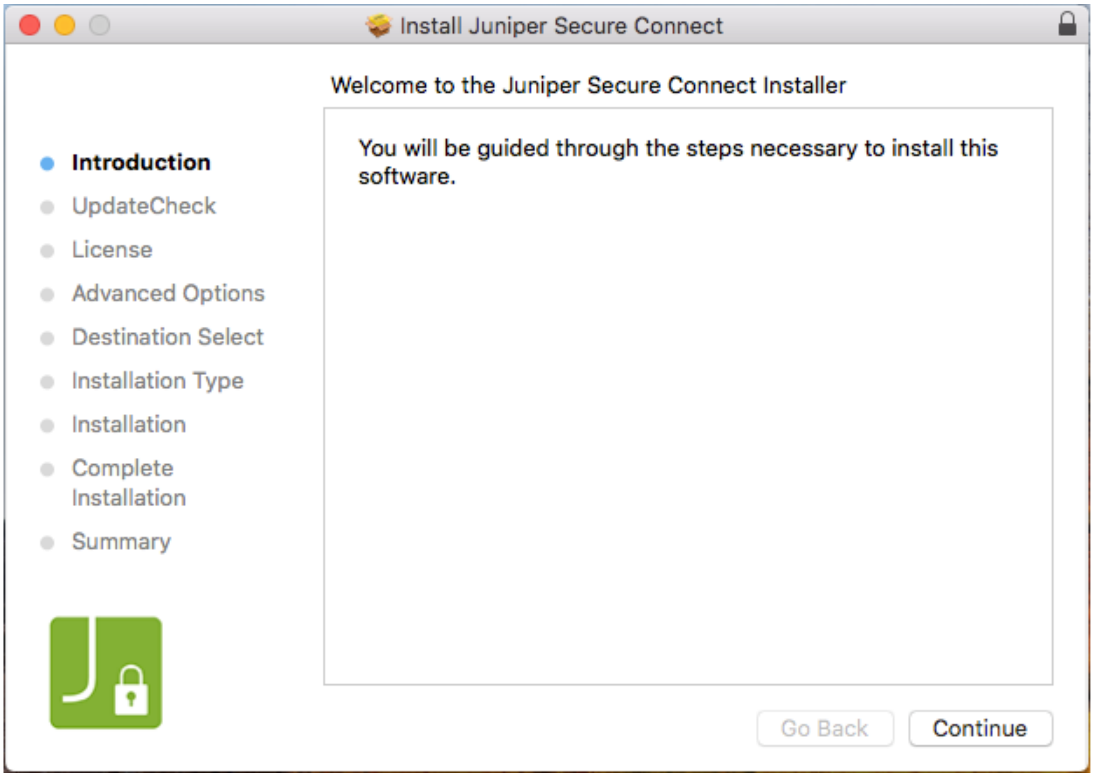


This package will run a program to determine if the software can be installed.

To keep your computer secure, you should only run programs or install software from a trusted source. If you're not sure about this software's source, click Cancel to stop the program and the installation.

3. Juniper Secure Connect welcome page appears. See Figure 3. Click **Continue**.

Figure 3: Installer Welcome Window

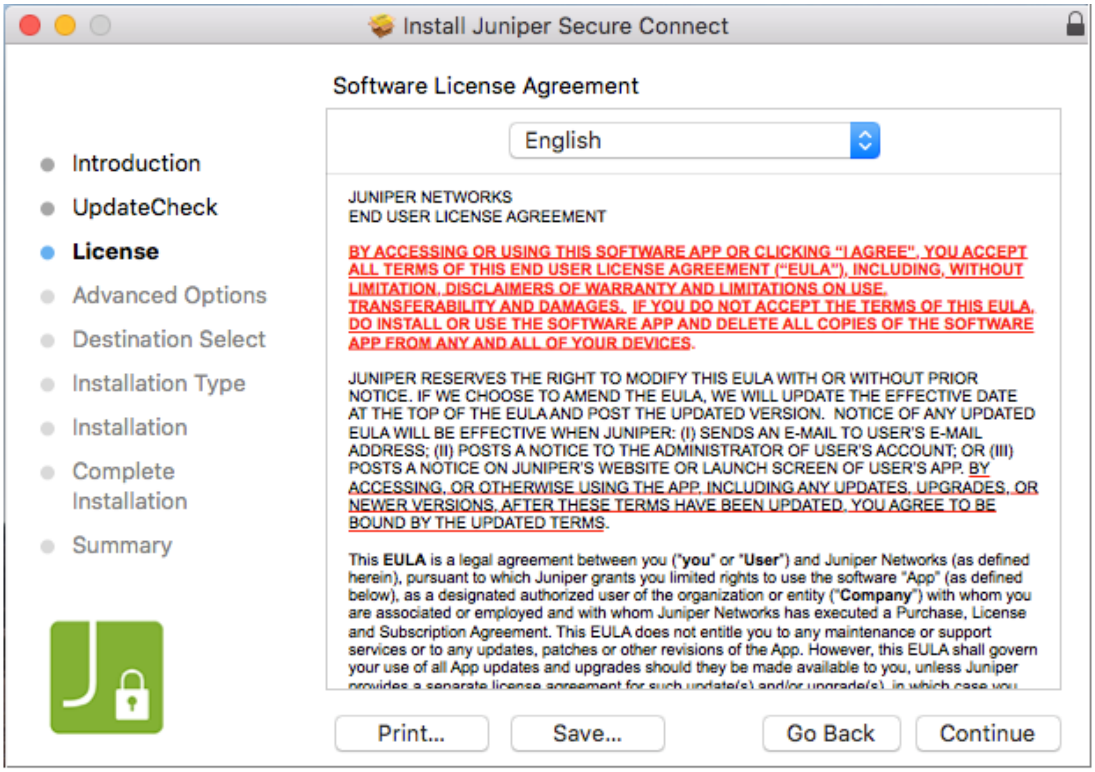


Welcome to the Juniper Secure Connect Installer

You will be guided through the steps necessary to install this software.

4. Juniper Secure Connect **Software License Agreement** page appears. See Figure 4.

Figure 4: License Agreement Window



JUNIPER NETWORKS
END USER LICENSE AGREEMENT

BY ACCESSING OR USING THIS SOFTWARE APP OR CLICKING "I AGREE", YOU ACCEPT ALL TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"), INCLUDING, WITHOUT LIMITATION, DISCLAIMERS OF WARRANTY AND LIMITATIONS ON USE, TRANSFERABILITY AND DAMAGES. IF YOU DO NOT ACCEPT THE TERMS OF THIS EULA, DO INSTALL OR USE THE SOFTWARE APP AND DELETE ALL COPIES OF THE SOFTWARE APP FROM ANY AND ALL OF YOUR DEVICES.

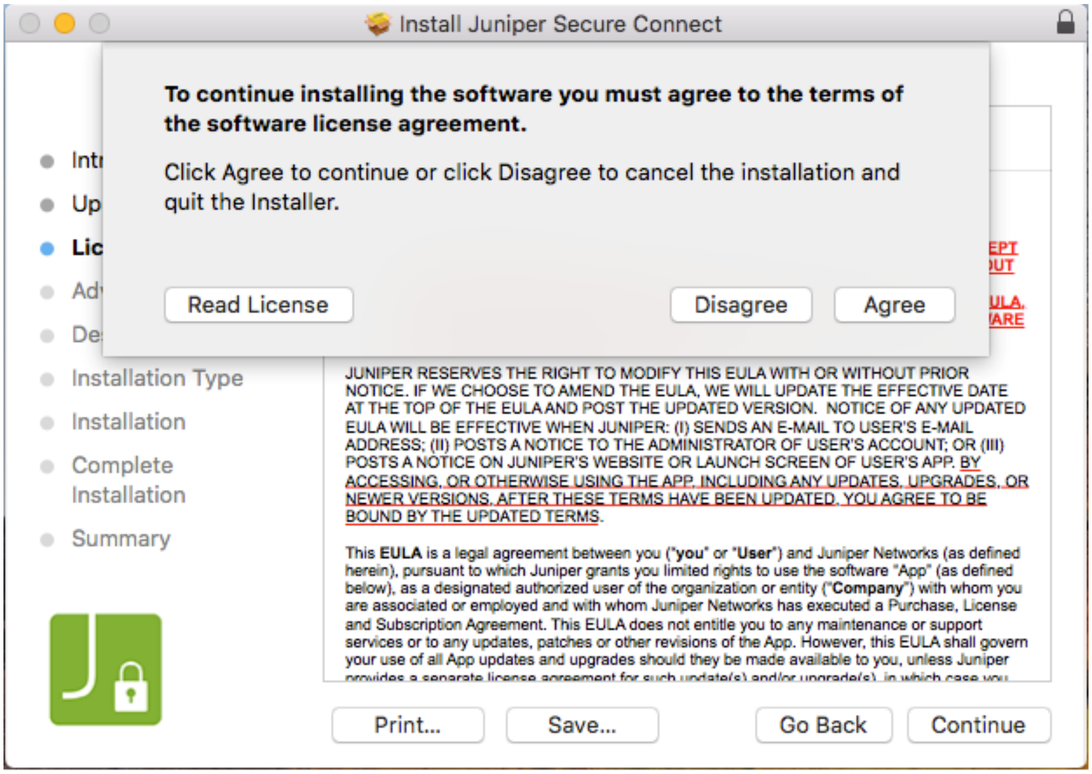
JUNIPER RESERVES THE RIGHT TO MODIFY THIS EULA WITH OR WITHOUT PRIOR NOTICE. IF WE CHOOSE TO AMEND THE EULA, WE WILL UPDATE THE EFFECTIVE DATE AT THE TOP OF THE EULA AND POST THE UPDATED VERSION. NOTICE OF ANY UPDATED EULA WILL BE EFFECTIVE WHEN JUNIPER: (I) SENDS AN E-MAIL TO USER'S E-MAIL ADDRESS; (II) POSTS A NOTICE TO THE ADMINISTRATOR OF USER'S ACCOUNT; OR (III) POSTS A NOTICE ON JUNIPER'S WEBSITE OR LAUNCH SCREEN OF USER'S APP. BY ACCESSING, OR OTHERWISE USING THE APP, INCLUDING ANY UPDATES, UPGRADES, OR NEWER VERSIONS, AFTER THESE TERMS HAVE BEEN UPDATED, YOU AGREE TO BE BOUND BY THE UPDATED TERMS.

This **EULA** is a legal agreement between you ("**you**" or "**User**") and Juniper Networks (as defined herein), pursuant to which Juniper grants you limited rights to use the software "App" (as defined below), as a designated authorized user of the organization or entity ("**Company**") with whom you are associated or employed and with whom Juniper Networks has executed a Purchase, License and Subscription Agreement. This EULA does not entitle you to any maintenance or support services or to any updates, patches or other revisions of the App. However, this EULA shall govern your use of all App updates and upgrades should they be made available to you, unless Juniper provides a separate license agreement for such update(s) and/or upgrade(s), in which case you

Read the license agreement carefully. If you accept the terms, then select **I accept the terms in the license agreement** check box to accept the license agreement.
Click **Continue**.

See Figure 5. You can also save or print the software license agreement. To continue the installation, you must agree to the terms of the software license agreement and click **Continue**.

Figure 5: Agree or Cancel License Agreement



To continue installing the software you must agree to the terms of the software license agreement.

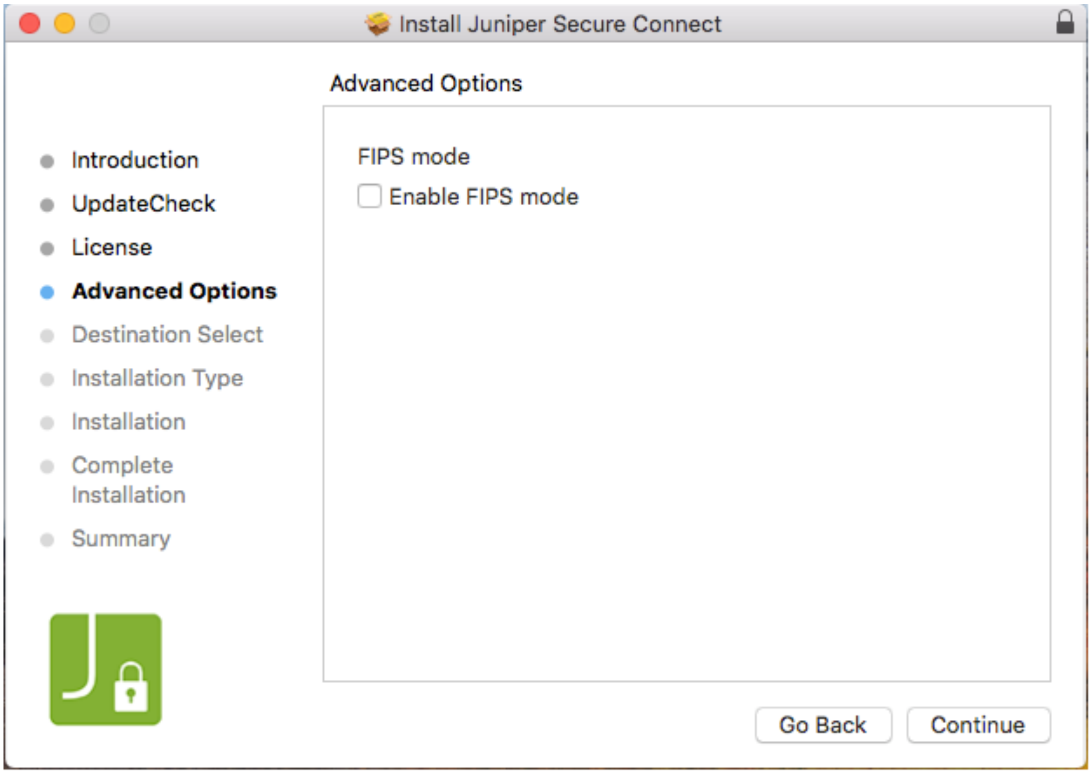
Click Agree to continue or click Disagree to cancel the installation and quit the Installer.

JUNIPER RESERVES THE RIGHT TO MODIFY THIS EULA WITH OR WITHOUT PRIOR NOTICE. IF WE CHOOSE TO AMEND THE EULA, WE WILL UPDATE THE EFFECTIVE DATE AT THE TOP OF THE EULA AND POST THE UPDATED VERSION. NOTICE OF ANY UPDATED EULA WILL BE EFFECTIVE WHEN JUNIPER: (I) SENDS AN E-MAIL TO USER'S E-MAIL ADDRESS; (II) POSTS A NOTICE TO THE ADMINISTRATOR OF USER'S ACCOUNT; OR (III) POSTS A NOTICE ON JUNIPER'S WEBSITE OR LAUNCH SCREEN OF USER'S APP. BY ACCESSING, OR OTHERWISE USING THE APP, INCLUDING ANY UPDATES, UPGRADES, OR NEWER VERSIONS, AFTER THESE TERMS HAVE BEEN UPDATED, YOU AGREE TO BE BOUND BY THE UPDATED TERMS.

This **EULA** is a legal agreement between you ("**you**" or "**User**") and Juniper Networks (as defined herein), pursuant to which Juniper grants you limited rights to use the software "App" (as defined below), as a designated authorized user of the organization or entity ("**Company**") with whom you are associated or employed and with whom Juniper Networks has executed a Purchase, License and Subscription Agreement. This EULA does not entitle you to any maintenance or support services or to any updates, patches or other revisions of the App. However, this EULA shall govern your use of all App updates and upgrades should they be made available to you, unless Juniper provides a separate license agreement for such update(s) and/or upgrade(s), in which case you

5. The **Advanced Options** page appears. See Figure 6. Click **Continue**.

Figure 6: Configure FIPS Mode Option



FIPS mode

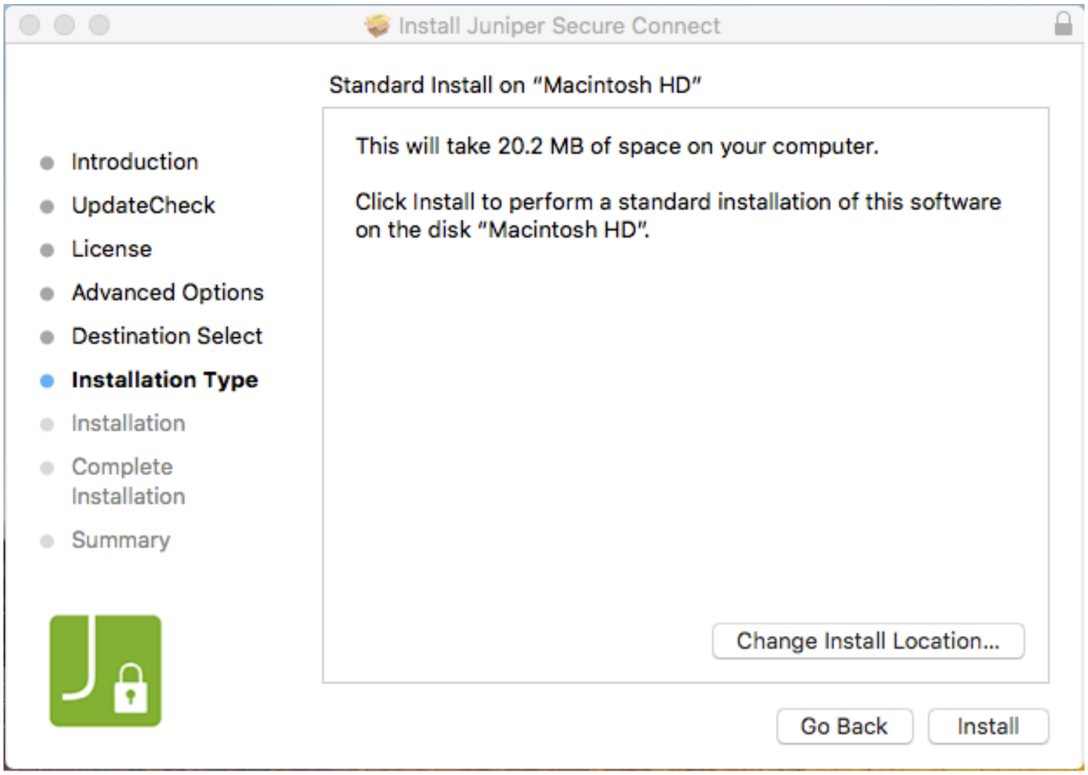
□ Enable FIPS mode

NOTE:

The vSRX Series Firewall and the Juniper Secure Connect application are independent FIPS compliant products. For remote access VPN solution on FIPS evaluated vSRX Series Firewall, see Juniper Secure Connect.

6. In the **Installation Type** page, you can change the installation location if you wish. Verify that you have enough space on your system. Click **Install** to begin the installation process. See Figure 7.

Figure 7: Start Juniper Secure Connect Installation



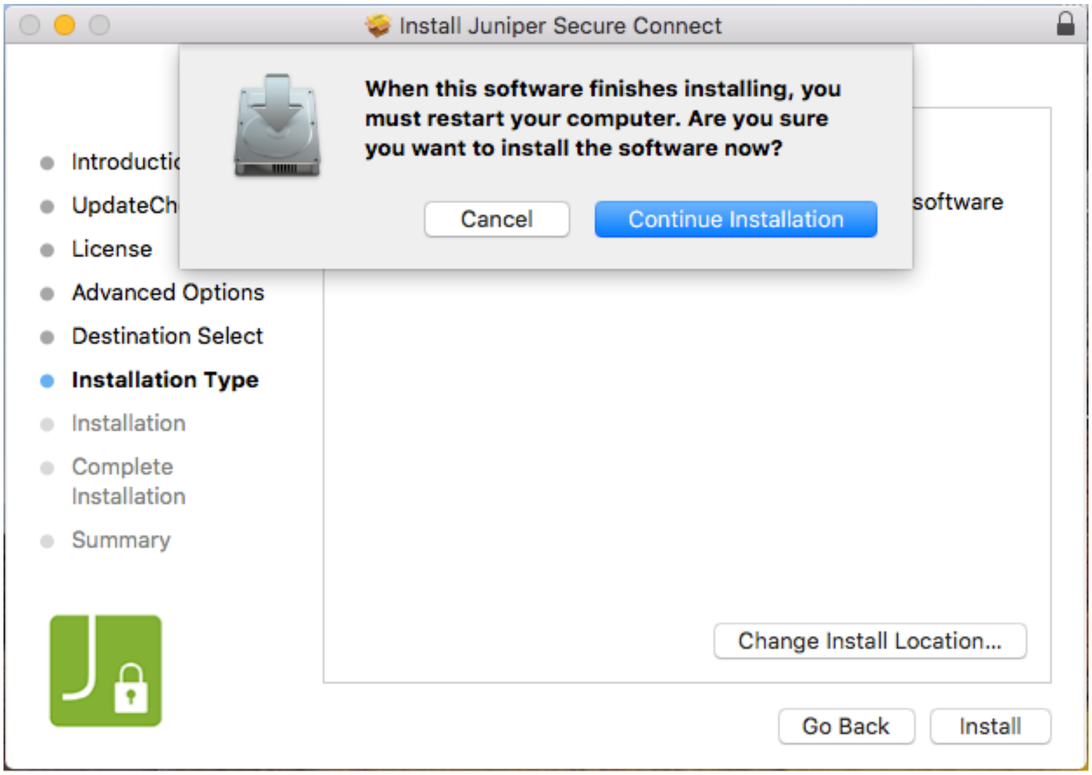
Standard Install on "Macintosh HD"

This will take 20.2 MB of space on your computer.

Click Install to perform a standard installation of this software on the disk "Macintosh HD".

A pop-up message as shown in Figure 8 is displayed to confirm restarting the computer when the installation is complete. Click **Continue Installation** to confirm restart.

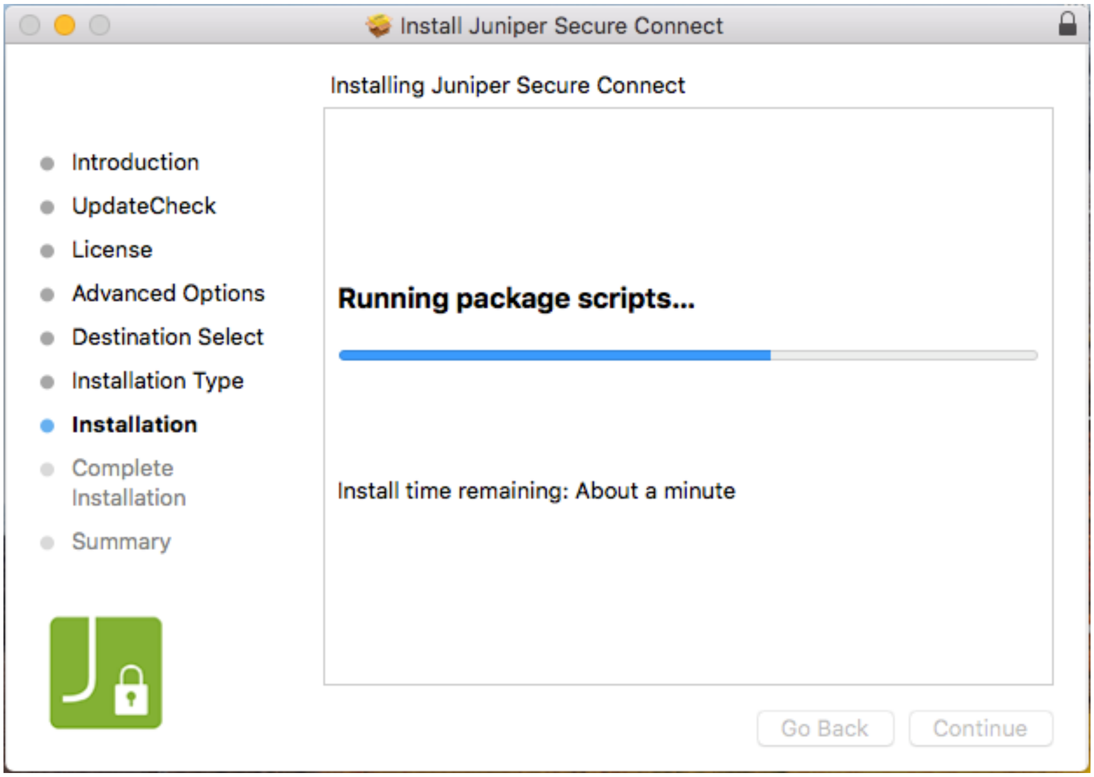
Figure 8: Confirm Restart after Installation



When this software finishes installing, you must restart your computer. Are you sure you want to install the software now?

7. Juniper Secure Connect installer runs the package scripts as shown in Figure 9.

Figure 9: Running Juniper Secure Connect Installation Package



Install Juniper Secure Connect

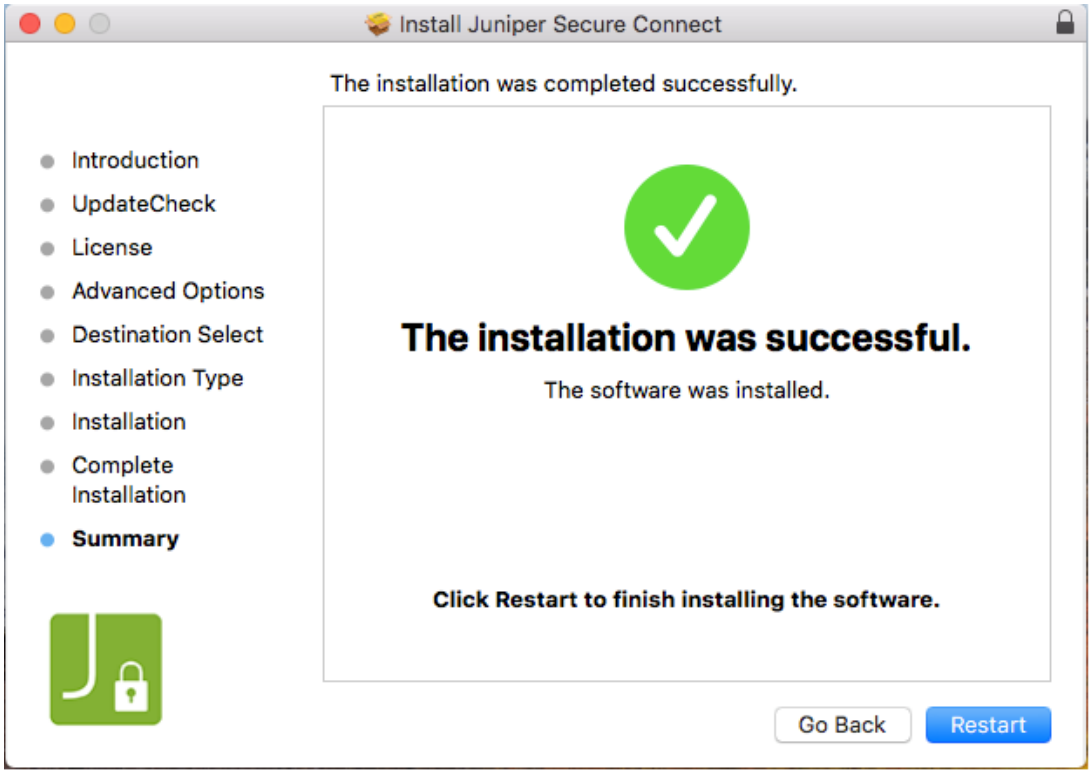
Installing Juniper Secure Connect

Running package scripts...

Install time remaining: About a minute

Figure 10 shows an example of the Juniper Secure Connect installation window when the installation is successfully completed.

Figure 10: Juniper Secure Connect Installation Completed


The installation was completed successfully.

The installation was successful.

The software was installed.

Click Restart to finish installing the software.

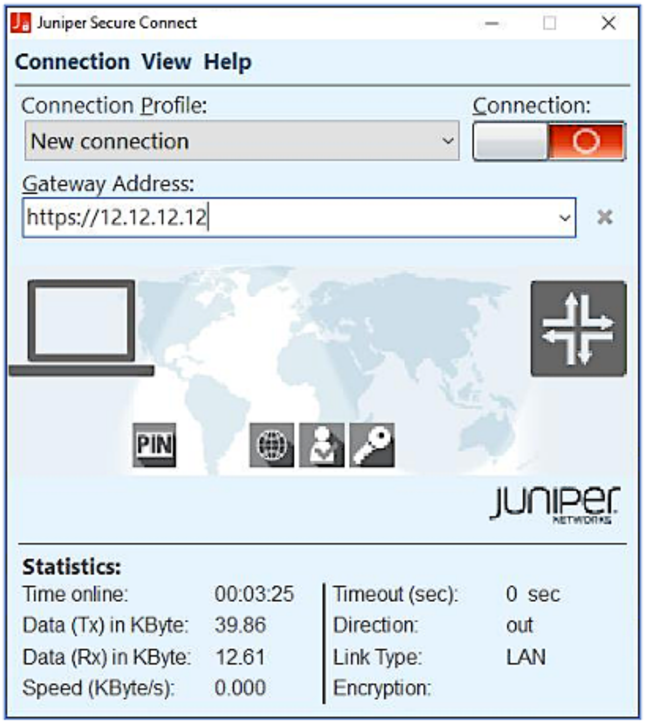
Congratulations! The Juniper Secure Connect application is successfully installed in your Mac.

Establishing a Connection from Juniper Secure Connect Client (MacOS)

8. To use the application, you must first restart your system.
9. You can now launch the Juniper Secure Connect and enter the **Gateway Address** URL to connect with the SRX Series Firewall. Figure 11 shows an example to enter the gateway address to the SRX Series Firewall.

   You can also enter a fully qualified domain name (FQDN) in the **Gateway Address** URL to connect with the SRX Series Firewall. For example: https://vpn.juniper.net. After entering the gateway address, click the connection toggle button to establish connection manually to the destination system. You can also select **Connection > Connect** from the menu bar to manually establish a VPN connection. When the connection is established successfully, the application window minimizes in the task bar.

   Figure 11: Launch Juniper Secure Connect



Connection Profile: New connection

Connection:

Gateway Address: https://12.12.12.12

Statistics:

Time online: 00:03:25
Data (Tx) in KByte: 39.86
Data (Rx) in KByte: 12.61
Speed (KByte/s): 0.000
Timeout (sec): 0 sec
Direction: out
Link Type: LAN
Encryption:

The following link provides a quick display of additional information about your remote access connection GUI Elements.

https://www.juniper.net/documentation/us/en/software/secure-connect/secure-connect-user-guide/topics/concept/explore-juniper-secure-connect-macos.html

Installing Juniper Secure Connect Client (Windows)

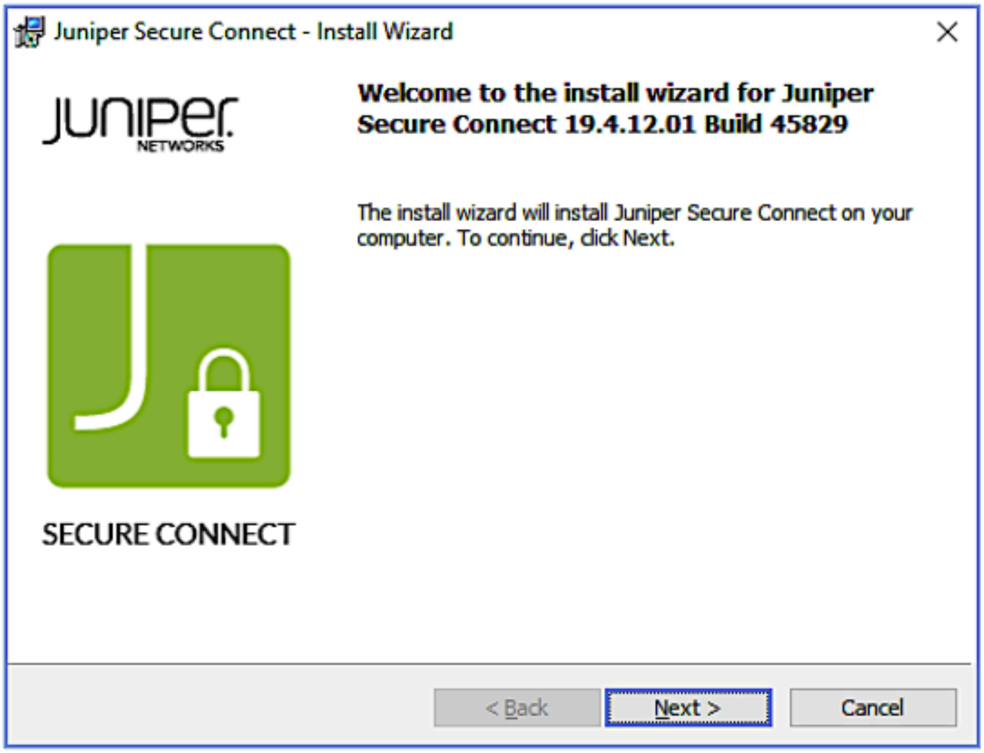
The following are the steps to install the Juniper Secure Connect on your Windows machine.

Download Juniper Secure Connect - Windows

https://support.juniper.net/support/downloads/?p=jsc-win

1. Run the Windows installer (.exe) for Juniper Secure Connect . See Figure 1. The version that you see on the figure is dependent on the Juniper Secure Connect application release number.

   Figure 1: Installer Welcome Window



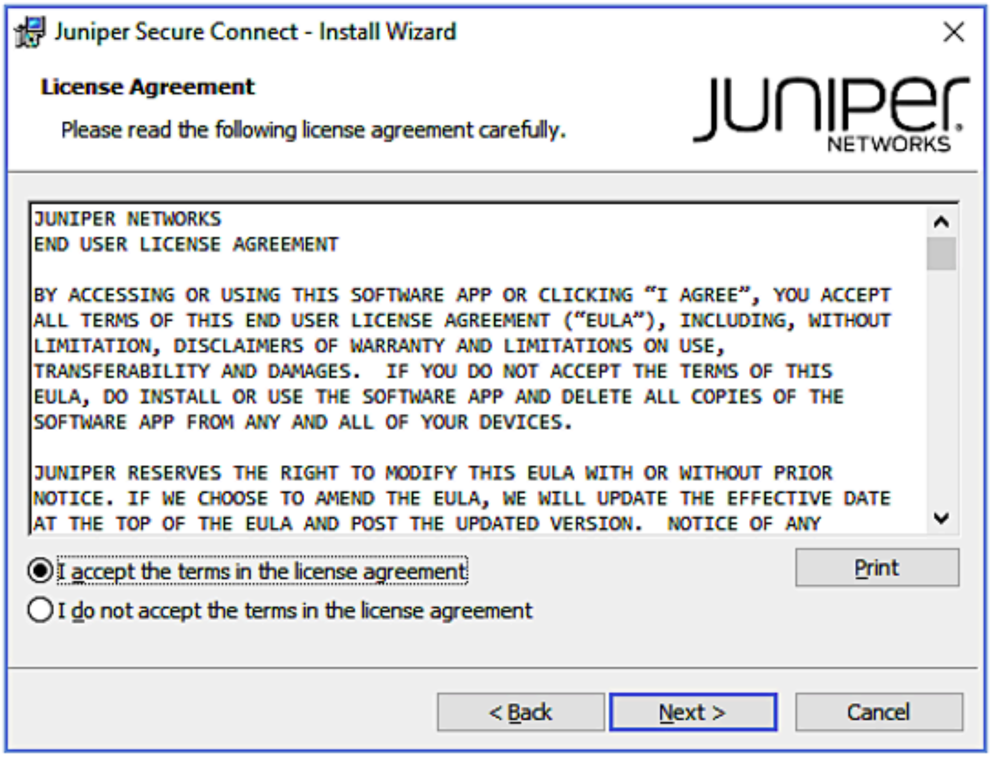
Juniper Secure Connect - Install Wizard

Welcome to the install wizard for Juniper Secure Connect 19.4.12.01 Build 45829

The install wizard will install Juniper Secure Connect on your computer. To continue, click Next.

2. Read the license agreement carefully. If you accept the terms, then select **I accept the terms in the license agreement** check box to accept the license agreement. See Figure 2.

   Figure 2: License Agreement Window



Juniper Secure Connect - Install Wizard
License Agreement
Please read the following license agreement carefully.

JUNIPER NETWORKS
END USER LICENSE AGREEMENT

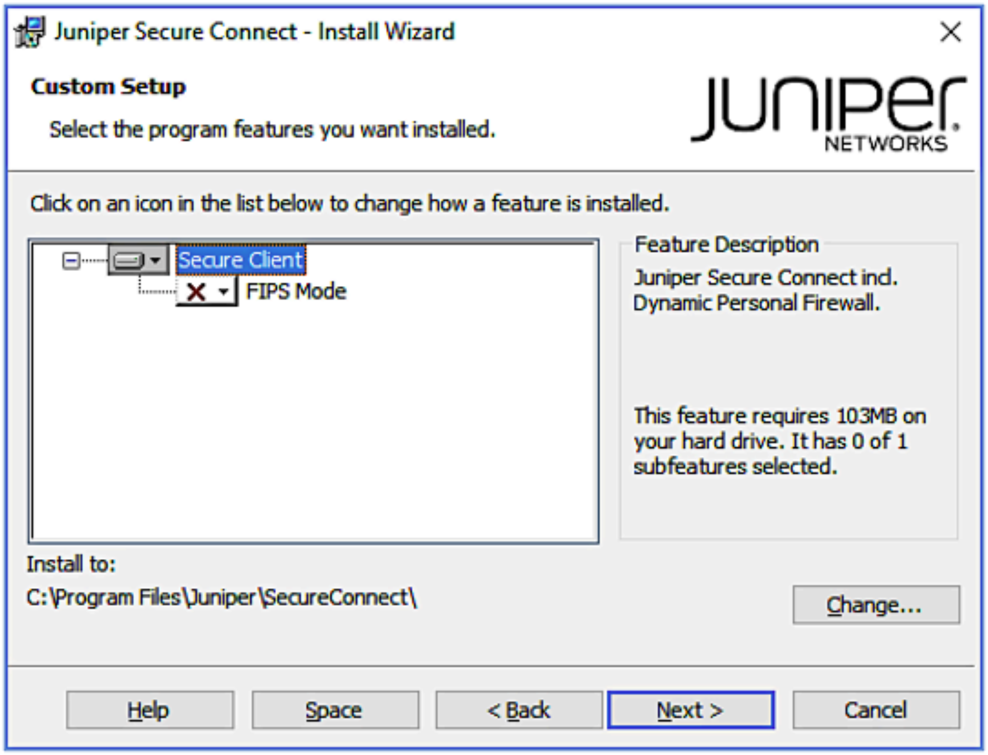
BY ACCESSING OR USING THIS SOFTWARE APP OR CLICKING "I AGREE", YOU ACCEPT ALL TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"), INCLUDING, WITHOUT LIMITATION, DISCLAIMERS OF WARRANTY AND LIMITATIONS ON USE, TRANSFERABILITY AND DAMAGES. IF YOU DO NOT ACCEPT THE TERMS OF THIS EULA, DO INSTALL OR USE THE SOFTWARE APP AND DELETE ALL COPIES OF THE SOFTWARE APP FROM ANY AND ALL OF YOUR DEVICES.

JUNIPER RESERVES THE RIGHT TO MODIFY THIS EULA WITH OR WITHOUT PRIOR NOTICE. IF WE CHOOSE TO AMEND THE EULA, WE WILL UPDATE THE EFFECTIVE DATE AT THE TOP OF THE EULA AND POST THE UPDATED VERSION. NOTICE OF ANY

● I accept the terms in the license agreement
○ I do not accept the terms in the license agreement

3. Click **Next** and choose the installation folder for downloading the Juniper Secure Connect software. See Figure 3.

Figure 3: Choose Installation Folder



Juniper Secure Connect - Install Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

Feature Description

Juniper Secure Connect incl. Dynamic Personal Firewall.

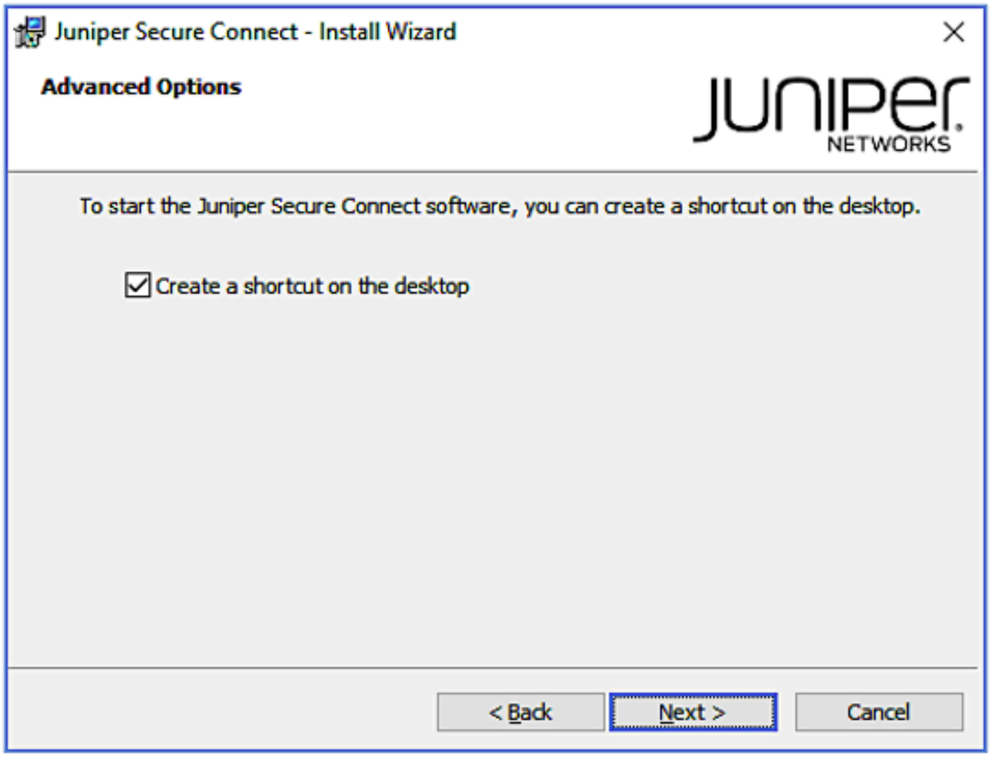
This feature requires 103MB on your hard drive. It has 0 of 1 subfeatures selected.

Install to:

C:\Program Files\Juniper\SecureConnect\

4. Click **Next** and select **Create a shortcut on the desktop** to create a shortcut for Juniper Secure Connect on your desktop. See Figure 4.

Figure 4: Create Juniper Secure Connect Shortcut on Desktop



Juniper Secure Connect - Install Wizard

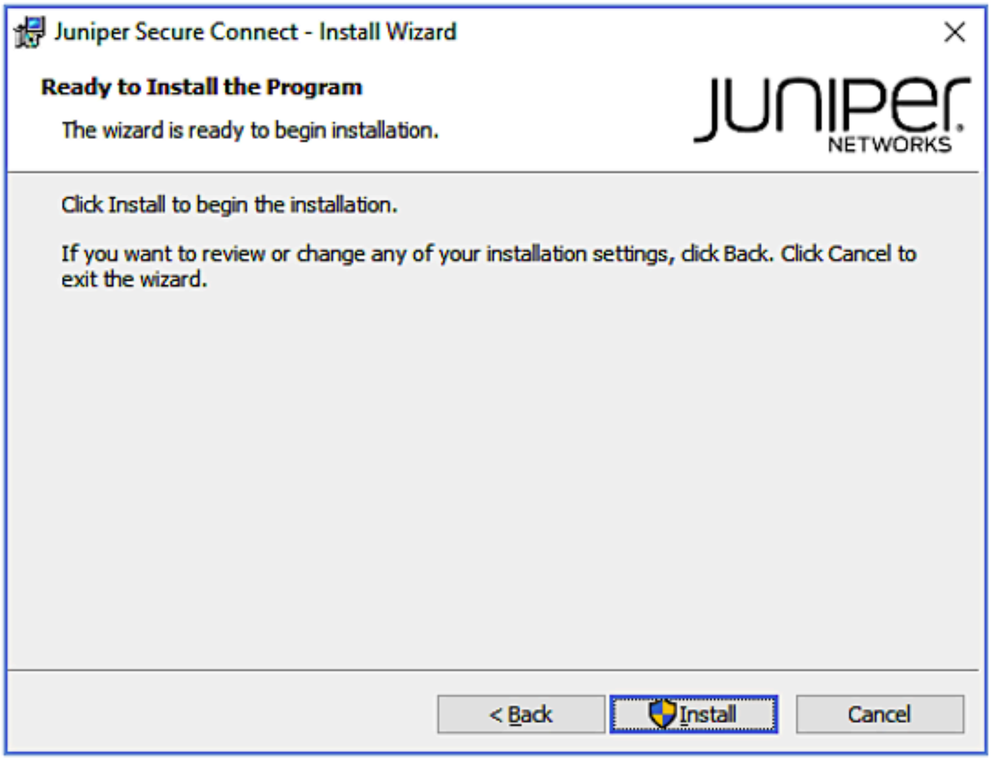
Advanced Options

To start the Juniper Secure Connect software, you can create a shortcut on the desktop.

☑ Create a shortcut on the desktop

5. Click **Next** and the installation page screen appears. Verify that you have enough space on your system. Click **Install** to begin the installation process. See Figure 5.

Figure 5: Start Juniper Secure Connect Installation



Ready to Install the Program

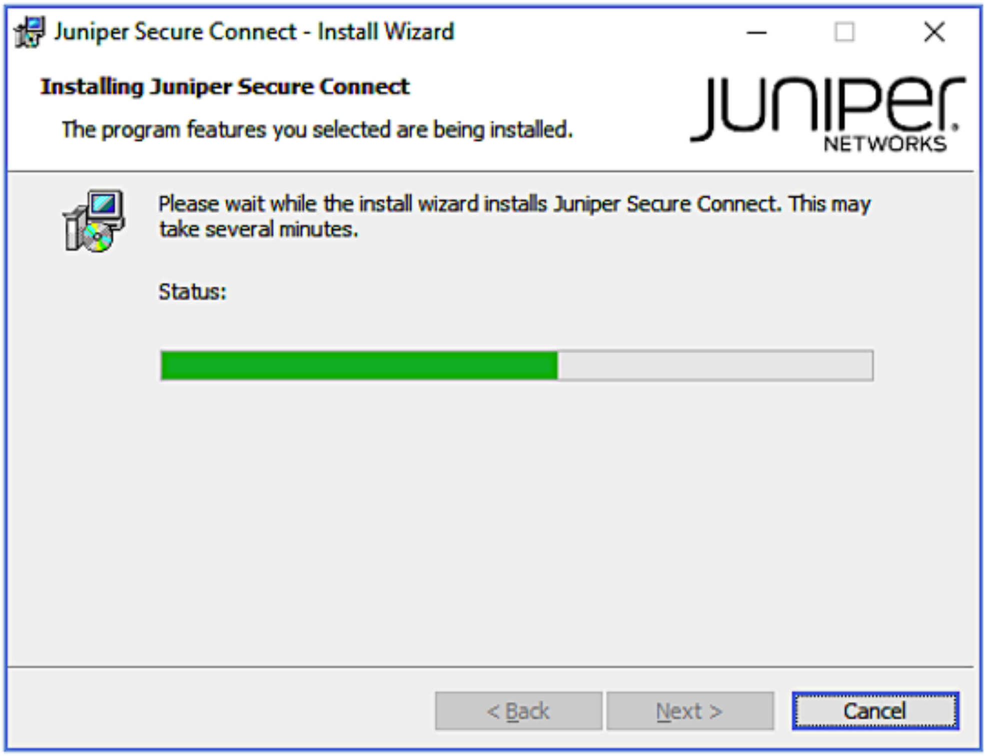
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

The installation takes several minutes to complete. Please wait till the installation is completed. See Figure 6.

Figure 6: Juniper Secure Connect Installation Status Display



Juniper Secure Connect - Install Wizard

Installing Juniper Secure Connect

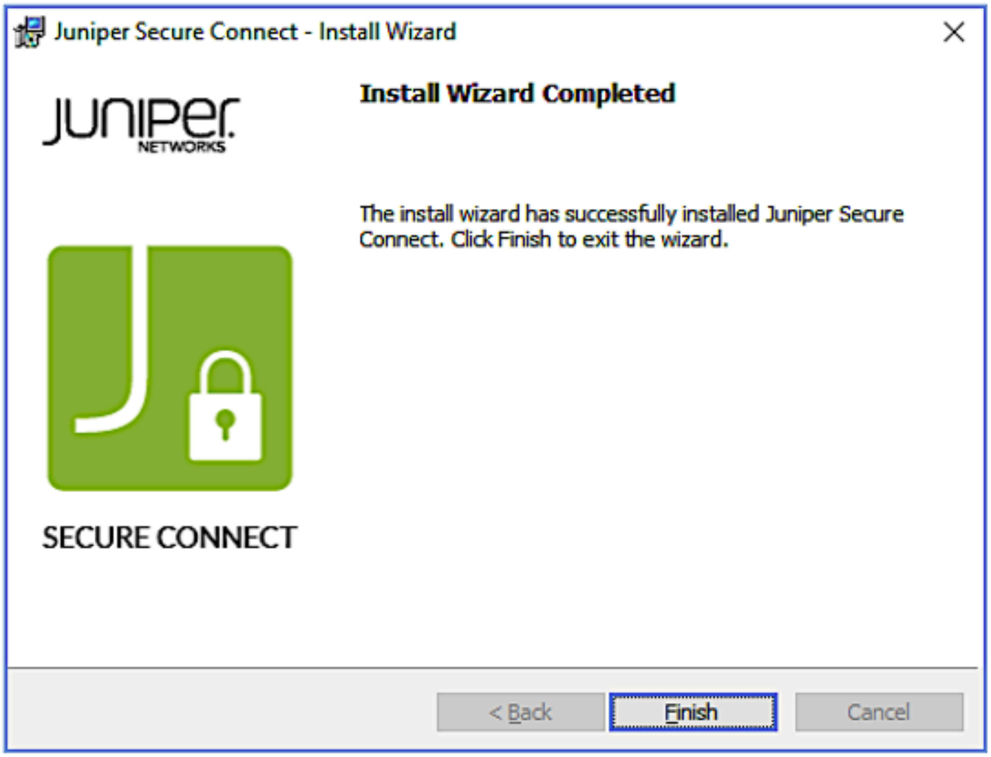
The program features you selected are being installed.

Please wait while the install wizard installs Juniper Secure Connect. This may take several minutes.

Status:

6. Once the installation is complete, click **Finish**. See Figure 7.

Figure 7: Juniper Secure Connect Installation Completed



Install Wizard Completed

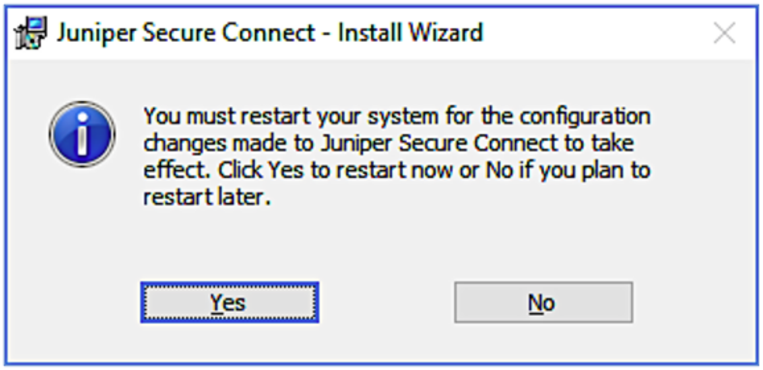
The install wizard has successfully installed Juniper Secure Connect. Click Finish to exit the wizard.

Congratulations! The Juniper Secure Connect application is successfully installed on your Windows machine.

Establishing a Connection from Juniper Secure Connect Client (Windows)

7. To use the application, you must first restart your system. See Figure 8.

Figure 8: System Restart Notification



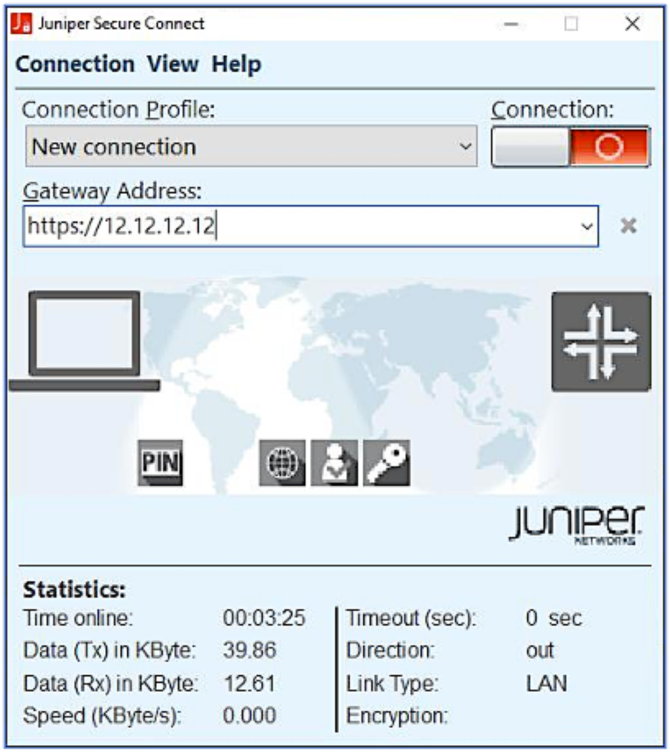
Juniper Secure Connect - Install Wizard

You must restart your system for the configuration changes made to Juniper Secure Connect to take effect. Click Yes to restart now or No if you plan to restart later.

8. You can now launch the Juniper Secure Connect and enter the **Gateway Address** URL to connect with the SRX Series Firewall. Figure 9 shows an example to enter the gateway address to the SRX Series Firewall.

   You can also enter a fully qualified domain name (FQDN) in the **Gateway Address** URL to connect with the SRX Series Firewall. For example: https://vpn.juniper.net. After entering the gateway address, click the connection toggle button to establish connection manually to the destination system. You can also select **Connection > Connect** from the menu bar to manually establish a VPN connection. When the connection is established successfully, the application window minimizes in the task bar.

   Figure 9: Launch Juniper Secure Connect



Connection Profile: New connection

Connection:

Gateway Address: https://12.12.12.12

Statistics:

Time online:	00:03:25	Timeout (sec):	0 sec
Data (Tx) in KByte:	39.86	Direction:	out
Data (Rx) in KByte:	12.61	Link Type:	LAN
Speed (KByte/s):	0.000	Encryption:	

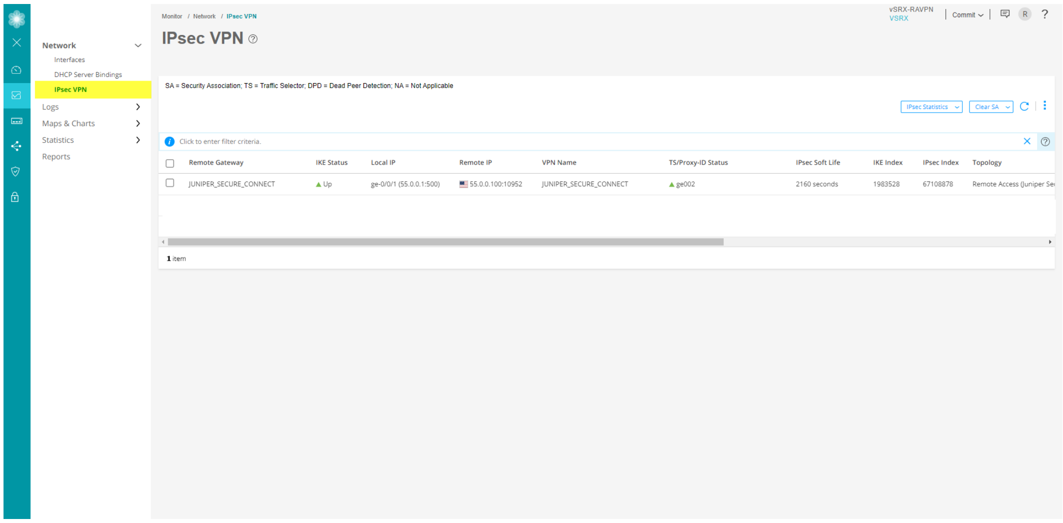
The following link provides a quick display of additional information about your remote access connection GUI Elements.

https://www.juniper.net/documentation/us/en/software/secure-connect/secure-connect-user-guide/topics/concept/explore-juniper-secure-connect-macos.html

Monitoring Remote Sessions on the vSRX

You can use the J-Web interface to monitor the existing remote access VPN connection. To do this, navigate to **Monitor > Network > IPsec VPN** page. Figure 1 shows the sample IPsec VPN page under monitoring menu option.

Figure 1: Monitor **IPsec VPN** Page



SA = Security Association; TS = Traffic Selector; DPD = Dead Peer Detection; NA = Not Applicable

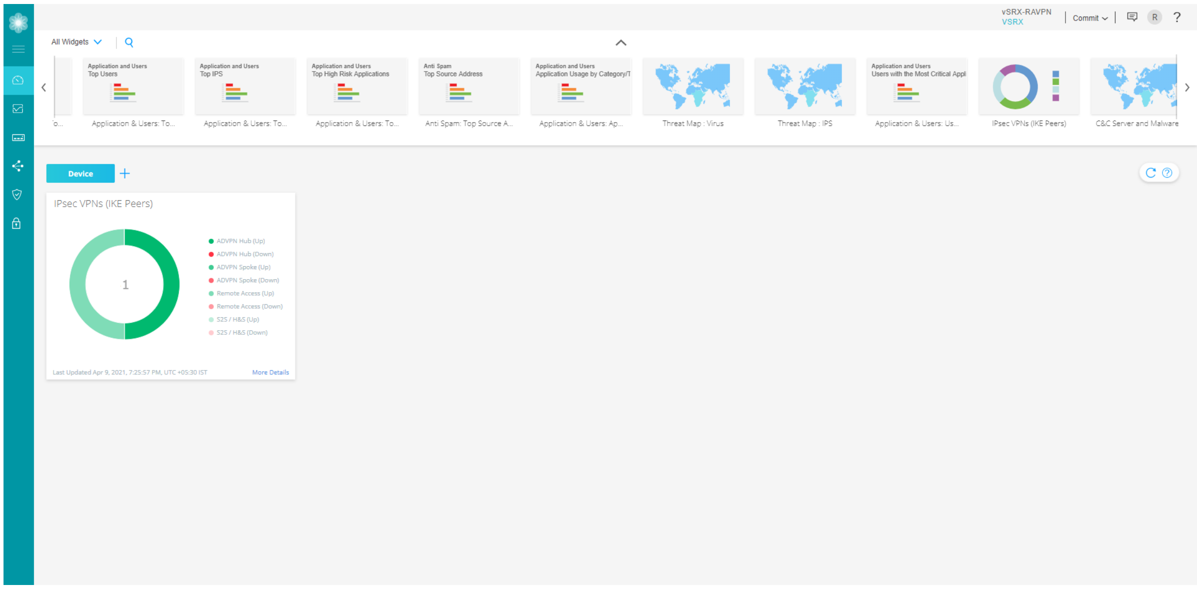
☐	Remote Gateway	IKE Status	Local IP	Remote IP	VPN Name	TS/Proxy-ID Status	IPsec Soft Life	IKE Index	IPsec Index	Topology
☐	JUNIPER_SECURE_CONNECT	▲ Up	ge-0/0/1 (55.0.0.1:500)	55.0.0.100:10952	JUNIPER_SECURE_CONNECT	▲ ge002	2160 seconds	1983528	67108878	Remote Access (Juniper Se

The **IPsec VPN** page displays IKE/IPsec configuration, Security associations (SA), and IPsec statistics information.

See Monitor IPsec VPN for more details.

You can also view J-Web Dashboard to get the status and count of IKE peers as shown in Figure 2. Hover over the sections in the widget, to view the IKE peers count with VPN topology type. See Dashboard Overview .

Figure 2: Sample **IPsec VPNs (IKE Peers)** Dashboard



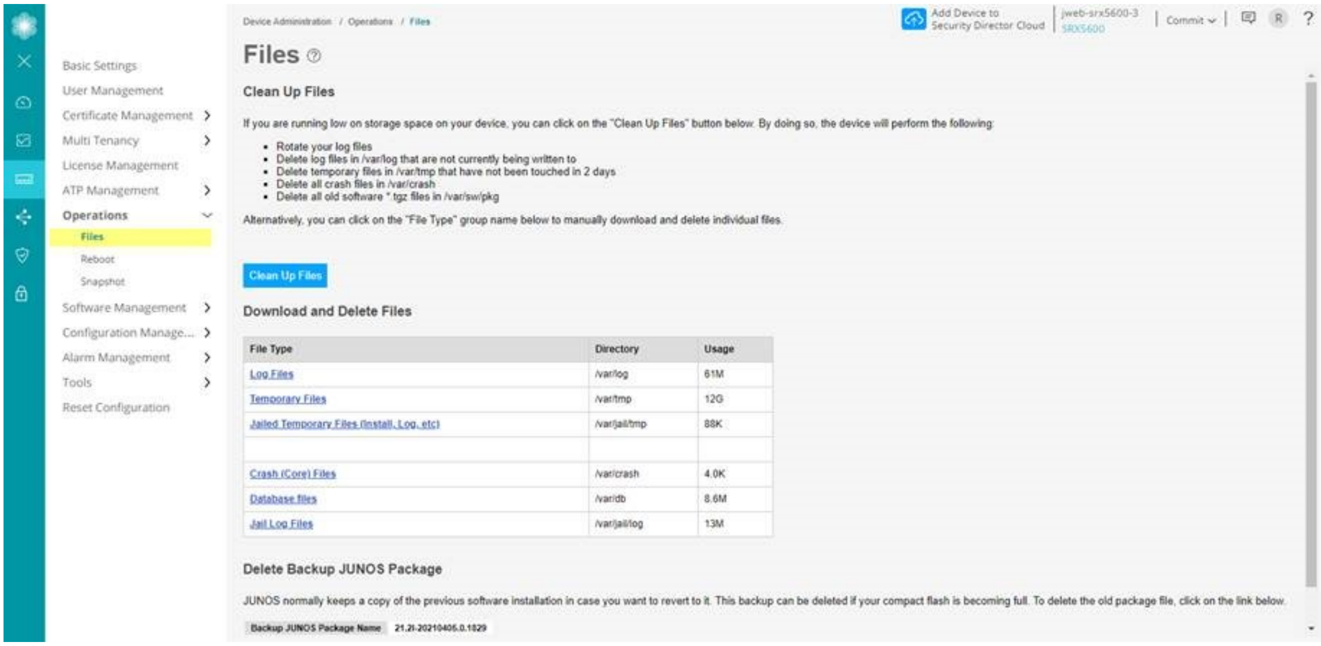
Last Updated Apr 9, 2021, 7:25:57 PM, UTC +05:30 IST

Check Junos OS Logs

You must configure syslog to save the syslog file on your device. Currently, J-Web does not support structured logs. Only unstructured logs are supported.

To view the system logs in J-Web interface, navigate to **Device Administration > Operations > Files** as shown below:

Figure 3: **Files** Page



Device Administration / Operations / Files

Files

Clean Up Files

If you are running low on storage space on your device, you can click on the "Clean Up Files" button below. By doing so, the device will perform the following:

- Rotate your log files
- Delete log files in /var/log that are not currently being written to
- Delete temporary files in /var/tmp that have not been touched in 2 days
- Delete all crash files in /var/crash
- Delete all old software *.tgz files in /var/sw/pkg

Alternatively, you can click on the "File Type" group name below to manually download and delete individual files.

Download and Delete Files

File Type	Directory	Usage
Log Files	/var/log	61M
Temporary Files	/var/tmp	12G
Jailed Temporary Files (Install, Log, etc)	/var/jail/tmp	88K
Crash (Core) Files	/var/crash	4.0K
Database files	/var/db	8.6M
Jail Log Files	/var/jail/log	13M

Delete Backup JUNOS Package

JUNOS normally keeps a copy of the previous software installation in case you want to revert to it. This backup can be deleted if your compact flash is becoming full. To delete the old package file, click on the link below.

Backup JUNOS Package Name 21.2I-20210406.0.1829

The default logs files and trace options are automatically created under `/var/log` folder.

You can view the stream (traffic or routing engine) logs by navigating to **Monitor > Events > IPsec VPN** page.

Check Juniper Secure Connect Application Logs

WINDOWS

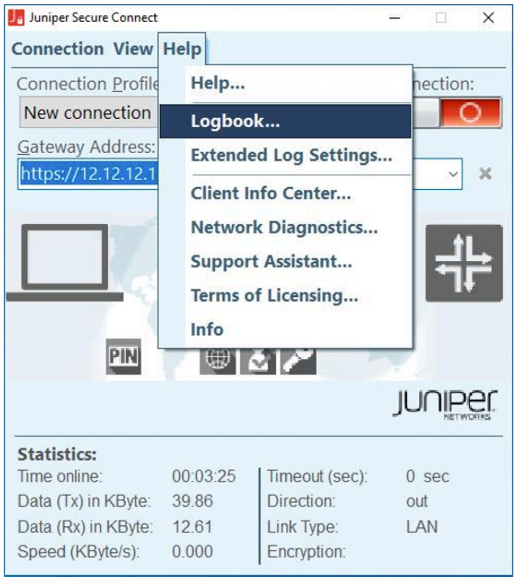
Following are the steps to check the Juniper Secure Connect application logs on a Windows device:

1. The log is continuously active in the background, even if the log window is not open. All the relevant Juniper Secure Connect communication events are displayed and saved for one week per operation day, in a log file. The files older than seven online days are automatically deleted.

The log file is generated automatically in the installation directory under the `Log` folder when the communication process is completed. The log file is named in `NCPyymmdd.LOG`format, where yy=year, mm=month, and dd=date. Select **Help > Logbook** to view the log messages in the log book page.

You can change the storage time for log files using the **Extended Log Settings** option. You can open and analyze the log files using a text editor.

Figure 4: Logbook Menu Option



Connection Profile: New connection

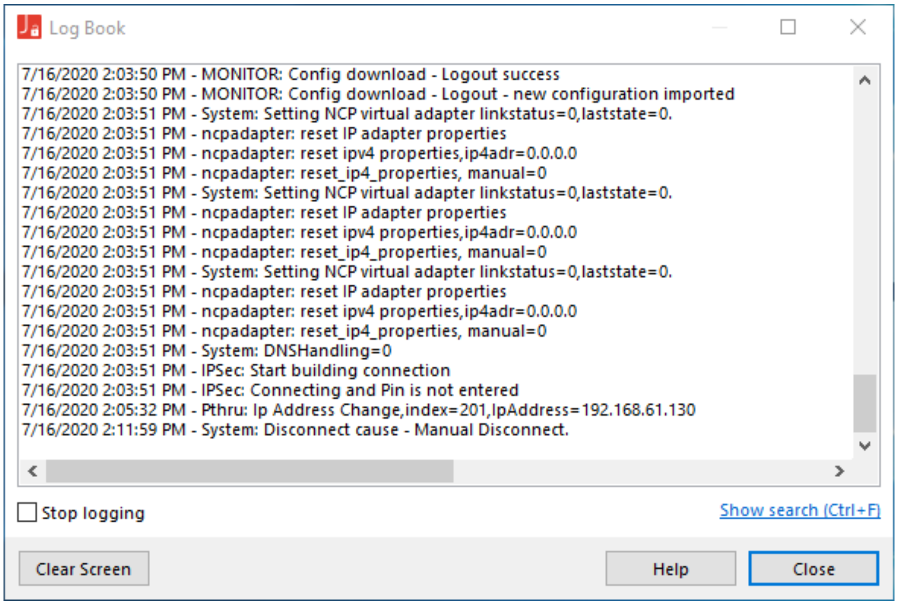
Gateway Address: https://12.12.12.1

Statistics:

Time online: 00:03:25
Data (Tx) in KByte: 39.86
Data (Rx) in KByte: 12.61
Speed (KByte/s): 0.000

Timeout (sec): 0 sec
Direction: out
Link Type: LAN
Encryption:

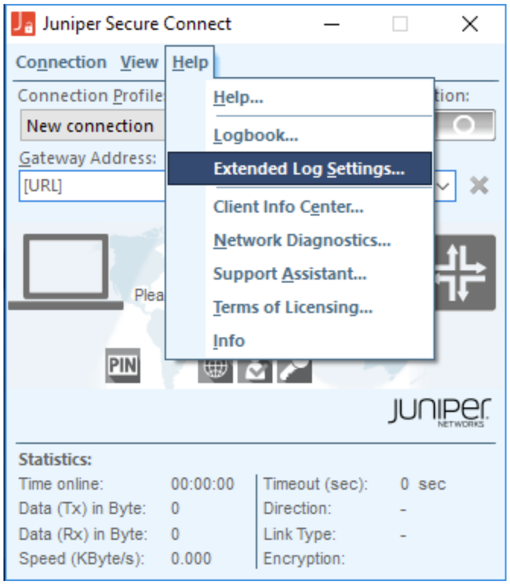
Figure 5: Log Message Display



```
7/16/2020 2:03:50 PM - MONITOR: Config download - Logout success
7/16/2020 2:03:50 PM - MONITOR: Config download - Logout - new configuration imported
7/16/2020 2:03:51 PM - System: Setting NCP virtual adapter linkstatus=0,laststate=0.
7/16/2020 2:03:51 PM - ncpadapter: reset IP adapter properties
7/16/2020 2:03:51 PM - ncpadapter: reset ipv4 properties,ip4adr=0.0.0.0
7/16/2020 2:03:51 PM - ncpadapter: reset_ip4_properties, manual=0
7/16/2020 2:03:51 PM - System: Setting NCP virtual adapter linkstatus=0,laststate=0.
7/16/2020 2:03:51 PM - ncpadapter: reset IP adapter properties
7/16/2020 2:03:51 PM - ncpadapter: reset ipv4 properties,ip4adr=0.0.0.0
7/16/2020 2:03:51 PM - ncpadapter: reset_ip4_properties, manual=0
7/16/2020 2:03:51 PM - System: Setting NCP virtual adapter linkstatus=0,laststate=0.
7/16/2020 2:03:51 PM - ncpadapter: reset IP adapter properties
7/16/2020 2:03:51 PM - ncpadapter: reset ipv4 properties,ip4adr=0.0.0.0
7/16/2020 2:03:51 PM - ncpadapter: reset_ip4_properties, manual=0
7/16/2020 2:03:51 PM - System: DNSHandling=0
7/16/2020 2:03:51 PM - IPSec: Start building connection
7/16/2020 2:03:51 PM - IPSec: Connecting and Pin is not entered
7/16/2020 2:05:32 PM - Pthru: Ip Address Change,index=201,IpAddress=192.168.61.130
7/16/2020 2:11:59 PM - System: Disconnect cause - Manual Disconnect.
```

2. From the menu bar, click **Help** and then select **Extended Log Settings**.

Figure 6: Extended Log Settings Menu Option

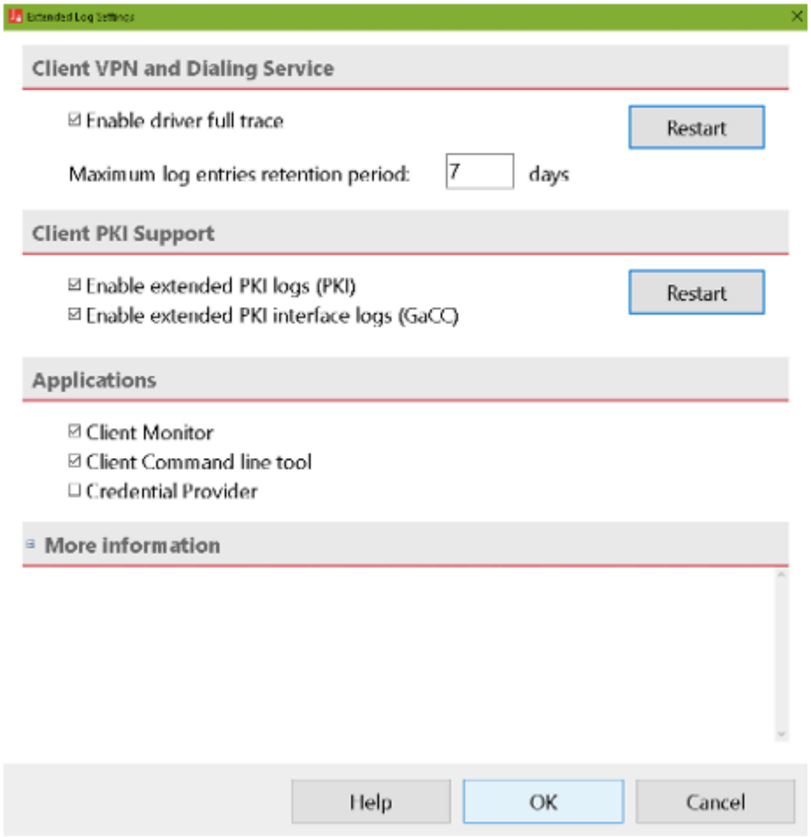


Statistics:

Time online:	00:00:00	Timeout (sec):	0 sec
Data (Tx) in Byte:	0	Direction:	-
Data (Rx) in Byte:	0	Link Type:	-
Speed (KByte/s):	0.000	Encryption:	

3. Enable all options by selecting all the check boxes, and then click OK.

Figure 7: Extended Log Settings



Extended Log Settings

Client VPN and Dialing Service

☑ Enable driver full trace

Maximum log entries retention period: 7 days

Client PKI Support

☑ Enable extended PKI logs (PKI)

☑ Enable extended PKI interface logs (GaCC)

Applications

☑ Client Monitor

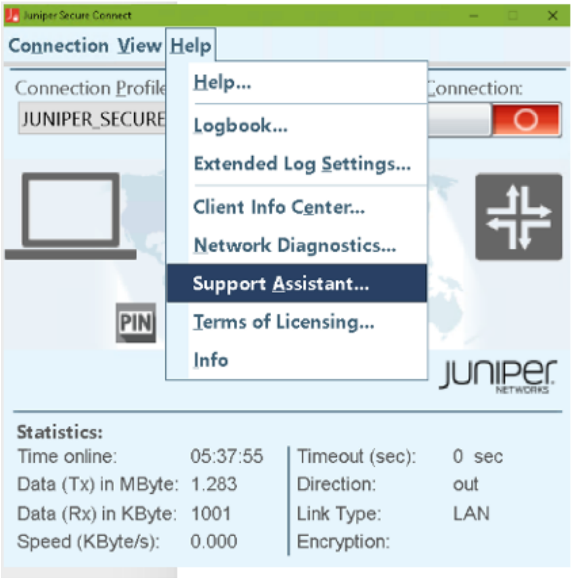
☑ Client Command line tool

□ Credential Provider

More information

4. Open the logbook and check for any log messages that indicate the problem. If you cannot resolve your issue based upon the log messages, start the Support Assistant by clicking **Help** and then selecting **Support Assistant**. The Support Assistant collects all the required data.

Figure 8: Support Assistant Menu Option



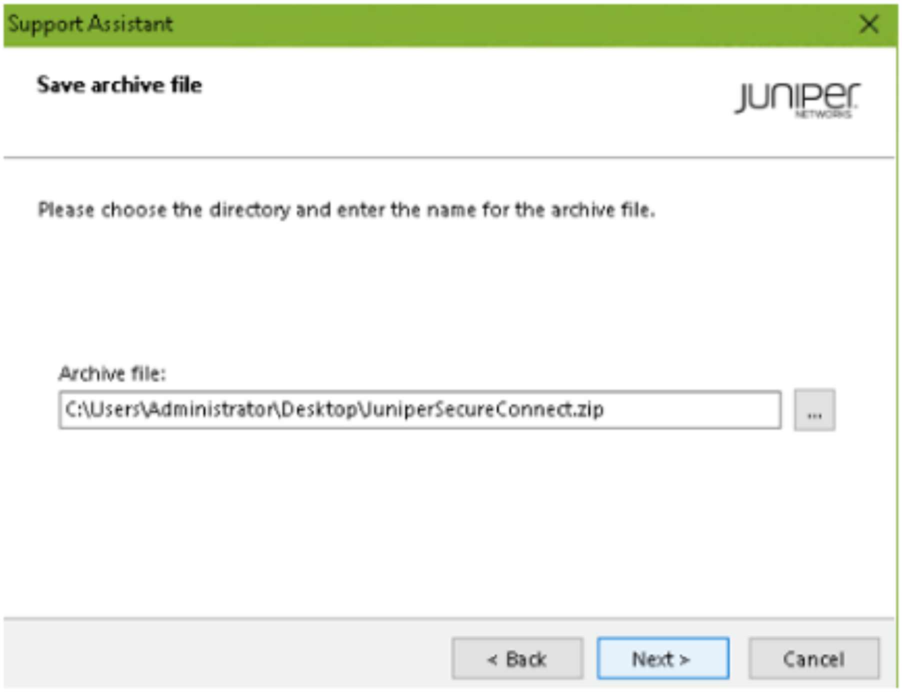
JUNIPER_SECURE

Statistics:

Time online:	05:37:55	Timeout (sec):	0 sec
Data (Tx) in MByte:	1.283	Direction:	out
Data (Rx) in KByte:	1001	Link Type:	LAN
Speed (KByte/s):	0.000	Encryption:	

5. Click **Add** to attach any additional files, and then click **Next**. The **Save archive file** page opens.

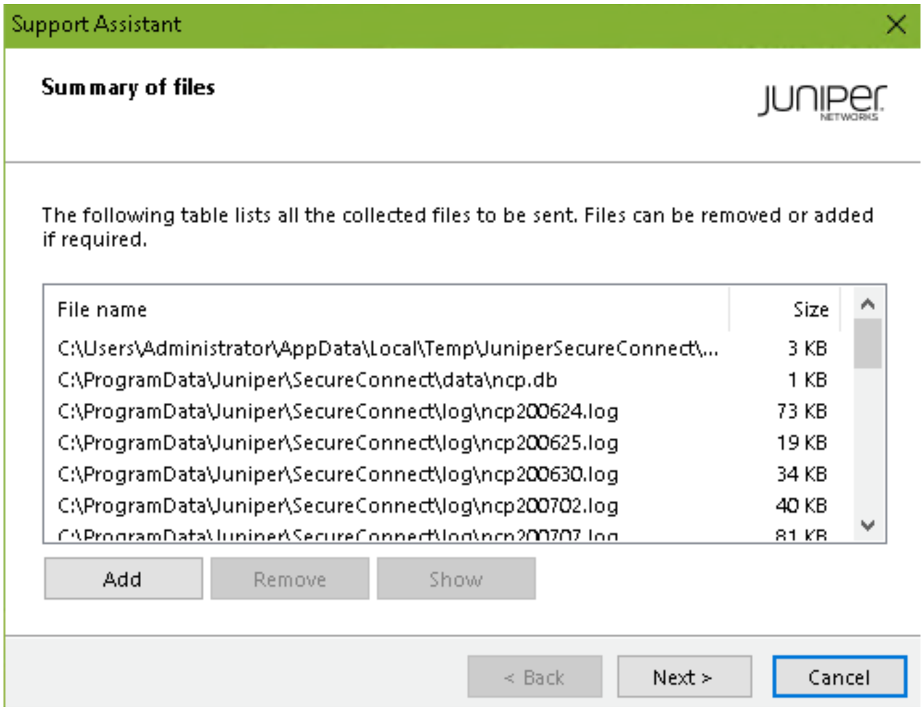
Figure 9: Save Archive File



Please choose the directory and enter the name for the archive file.

Archive file: C:\Users\Administrator\Desktop\JuniperSecureConnect.zip

Figure 10: Log Files List



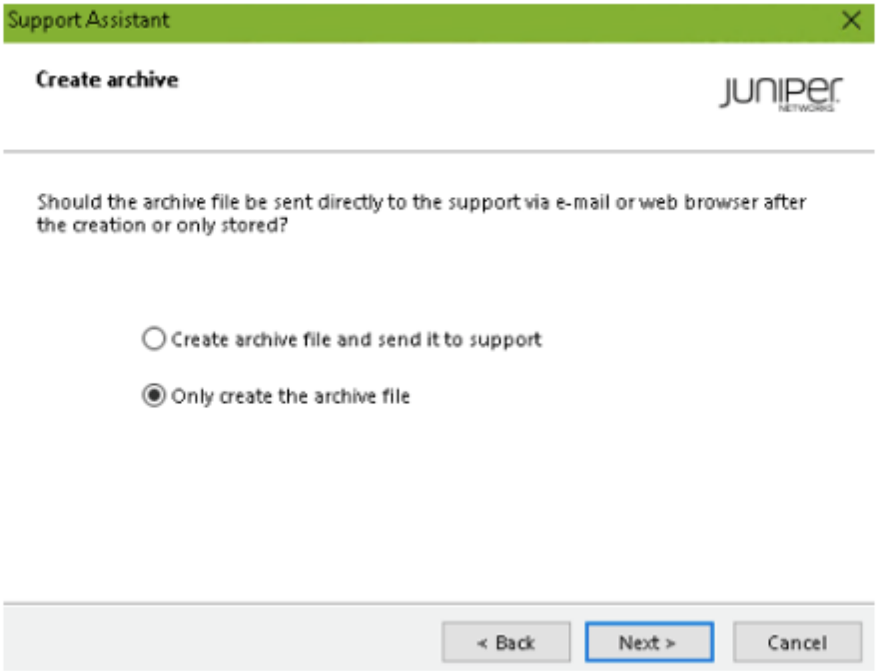
Summary of files

The following table lists all the collected files to be sent. Files can be removed or added if required.

File name	Size
C:\Users\Administrator\AppData\Local\Temp\JuniperSecureConnect\...	3 KB
C:\ProgramData\Juniper\SecureConnect\data\ncp.db	1 KB
C:\ProgramData\Juniper\SecureConnect\log\ncp200624.log	73 KB
C:\ProgramData\Juniper\SecureConnect\log\ncp200625.log	19 KB
C:\ProgramData\Juniper\SecureConnect\log\ncp200630.log	34 KB
C:\ProgramData\Juniper\SecureConnect\log\ncp200702.log	40 KB
C:\ProgramData\Juniper\SecureConnect\log\ncp200707.log	81 KB

6. Select the **Only create the archive file** option button. Then, click **Next**.

Figure 11: Create Only Archive File



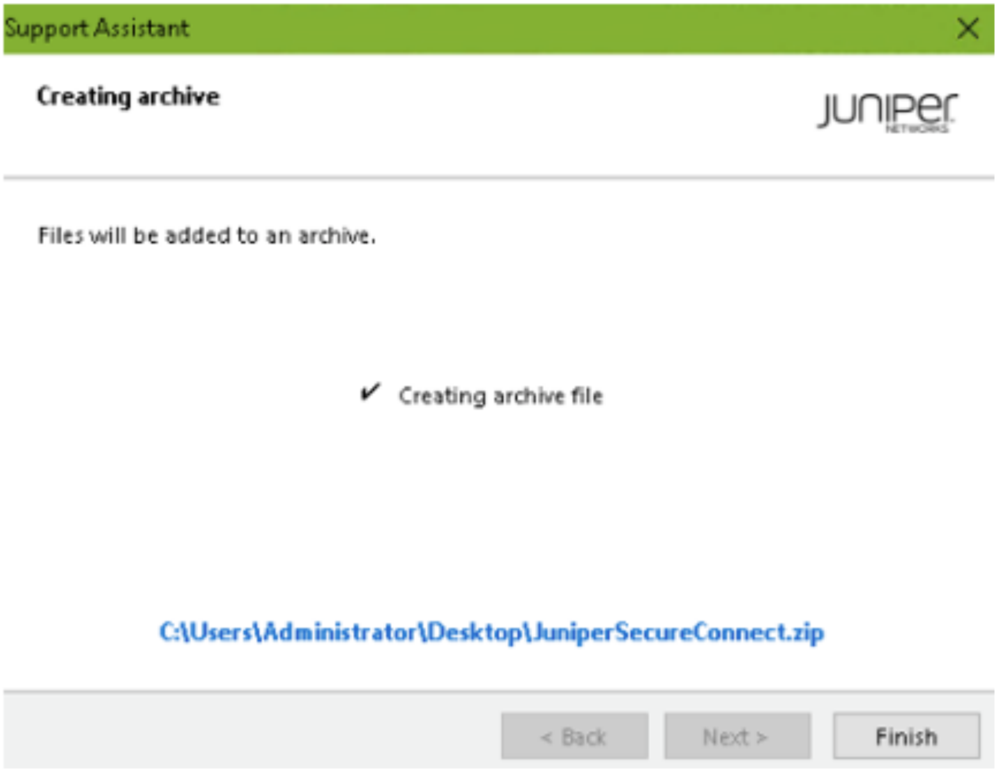
Should the archive file be sent directly to the support via e-mail or web browser after the creation or only stored?

○ Create archive file and send it to support

● Only create the archive file

After the archival process is completed, Juniper Secure Connect displays the archived file location.

Figure 12: Successful Creation of Log Files Archival



Files will be added to an archive.

✔ Creating archive file

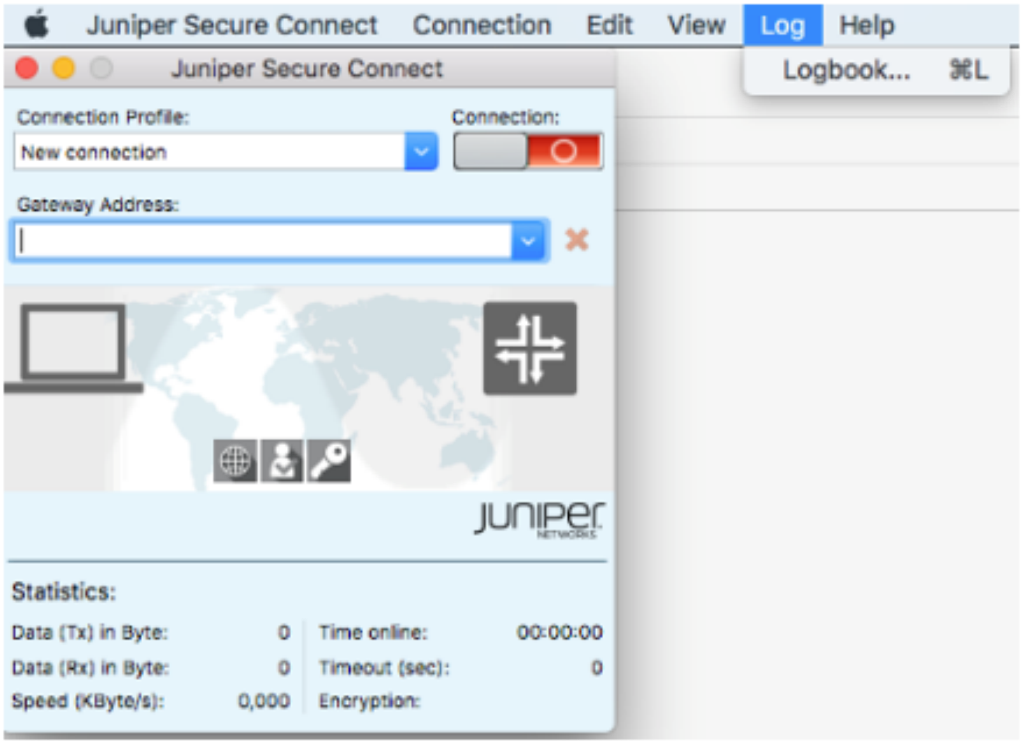
C:\Users\Administrator\Desktop\JuniperSecureConnect.zip

7. Click **Finish**.

MACOS

1. Select **Log** > **Logbook** through the Juniper Secure Connect application menu to open the logbook.

Figure 13: Logbook Menu Option



Connection Profile: New connection

Connection:

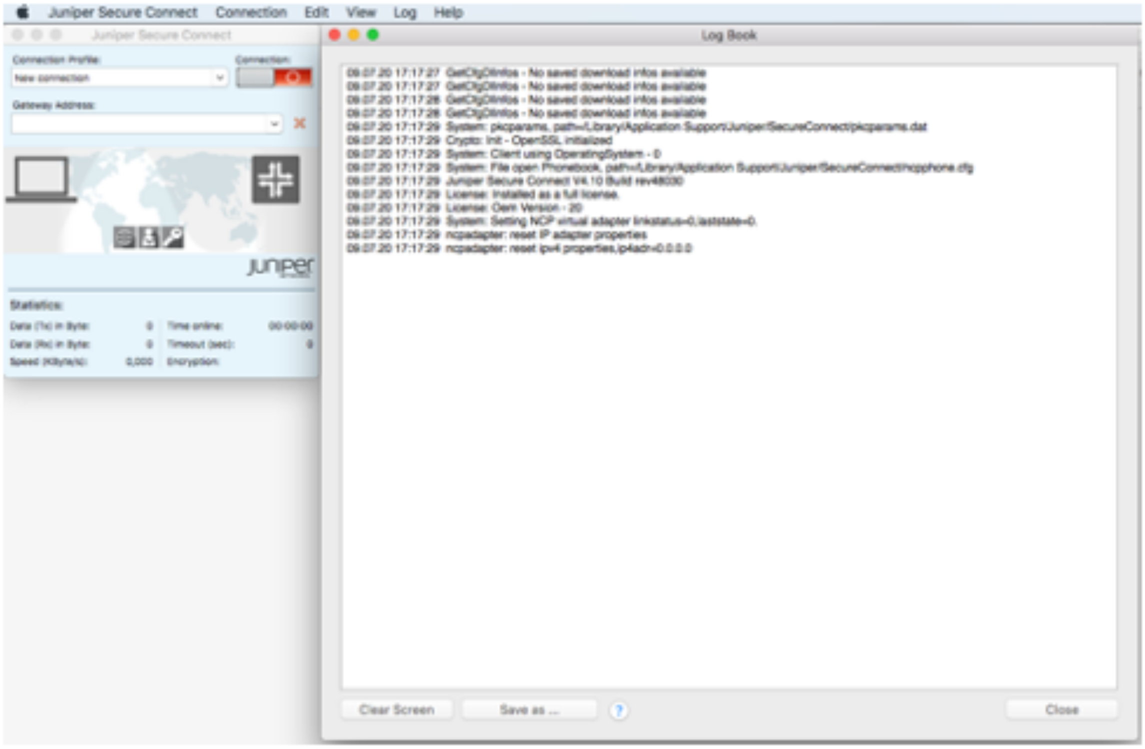
Gateway Address:

Statistics:

Data (Tx) in Byte:	0	Time online:	00:00:00
Data (Rx) in Byte:	0	Timeout (sec):	0
Speed (KByte/s):	0,000	Encryption:	

Check for any log messages that indicate the problem.

Figure 14: Displaying Log Information



Connection Profile: New connection
Connection:
Gateway Address:

Statistics:

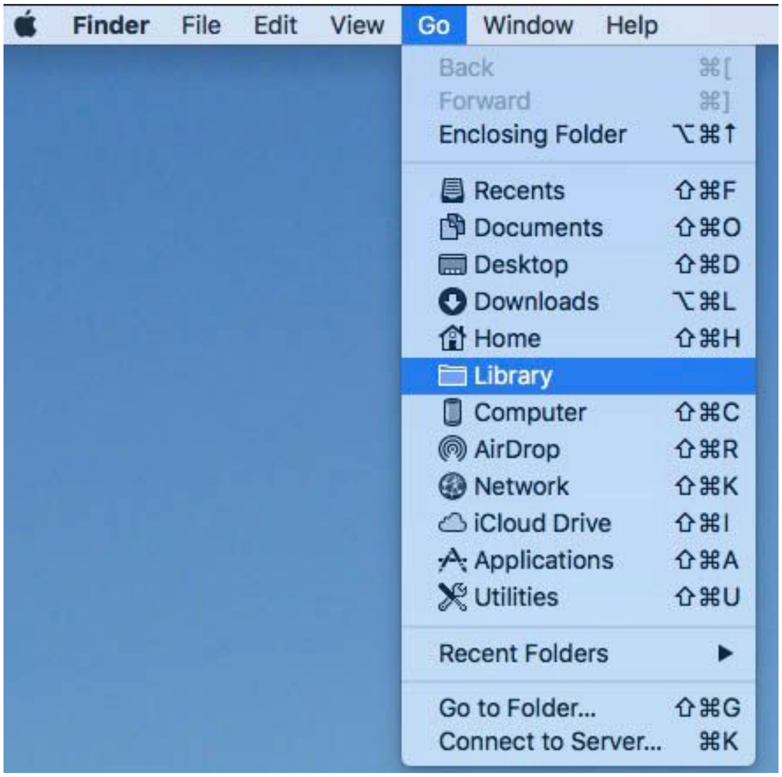
Data (Tx) in Byte: 0
Data (Rx) in Byte: 0
Speed (KByte/s): 0,000
Time online: 00:00:00
Timeout (sec): 0
Encryption:

```
09.07.20 17:17:27  GetCfgDlInfos - No saved download infos available
09.07.20 17:17:27  GetCfgDlInfos - No saved download infos available
09.07.20 17:17:28  GetCfgDlInfos - No saved download infos available
09.07.20 17:17:28  GetCfgDlInfos - No saved download infos available
09.07.20 17:17:29  System: pkcparams, path=/Library/Application Support/Juniper/SecureConnect/pkcparams.dat
09.07.20 17:17:29  Crypto: Init - OpenSSL initialized
09.07.20 17:17:29  System: Client using OperatingSystem - 0
09.07.20 17:17:29  System: File open Phonebook, path=/Library/Application Support/Juniper/SecureConnect/ncpphone.cfg
09.07.20 17:17:29  Juniper Secure Connect V4.10 Build rev48030
09.07.20 17:17:29  License: Installed as a full license.
09.07.20 17:17:29  License: Oem Version - 20
09.07.20 17:17:29  System: Setting NCP virtual adapter linkstatus=0,laststate=0.
09.07.20 17:17:29  ncpadapter: reset IP adapter properties
09.07.20 17:17:29  ncpadapter: reset ipv4 properties,ip4adr=0.0.0.0
```

2. If you are not able to resolve the issue, save this log message into a file with the `ncpmonlog.txt` filename. Copy the file `ncpphone.cfg` to the same location where you saved the logbook file `/Library/Application Support/Juniper/SecureConnect/ncpphone.cfg`.

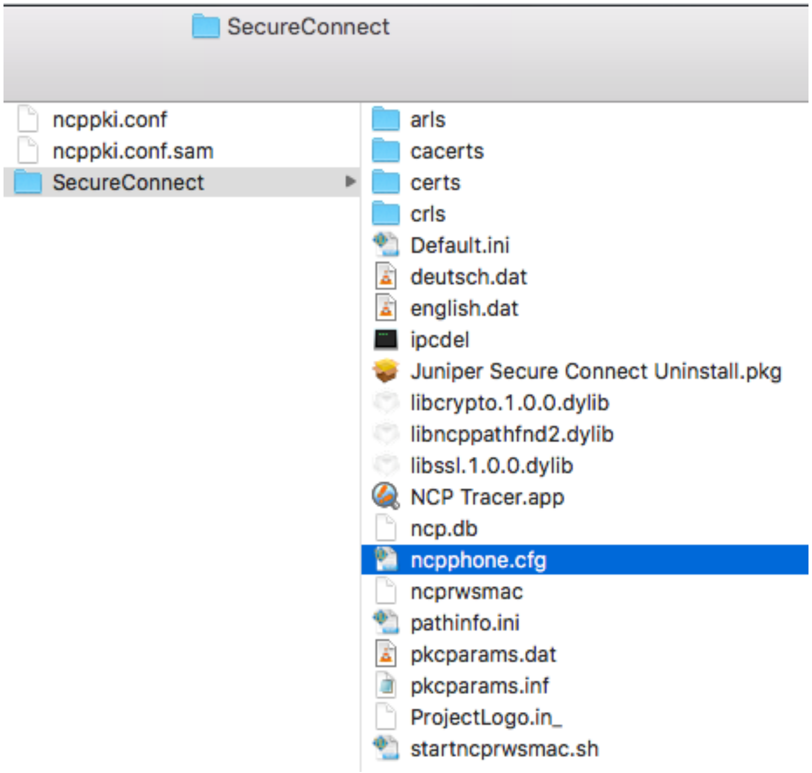
3. To locate the ncpphone.cfg file, open the Finder and select Go in the menu bar and at the same time press down the “Option” key on your keyboard.

Figure 15: Open File Library



The directory location where the Juniper Secure Connect files are saved is displayed.

Figure 16: Juniper Secure Connect Directory



SecureConnect

- ncppki.conf
- ncppki.conf.sam
- SecureConnect

- arls
- cacerts
- certs
- crls
- Default.ini
- deutsch.dat
- english.dat
- ipcdel
- Juniper Secure Connect Uninstall.pkg
- libcrypto.1.0.0.dylib
- libncppathfnd2.dylib
- libssl.1.0.0.dylib
- NCP Tracer.app
- ncp.db
- ncpphone.cfg
- ncprwsmac
- pathinfo.ini
- pkcparams.dat
- pkcparams.inf
- ProjectLogo.in_
- startncprwsmac.sh

ANDROID

Following are the steps to check the Juniper Secure Connect application logs on an Android device:

In the Juniper Secure Connect application menu, click the three vertical dots at the top right corner and select **Log** from the menu.

Figure 17: Juniper Secure Connect Application Screen

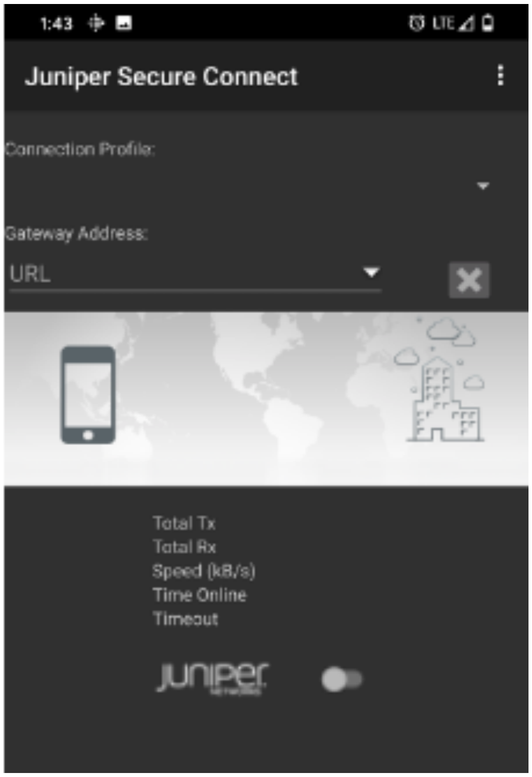
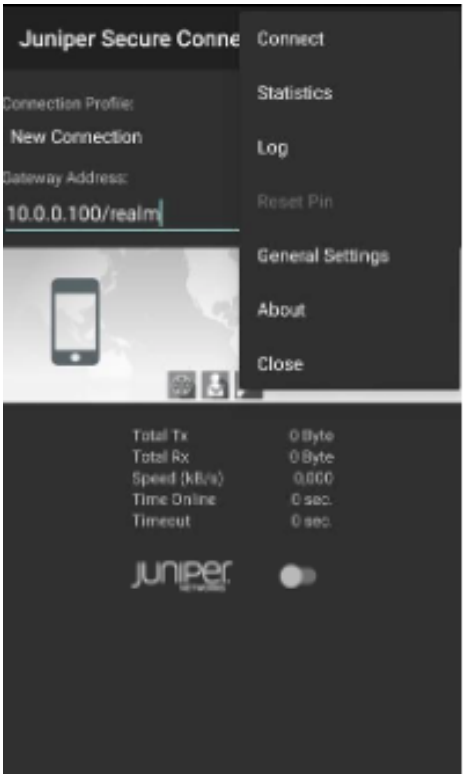


Figure 18: Log Menu Option



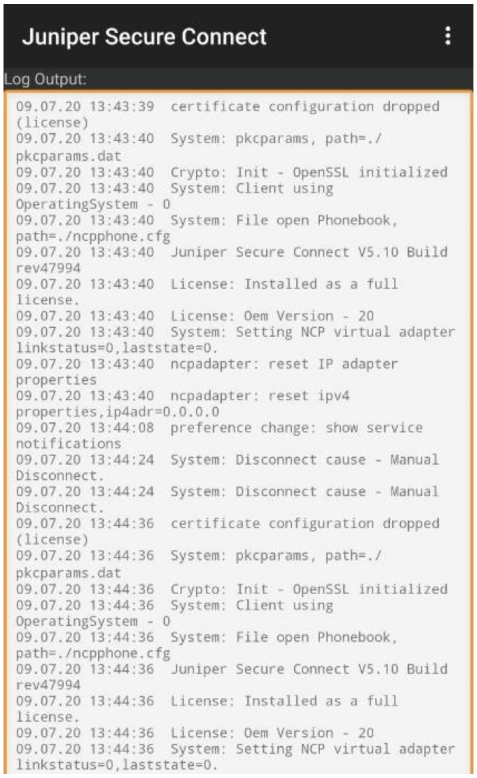
Connection Profile:
New Connection

Gateway Address:
10.0.0.100/realm

Total Tx	0 Byte
Total Rx	0 Byte
Speed (kB/s)	0,000
Time Online	0 sec.
Timeout	0 sec.

The log output window appears, displaying the log messages.

Figure 19: Displaying Log Information

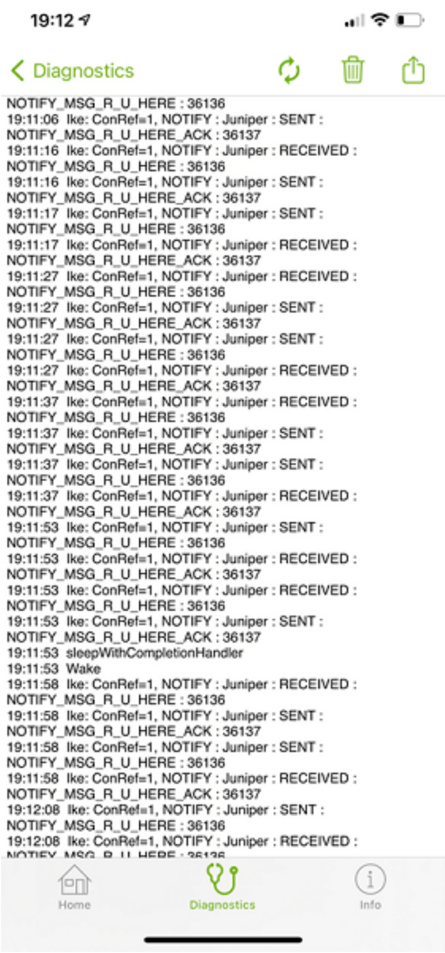


```
09.07.20 13:43:39  certificate configuration dropped
(license)
09.07.20 13:43:40  System: pkcparams, path=./
pkcparams.dat
09.07.20 13:43:40  Crypto: Init - OpenSSL initialized
09.07.20 13:43:40  System: Client using
OperatingSystem - 0
09.07.20 13:43:40  System: File open Phonebook,
path=./ncpphone.cfg
09.07.20 13:43:40  Juniper Secure Connect V5.10 Build
rev47994
09.07.20 13:43:40  License: Installed as a full
license.
09.07.20 13:43:40  License: Oem Version - 20
09.07.20 13:43:40  System: Setting NCP virtual adapter
linkstatus=0,laststate=0.
09.07.20 13:43:40  ncpadapter: reset IP adapter
properties
09.07.20 13:43:40  ncpadapter: reset ipv4
properties,ip4adr=0.0.0.0
09.07.20 13:44:08  preference change: show service
notifications
09.07.20 13:44:24  System: Disconnect cause - Manual
Disconnect.
09.07.20 13:44:24  System: Disconnect cause - Manual
Disconnect.
09.07.20 13:44:36  certificate configuration dropped
(license)
09.07.20 13:44:36  System: pkcparams, path=./
pkcparams.dat
09.07.20 13:44:36  Crypto: Init - OpenSSL initialized
09.07.20 13:44:36  System: Client using
OperatingSystem - 0
09.07.20 13:44:36  System: File open Phonebook,
path=./ncpphone.cfg
09.07.20 13:44:36  Juniper Secure Connect V5.10 Build
rev47994
09.07.20 13:44:36  License: Installed as a full
license.
09.07.20 13:44:36  License: Oem Version - 20
09.07.20 13:44:36  System: Setting NCP virtual adapter
linkstatus=0,laststate=0.
```

IOS

The log is continuously active in the background, even if the log window is closed. All the relevant Juniper Secure Connect communication events are saved in the log file. Navigate to **Diagnostics** > **Debugging** > **Error Log** to view the log messages. Click on the export icon right on top of the screen to send the log file through the offered applications.

Figure 20: Log Messages



```
NOTIFY_MSG_R_U_HERE : 36136
19:11:06  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:11:16  Ike: ConRef=1, NOTIFY : Juniper : RECEIVED :
NOTIFY_MSG_R_U_HERE : 36136
19:11:16  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:11:17  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE : 36136
19:11:17  Ike: ConRef=1, NOTIFY : Juniper : RECEIVED :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:11:27  Ike: ConRef=1, NOTIFY : Juniper : RECEIVED :
NOTIFY_MSG_R_U_HERE : 36136
19:11:27  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:11:27  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE : 36136
19:11:27  Ike: ConRef=1, NOTIFY : Juniper : RECEIVED :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:11:37  Ike: ConRef=1, NOTIFY : Juniper : RECEIVED :
NOTIFY_MSG_R_U_HERE : 36136
19:11:37  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:11:37  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE : 36136
19:11:37  Ike: ConRef=1, NOTIFY : Juniper : RECEIVED :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:11:53  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE : 36136
19:11:53  Ike: ConRef=1, NOTIFY : Juniper : RECEIVED :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:11:53  Ike: ConRef=1, NOTIFY : Juniper : RECEIVED :
NOTIFY_MSG_R_U_HERE : 36136
19:11:53  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:11:53  sleepWithCompletionHandler
19:11:53  Wake
19:11:58  Ike: ConRef=1, NOTIFY : Juniper : RECEIVED :
NOTIFY_MSG_R_U_HERE : 36136
19:11:58  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:11:58  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE : 36136
19:11:58  Ike: ConRef=1, NOTIFY : Juniper : RECEIVED :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:12:08  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE : 36136
19:12:08  Ike: ConRef=1, NOTIFY : Juniper : RECEIVED :
NOTIFY_MSG_R_U_HERE : 36136
```

Recent Knowledge Base Articles

KB79844- [SRX] How to Configure Juniper Secure Connect

KB80171- [SRX] JSC Doesn't Connect When Framed-IP-Netmask Attribute Isn't Configured on Radius

KB74733- [JSC] [SRX] How to create two or more Juniper Secure Connect VPNs using the same IP address.

KB77389- [SRX] Troubleshooting: Juniper Secure Connect Fails to Support More Than 2 Users on VPN Despite Applied License

KB71326- SRX GUI and Secure connect using same port for connectivity

KB78412- Maximum JSC connections per vSRX

KB73506- Unable to login via Juniper Secure Connect

KB74476- [SRX] Implementing Two-Factor Authentication with External App for SRX Juniper Secure Connect

KB76547- Certificate for J-Web administrative access

KB75847- Juniper Secure Connect (JSC) VPN app asks for a PIN to authenticate the user

KB75282- Which Operating Systems Support Juniper Secure Connect?

KB73398- Multi Factor Authentication with Juniper secure connect.

KB80402- JSC tunnel establishment works but drops when using HTTPS

KB80764- [SRX] How to Save Username and Password on Juniper Secure Connect Client

KB79204- vSRX not stacking remote-access-ipsec-vpn-client licenses.

KB80267- android login to jsc does not show all fields

KB72633- How to enable Split Tunnelling in Juniper Secure Connect

KB74733 - How to create two or more Juniper Secure Connect VPNs using the same IP address.

Helpful Links

Juniper Secure Connect Official Documentation

https://www.juniper.net/documentation/product/us/en/juniper-secure-connect/

Get Yourself Familiar with Juniper Secure Connect Wizard on J-Web

https://www.juniper.net/documentation/us/en/software/secure-connect/secure-connect-administrator-guide/topics/topic-map/secure-connect-getting-started.html#id-get-yourself-familiar-with-juniper-secure-connect-wizard-on-jweb

Juniper Secure Connect User Guide

https://www.juniper.net/documentation/us/en/software/secure-connect/secure-connect-user-guide/index.html

Juniper Secure Connect Administrator Guide

https://www.juniper.net/documentation/us/en/software/secure-connect/secure-connect-administrator-guide/index.html

Video Tutorial on how to configure Juniper Secure Connect using J-WEB

https://www.youtube.com/watch?v=RsswMJcTDSg

Juniper Secure Connect Administrator Guide

https://www.juniper.net/documentation/us/en/software/secure-connect/secure-connect-administrator-guide/topics/topic-map/overview.html

Data Sheet for Juniper Secure Connect

https://www.juniper.net/content/dam/www/assets/datasheets/us/en/security/juniper-secure-connect-datasheet.pdf