Engineering
Simplicity

Juniper Secure Connect User Guide

Published
2025-12-16

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Secure Connect User Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

System administrators can use this guide to understand Juniper Secure Connect and configure remote access VPN on SRX Series Firewalls. This guide also provides information about managing and monitoring VPN connections. Explore these chapters about Juniper Secure Connect:

- "Juniper Secure Connect Overview" on page 1
- "Get Started with Juniper Secure Connect" on page 10
- "Authentication in Juniper Secure Connect" on page 34
- "Configure Juniper Secure Connect" on page 228
- "Monitor Juniper Secure Connect" on page 238
- "Migrate to Juniper Secure Connect" on page 259

Remote users can refer to this guide to learn about using the Juniper Secure Connect application for secure connection to corporate private resources. See the following chapters to learn about OS-specific menu options in the Juniper Secure Connect application:

- "Juniper Secure Connect for Windows" on page 264
- "Juniper Secure Connect for macOS" on page 322
- "Juniper Secure Connect for Android" on page 361
- "Juniper Secure Connect for iOS" on page 378

RELATED DOCUMENTATION

Juniper Secure Connect

1

CHAPTER

Juniper Secure Connect Overview

SUMMARY

Explore Juniper Secure Connect as your remote access VPN solution. Learn about its features and benefits.

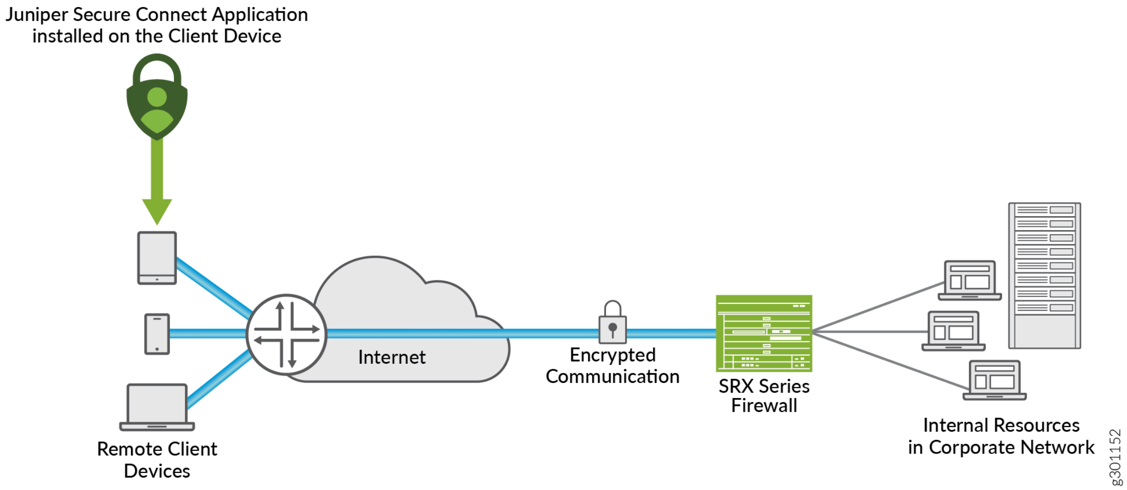
IN THIS CHAPTER

With today's modern, distributed workforce, your organization needs to keep remote users connected and productive while ensuring business continuity and security. Your organization needs to provide endpoint protection as part of a comprehensive and connected security strategy. Juniper Secure Connect® is a Juniper Networks remote access VPN solution that addresses these needs.

Juniper Secure Connect is a client-based SSL-VPN solution that allows you to securely connect and access protected resources on your network.

Figure 1 on page 2 illustrates the Juniper Secure Connect remote access solution for establishing secure VPN connectivity for remote users at different locations. The solution allows your device to connect securely to the corporate network through encrypted tunnels over the internet.

Figure 1: Juniper Secure Connect Remote Access Solution



Feature Support for Juniper Secure Connect

Table 1: Features Support for Juniper Secure Connect

Feature	Description
Multi-Platform support	Supports Windows, macOS, Android, and iOS platforms.

Table 1: Features Support for Juniper Secure Connect *(Continued)*

Feature	Description
Windows Pre-domain logon	Allows users to log on to the local Windows system through an already established VPN tunnel (using Windows Pre-Logon) so that it is authenticated to the central Windows domain or Active Directory.
Configuration support	Automatically validates that the most current policy is available before establishing the connection.
Biometric user authentication	Allows the user to protect their credentials using the operating system's built-in biometric authentication support.
Multi-Factor Authentication (MFA)	Allows you to use multi-factor authentication to extend the authentication.
Security Assertion Markup Language (SAML)	Allows you to use SAML authentication supporting single sign-on (SSO) federated identity.
IKE Support	Supports IKEv1 and IKEv2 with SSL VPN.
Juniper Secure Connect license	Licenses are available in 1-year, 3-year, and 5-year subscription models. SRX Series Firewalls and vSRX Virtual Firewall include two built-in free concurrent user/device licenses for testing.

Benefits of Juniper Secure Connect

- Flexible and secure SSL VPN access to remote users from any location.
- Less complexity with no additional hardware as you can use the existing SRX Series Firewalls deployed in your network.

- Central management of remote users, remote clients, and policies using CLI, J-Web, Security Director, and Security Director Cloud.
- Support with various bring-your-own device (BYOD) running on the most common OS types such as Windows, macOS, iOS, and Android.

What's Next

Read the following topics to know more about Juniper Secure Connect:

- "Juniper Secure Connect Components" on page 4
- "Juniper Secure Connect Deployment Setup" on page 5
- "Manage Juniper Secure Connect" on page 6
- "How Juniper Secure Connect Works" on page 8

RELATED DOCUMENTATION

System Requirements for Juniper Secure Connect | 11

Juniper Secure Connect Components

SUMMARY

Learn about the components of Juniper® Secure Connects—Juniper Networks SRX Series Firewall®, and Juniper Secure Connect application.

Juniper Secure Connect solution includes:

- SRX Series Firewall®—The firewall acts as a gateway for communication between the users of Juniper Secure Connect and protected corporate resources. The users can communicate with resources either on the network or in the cloud.

- Juniper Secure Connect application—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 (OS). It is a GUI-based easy-to-use application that connects through a VPN tunnel to the SRX Series Firewall to gain access to the protected resources in the network.

Juniper Secure Connect application, when combined with SRX Series Firewalls offers a robust remote access VPN solution. Juniper Secure Connect helps your organization quickly achieve dynamic, flexible, and adaptable connectivity from devices anywhere across the globe. Juniper Secure Connect extends visibility and enforcement from client to on-prem or cloud resources protected by SRX Series Firewalls or vSRX Virtual Firewalls, using secure VPN connections.

RELATED DOCUMENTATION

System Requirements for Juniper Secure Connect | 11

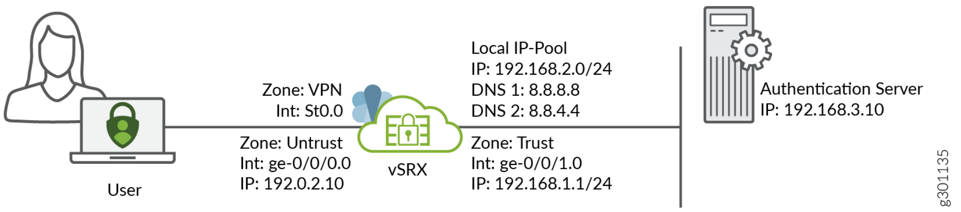
Juniper Secure Connect Deployment Setup

SUMMARY

In this topic, you'll learn about Juniper Secure Connect deployment.

Figure 2 on page 5 shows a typical deployment setup for Juniper Secure Connect. The remote user can access secured resources that are behind the firewall.

Figure 2: Juniper Secure Connect Deployment Setup



Know your remote access VPN use cases and prepare for deployment. Ensure you adjust the configuration values to map to your environment.

RELATED DOCUMENTATION

System Requirements for Juniper Secure Connect | 11

Manage Juniper Secure Connect

SUMMARY

Read this topic to understand how you can manage Juniper Secure Connect using Security Director Cloud, Junos CLIs, and J-Web.

IN THIS SECTION

You can configure Juniper Secure Connect VPN on SRX Series Firewall using Security Director Cloud, Junos OS command-line interface (CLI), and J-Web.

You can manage the Juniper Secure Connect application using the GUI interface that the application offers on the specific host Operating System (OS) such as Windows, macOS, Android, and iOS. A remote user needs to install Juniper Secure Connect only once. After providing the gateway IP address, the application initiates a connection to the SRX Series Firewall and configures the connection.

Use Security Director Cloud to Configure Juniper Secure Connect

For managing Juniper Secure Connect using a user interface (UI), we recommend you to use Security Director.

You can manage Juniper Secure Connect workloads using Juniper Security Director Cloud and Junos Space Security Director.

Juniper Security Director Cloud is a cloud-based portal that manages on-premises security, cloud-based security, and cloud-delivered security. It's a centralized security management platform that manages physical, virtual, and containerized firewall workloads. It provides a modern web-based interface for easy management.

To configure remote access VPN features, and monitor logs and reports, see Security Director Cloud User Guide, and Security Director User Guide.

See the following video to configure Juniper Secure Connect using Security Director.

Video: Configure Juniper Secure Connect using Security Director

Use Junos OS CLI to Configure Juniper Secure Connect

You can configure Juniper Secure Connect using Junos OS CLIs. Use configuration statements to configure and operational commands to monitor Juniper Secure Connect. See Junos CLI Reference for more information.

See the following video to configure Juniper Secure Connect using Junos OS CLI.

Video: Configure Juniper Secure Connect using Junos CLI

Use J-Web to Configure Juniper Secure Connect

You can manage your SRX Series Firewall using J-Web to configure and monitor Juniper Secure Connect. See J-Web User Guide for SRX Series Firewalls.

See the following video to configure Juniper Secure Connect using J-Web.

Video: Configure Juniper Secure Connect using J-Web

NOTE: The Junos-FIPS devices do not support `web-management` statement at [`edit system services`] hierarchy level. For detailed list of Junos-FIPS configuration restrictions on the FIPS compliant SRX Series Firewalls, see platform specific Junos-FIPS configuration restrictions on the Juniper Tech Library. Search for the specific SRX Series Firewall and navigate to **System Admin Guides** > **FIPS Evaluated Configuration Guide**.

RELATED DOCUMENTATION

Junos Space Security Director Overview

Security Director

How Juniper Secure Connect Works

SUMMARY

Read this topic to learn how Juniper Secure Connect works.

Before you get started with Juniper Secure Connect, let's understand how Juniper Secure Connect solution works.

The steps to connect Juniper Secure Connect application with an SRX Series Firewall are as follows:

1. A remote user downloads the Juniper Secure Connect application on a smart phone or a laptop. Alternatively, the administrator distributes it by the organization's software distribution system.

2. The remote user enters the gateway address in the URL: https://<srx_gtw_ip_or_dns_name>.

   For example, https://demo.example.com/sslvpn.

3. When the user initiates a connection, the application validates whether the gateway certificate is valid.

4. Before authenticating, the SRX Series Firewall validates the status of the connecting client device based on the match criteria configured by your administrator.

5. SRX Series Firewall authenticates the user based on credentials (user name, password, and domain) or certificates.

6. After a successful authentication, the client device downloads and installs the latest configuration policy defined on the SRX Series Firewall. This step ensures that the client always uses the latest configuration policy defined by your administrator. All the required configurations are downloaded automatically over a secure and encrypted channel when you connect.

7. The client establishes a secure VPN connection based on downloaded configuration profile.

Now that you know how the solution works, let's get started with Juniper Secure Connect.

RELATED DOCUMENTATION

System Requirements for Juniper Secure Connect | **11**

2

CHAPTER

Get Started with Juniper Secure Connect

SUMMARY

Learn about preparing your environment for Juniper Secure Connect deployment.

IN THIS CHAPTER

Before you deploy Juniper Secure Connect, based on the Figure 2 on page 5 you must ensure the following:

- Include a route in the protected network for the IP address that you assign to the clients, so that it directs traffic to the SRX Series Firewalls.
- Implement NAT for the client traffic that enters the protected network.
- Ensure that the SRX Series Firewall uses either a signed certificate or a self-signed certificate instead of the default system-generated certificate. You can also use a signed certificate from Let's Encrypt for ACME protocol support.

Read the following topics to get started with the Juniper Secure Connect:

- "System Requirements for Juniper Secure Connect" on page 11
- "Download Juniper Secure Connect" on page 13
- "Deploy Certificates for Juniper Secure Connect" on page 14

RELATED DOCUMENTATION

Juniper Secure Connect Overview | 1

System Requirements for Juniper Secure Connect

SUMMARY

In this topic you'll learn about the Operating System support for Juniper Secure Connect.

IN THIS SECTION

To use Juniper Secure Connect as your remote access VPN solution, your system administrator must first configure remote access on the SRX Series Firewall. After configuring remote access, the Juniper Secure Connect application interacts with the SRX Series Firewall to access your secure corporate resources.

Operating System Support

Read the following information to know about the Operating System (OS) support for Juniper Secure Connect:

- SRX Series Firewall or vSRX Virtual Firewall instance running Junos OS Release 20.3R1 or later.
- The Juniper Secure Connect application software running on the supported OS listed in Table 2 on page 12.

Table 2: Operating Systems Support for the Juniper Secure Connect Application

Operating System	Supported Version
Windows	• Windows 10 and above
macOS	• macOS 11 Big Sur (x86 and Apple-designed processor based on the ARM architecture), macOS 10.15 Catalina, macOS 12 Monterey (x86 and Apple-designed processor based on the ARM architecture), macOS 13 Ventura, and macOS 14 Sonoma.
Android	• Android 10 and above
iOS and iPadOS	• iOS 12 and above (including iPadOS)

See "Download Juniper Secure Connect" on page 13 to download Juniper Secure Connect and understand the license requirements.

RELATED DOCUMENTATION

Juniper Secure Connect Overview | 1

Download Juniper Secure Connect

SUMMARY

Learn how to download Juniper Secure Connect and understand its license requirements.

IN THIS SECTION

Support for the Juniper Secure Connect application is available on various Operating Systems. Read the following sections to download and install the Juniper Secure Connect application and understand its license requirements.

Download and Install the Software

We assumes that you've installed Junos OS on SRX Series Firewalls.

Use Feature Explorer to confirm platform and release support for specific features.

See Table 3 on page 13 to download and install the Juniper Secure Connect application.

Table 3: Operating Systems That Support The Installation of Juniper Secure Connect Application

Supported Operating System	Download Details	Installation Details
Windows	Download Juniper Secure Connect for Microsoft Windows	Install Juniper Secure Connect on Windows
macOS	Download Juniper Secure Coneect for Apple macOS	Install Juniper Secure Connect on macOS
Android	Download Juniper Secure Connect for Android	Install Juniper Secure Connect on Android
iOS and iPadOS	Download Juniper Secure Connect for iOS	Juniper Secure Connect on iOS

License Requirements

You need an active SRX-based license to use Juniper Secure Connect. By default, each SRX Series Firewall includes two built-in concurrent user licenses. You must purchase and install a license for additional concurrent users. Contact your Juniper Networks representative for remote-access licensing. To understand more about Juniper Secure Connect licenses, see Software Licenses for Juniper Secure Connect and Managing Licenses.

RELATED DOCUMENTATION

Juniper Secure Connect Overview | 1

Deploy Certificates for Juniper Secure Connect

SUMMARY

Read this topic to understand about Juniper Secure Connect certificate deployment.

IN THIS SECTION

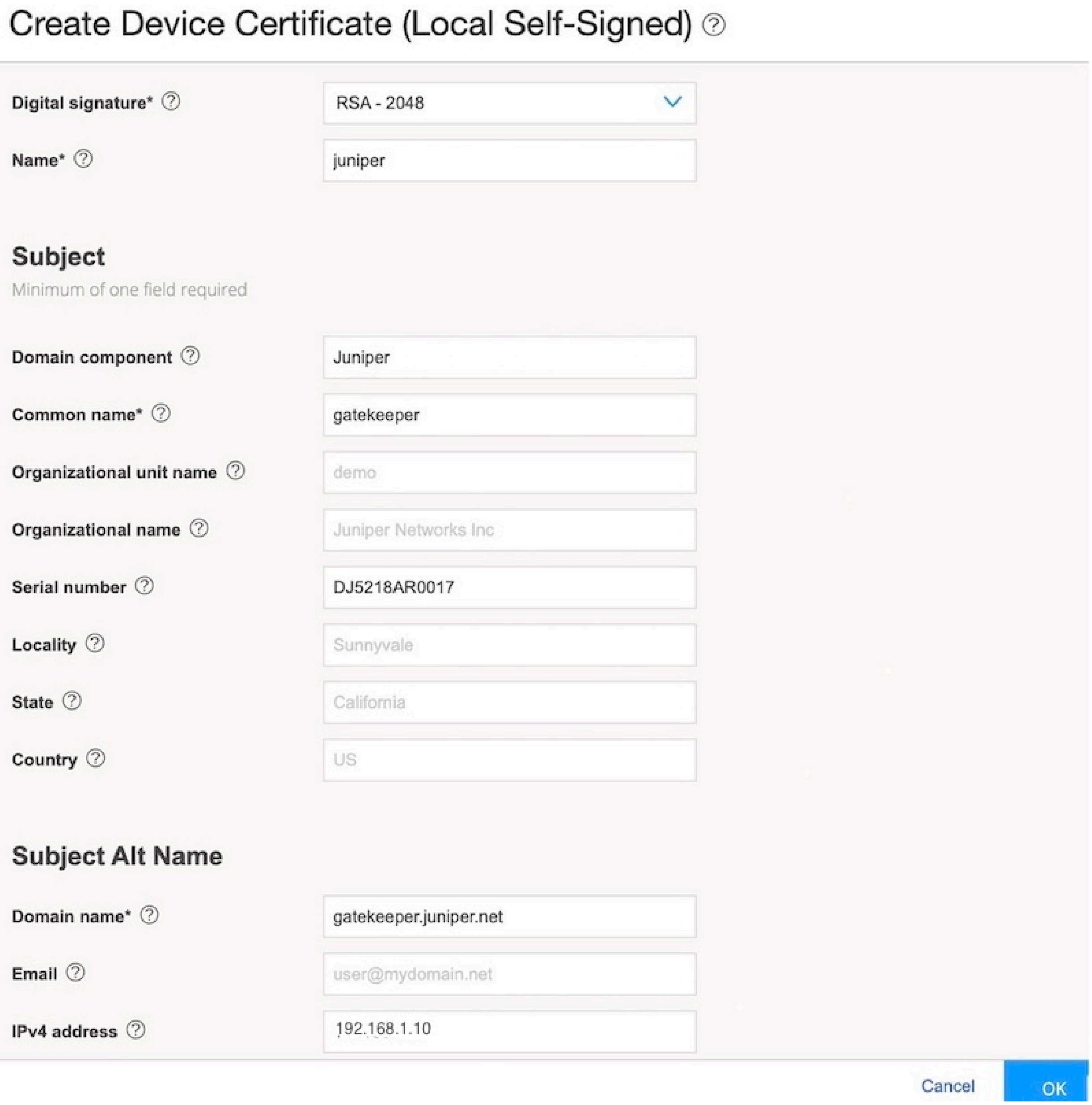
Before deploying Juniper Secure Connect, ensure that the SRX Series Firewall uses an appropriate certificate instead of the default system-generated certificate. You should choose either a signed certificate or a self-signed certificate or a signed certificate from Let's Encrypt. When the user initiates a connection to the SRX Series Firewall using Juniper Secure Connect, the application validates the gateway certificate.

How to Deploy a Certificate

To deploy a certificate, you must generate and install the required certificates. You can generate a certificate request or a self-signed certificate by navigating to **Device Administration** > **Certificates** > **Device** in the J-Web interface as shown in Figure 3 on page 16.

Figure 3 on page 16 shows the minimum of values that you should configure. Ensure that these values matches with your own organization. If you initiate a Certificate Signing Request (CSR), the certificate must be signed by your CA before it is loaded on the SRX Series Firewall.

Figure 3: Generate a Certificate Request or a Self-signed Certificate



Create Device Certificate (Local Self-Signed) ?

Digital signature* ?	RSA - 2048
Name* ?	juniper

Subject

Minimum of one field required

Domain component ?	Juniper
Common name* ?	gatekeeper
Organizational unit name ?	demo
Organizational name ?	Juniper Networks Inc
Serial number ?	DJ5218AR0017
Locality ?	Sunnyvale
State ?	California
Country ?	US

Subject Alt Name

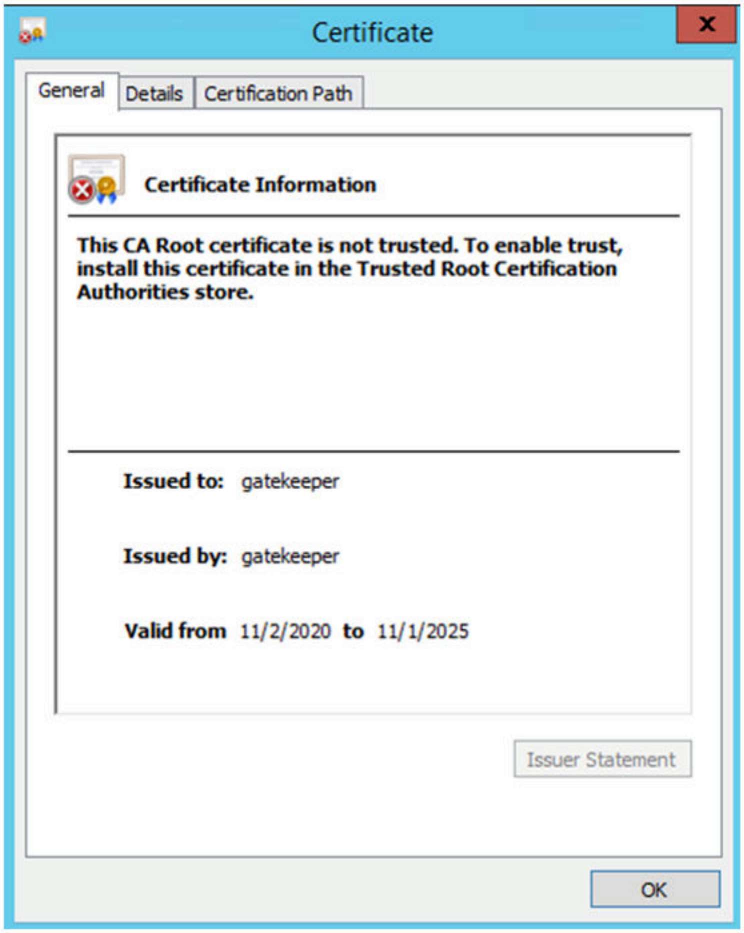
Domain name* ?	gatekeeper.juniper.net
Email ?	user@mydomain.net
IPv4 address ?	192.168.1.10

After creating a self-signed or loading a signed certificate, you must bind the certificate to the SRX Series Firewall by navigating to **Device Administration** > **Basic Settings** > **System Services** > **HTTPS** > **HTTPS certificate** and select the appropriate name.

To generate a self-signed certificate using command line interface (CLI), see "Configure Multiple Domains and Certificates" on page 20.

After loading the certificate to the SRX Series Firewall, you can validate the certificate by viewing the certificate information in your browser bar. The steps involved in viewing the certificate information depends on your browser and browser version. Figure 4 on page 17 shows the certificate in Windows after downloading the public certificate. It shows the certificate information that you configured in the SRX Series Firewall.

Figure 4: View Certificate Information



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

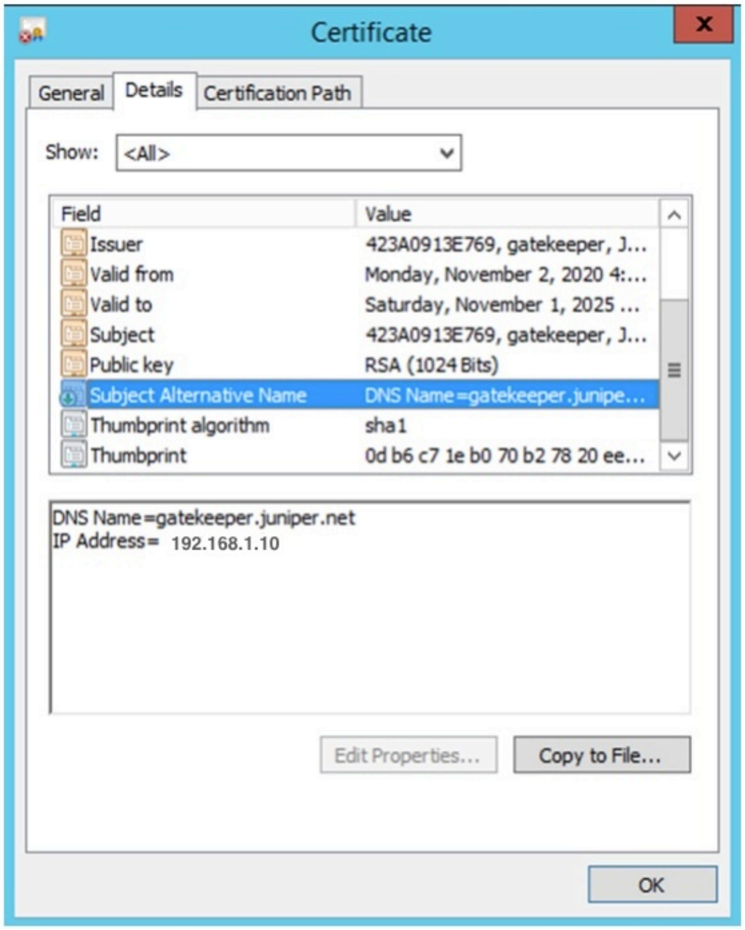
Issued to: gatekeeper

Issued by: gatekeeper

Valid from 11/2/2020 to 11/1/2025

Figure 5 on page 18 shows all the details of the certificate that is configured in the SRX Series Firewall.

Figure 5: Detailed Certificate Information



Show: <All>

Field	Value
Issuer	423A0913E769, gatekeeper, J...
Valid from	Monday, November 2, 2020 4:...
Valid to	Saturday, November 1, 2025 ...
Subject	423A0913E769, gatekeeper, J...
Public key	RSA (1024 Bits)
Subject Alternative Name	DNS Name=gatekeeper.junipe...
Thumbprint algorithm	sha1
Thumbprint	0d b6 c7 1e b0 70 b2 78 20 ee...

```
DNS Name=gatekeeper.juniper.net
IP Address= 192.168.1.10
```

You must check for the following from the certificate information in the browser:

- Check whether the Subject Alternative Name matches with your generated certificate.
- Check whether there is a warning message about the Thumbprint/Fingerprint. A warning message is displayed if you did not export the CA certificate from the SRX Series Firewall to all clients.

We recommend that you export the self-signed certificate from the SRX Series Firewall in **.pem** format, or the CA root certificate from the CA that signed your CSR to each client. You can do this manually or distribute it using a client rollout package for Windows and macOS. See "Create Installation Packages for Juniper Secure Connect Rollout on Windows" on page 271 and "Create Rollout Packages for Juniper Secure Connect Installation" on page 335.

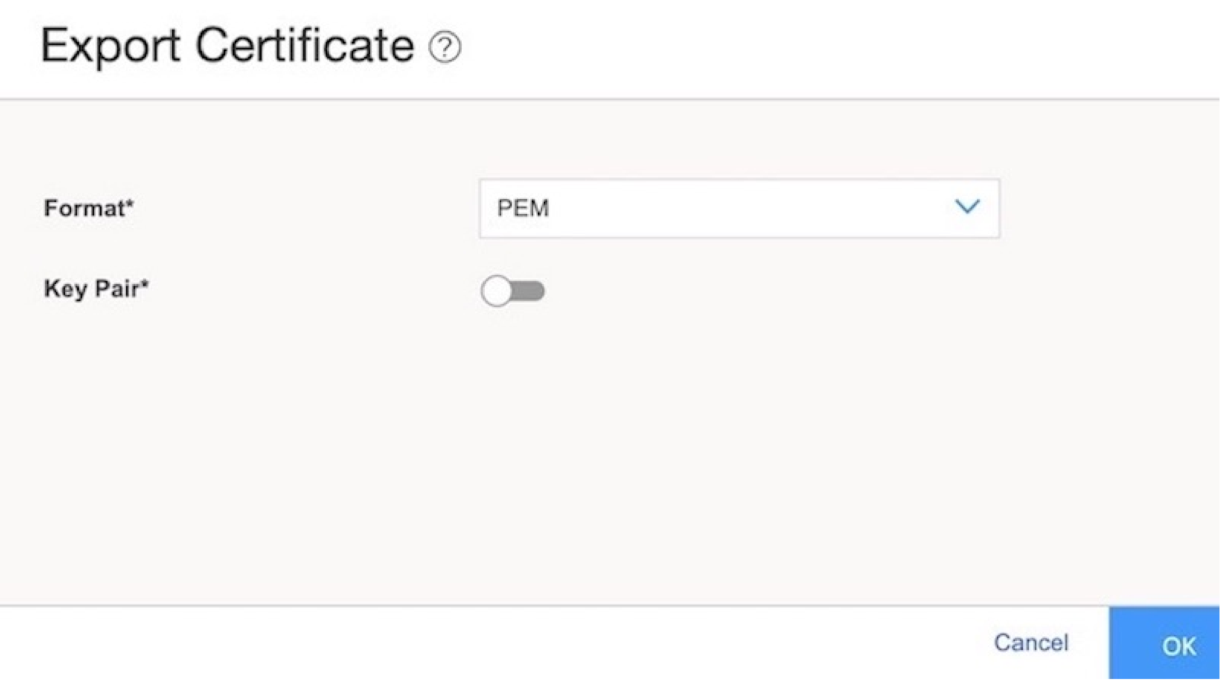
Table 4 on page 19 lists the Juniper Secure Connect application directory location where you can place the exported certificate on different platforms.

Table 4: Certificate Export File Location in Juniper Secure Connect Directory

Platform	Directory Location
Windows	**C:\ProgramData\Juniper\SecureConnect\cacerts\**
macOS	**/Library/Application Support/Juniper/SecureConnect/cacerts/**
Android	**/Juniper/Export**
iOS	**/Files/Secure Connect/**

Based on the versions of the OS and Juniper Secure Connect application, the absolute paths for the import and export locations can change. To export the certificate, select the certificate from **Device Administration** > **Certificate Management** > **Certificates** and export it.

Figure 6: Export Self-signed Certificate



Export Certificate

Format* PEM

Key Pair* ○

Configure Multiple Domains and Certificates

Juniper Secure Connect supports multiple connection profiles with different URLs in FQDN/RealmName format. To ensure that these connection requests do not show any certificate warning, as an administrator, you can bind multiple certificates to multiple domains or single certificate to multiple domains in the SRX Series Firewall. These URLs contain domain names used in connection profiles on your Juniper Secure Connect application.

In this configuration, you create multiple certificates with multiple domain names on the SRX Series Firewall.

Before you begin, as an administrator:

1. Complete the basic setup of the SRX Series Firewall.
2. Identify the domain names to be associated with Juniper Secure Connect. These are mapped to the Juniper Secure Connect Connection profiles which are URLs in FQDN or FQDN/RealmName format. See Table 5 on page 20, for the sample domain names and certificates used in this configuration.
3. If you need to map multiple domain names to a single certificate, generate the certificate externally. If you have a Let's Encrypt certificate, ensure that you generate it using Let's Encrypt server. See ACME Protocol.

Table 5: Domain Names and Certificates Mapping

Domain Name	Certificate
srx.example.com	*internal*
gateway.example.com	*external*
gateway1.example.com	*letsencrypt*
gateway2.example.com	*letsencrypt*

Configure the gateway certificates for the domain names mentioned in the URLs on your SRX Series Firewall using the configuration statements.

To configure multiple certificates and multiple domains using the CLI:

1. Log in to your SRX Series Firewall using the CLI.

2. If you need an self-signed certificate, generate a public key infrastructure (PKI) public/private key pair for a local digital certificate in the SRX Series Firewall.

```
user@host> request security pki generate-key-pair size 2048 type rsa certificate-id internal
user@host> request security pki generate-key-pair size 2048 type rsa certificate-id external
```

3. Manually generate and load self-signed certificate(s). You can also load an externally generated CA signed certificate.

```
user@host> request security pki local-certificate generate-self-signed certificate-id
internal subject DC=example.com CN=srx domain-name srx.example.com
user@host> request security pki local-certificate generate-self-signed certificate-id
external subject DC=example.com CN=gateway domain-name gateway.example.com
```

4. Enter the configuration mode.

5. Configure multiple domains using `virtual-domain` option and associate them with the corresponding certificate. Ensure to generate the certificate externally. If you have a Let's Encrypt certificate, see ACME Protocol.

```
user@host# set system services web-management https virtual-domain srx.example.com pki-local-
certificate internal
user@host# set system services web-management https virtual-domain gateway.example.com pki-
local-certificate external
```

6. Configure a certificate with multiple domain-names. Ensure that you generate these certificates separately. See ACME Protocol.

```
user@host# set system services web-management https virtual-domain gateway1.example.com pki-
local-certificate letsencrypt
user@host# set system services web-management https virtual-domain gateway2.example.com pki-
local-certificate letsencrypt
```

7. When you complete configuring the feature on your device, enter `commit` from configuration mode.

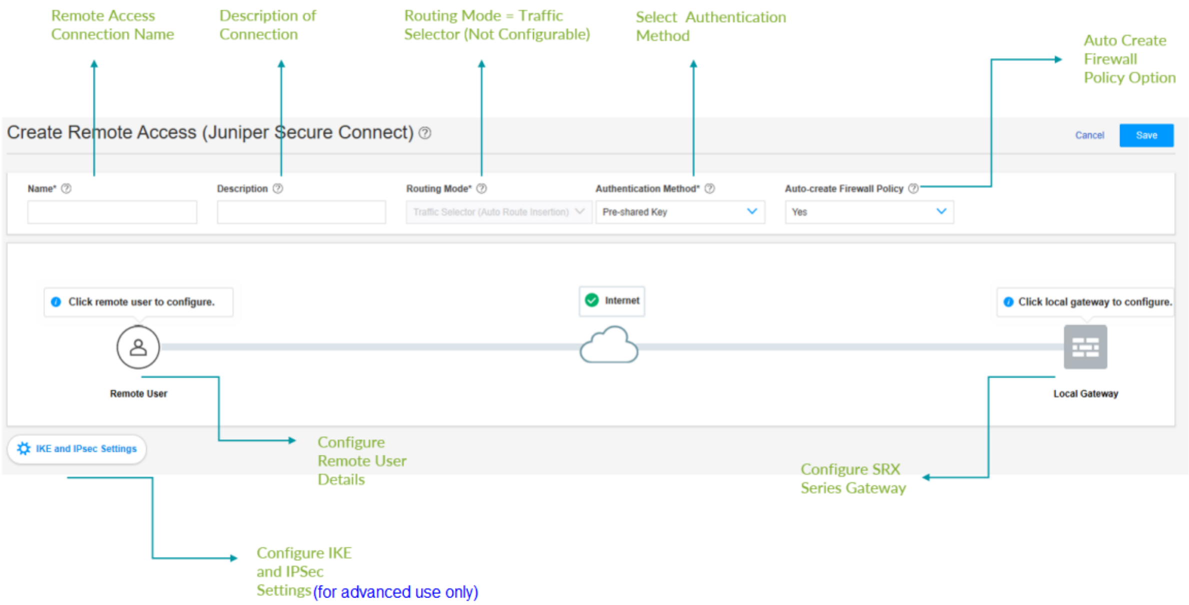
Your end users can now use the corresponding certificates to initiate a connection. This ensures that when the Juniper Secure Connect application initiates a connection, server-side certificate is validated and trusted if that corresponding certificate is loaded in the Juniper Secure Connect client.

Get Familiar with Juniper Secure Connect Wizard on J-Web

If you plan to use J-Web, get familiar with Juniper Secure Connect Wizard on J-Web. Juniper Secure Connect lets you create a remote access VPN tunnel between the remote user and the internal network in a few steps with an intuitive, easy to use VPN wizard in J-Web.

When you navigate to **VPN** > **IPsec VPN** and select **Create VPN** > **Remote Access** > **Juniper Secure Connect**, the **Create Remote Access (Juniper Secure Connect)** page appears as shown in Figure 7 on page 22.

Figure 7: J-Web Wizard for Configuring Juniper Secure Connect



Create Remote Access (Juniper Secure Connect)

Name*:

Description:

Routing Mode*: Traffic Selector (Auto Route Insertion)

Authentication Method*: Pre-shared Key

Auto-create Firewall Policy: Yes

The VPN configuration wizard allows you to configure Juniper Secure Connect in just few steps as shown in Table 6 on page 23.

Table 6: Juniper Secure Connect Configuration Wizard Fields

Options	What You Configure Here
Name	Name for the remote access connection. This name will be displayed on the Juniper Secure Connect application on remote client device when you do not select a default profile. Example: When you do not use a default profile: https://<*srx-series-device-ip-address*>/<*remote access connection name*>) When you use a default profile: https://<*srx-series-device-ip-address*>/).
Description	Description of remote access connection.
Routing Mode	Routing Mode is set to **Traffic Selector (Auto Route Insertion)** by default. You cannot change this option.
Authentication Method	Pre-shared: This authentication method is simple and easy to use, but it is less secure than the certificates. If you select pre-shared option, you can use: • Authentication with username/password using local authentication • Authentication with username/password using external authentication
	Certificate-based: This authentication method using Extensible Authentication Protocol (EAP). If you select certificate-based option, you can use: • Authentication with username/password using EAP-MSCHAPv2 • Authentication with client certificate using EAP-TLS.
Auto-create Firewall Policy	Option for auto-creating a firewall policy.

Table 6: Juniper Secure Connect Configuration Wizard Fields *(Continued)*

Options	What You Configure Here
Remote User	• Juniper Secure Connect application settings. • The settings you specify here generates a configuration file. • Facilitates auto configuration for Juniper Secure Connect remote clients when an authenticated Juniper Secure Connect application user downloads this file automatically upon connecting to the SRX Series Firewall for first time.
Local Gateway	• SRX Series Firewall settings such as interfaces, authentication options, tunnel interfaces, SSL VPN, and NAT details including the following options: • Network information to enable remote clients to connect to the gateway. • Specify how the gateway authenticates users.
IKE and IPSec	• IKE and IPSec options on the SRX Series Firewall for Juniper Secure Connect remote client connections. • IKE Settings and IPsec Settings are advanced options. J-Web is already configured with default values for IKE and IPsec fields. • IKE settings used in negotiation of authenticating the device when the Juniper Secure Connect application initiates a connection to the SRX Series Firewall. • IPsec settings specify connection settings, and security associations to govern authentication, encryption, encapsulation, and key management.

Now that you have an understanding of the configuration options. let's get started with the configuration.

Based on the authentication method you have selected, see either of these topics:

- "Local User Authentication Using Pre-shared Key" on page 164
- "External User Authentication Using RADIUS" on page 173

- "Certificate-Based Validation Using EAP-MSCHAPv2 Authentication" on page 189
- "Certificate-Based Validation Using EAP-TLS Authentication" on page 208

Gateway Certificate Warning Messages

When the user initiates a connection, the application validates whether the gateway certificate is valid. In this section, you'll see different warning messages related to the gateway certificate.

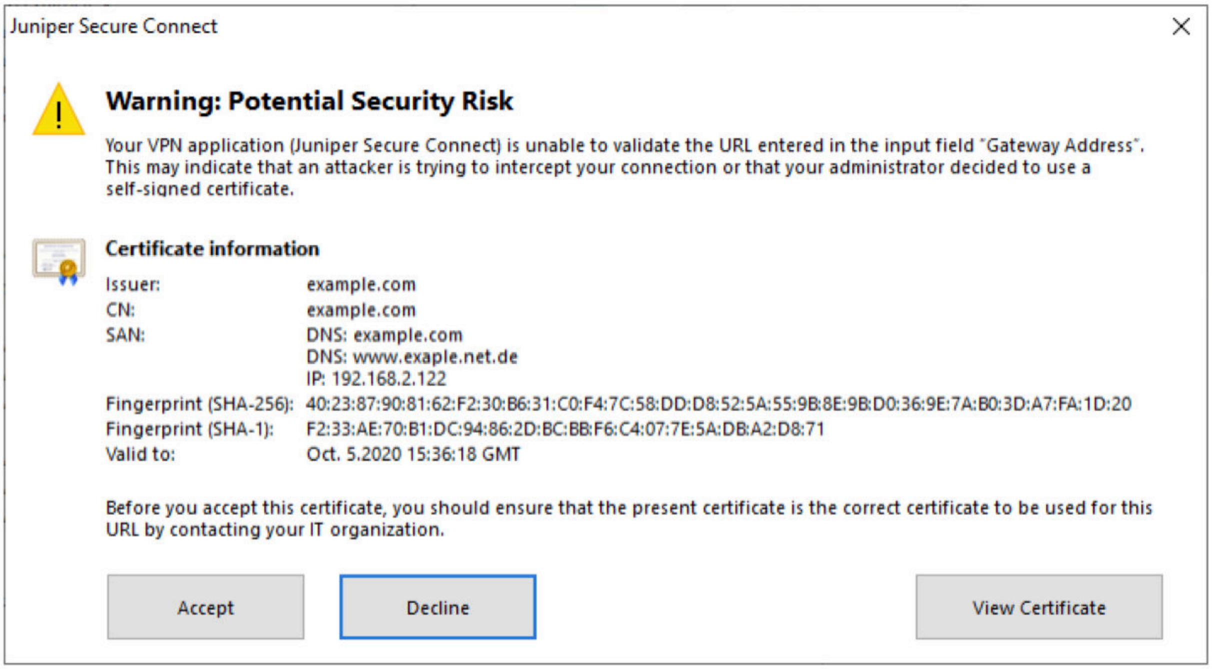
If the SRX Series Firewall has a system-generated certificate enabled, it cannot establish any connection with the application.

To know more about a valid gateway certificate, we recommend that you understand different warning messages you see on the Juniper Secure Connect application.

If the gateway uses a certificate where the root certificate has not been distributed to the application ("Create Installation Packages for Juniper Secure Connect Rollout on Windows" on page 271 and "Create Rollout Packages for Juniper Secure Connect Installation on macOS" on page 335), you will be prompted with a warning message shown in Figure 8 on page 26, Figure 9 on page 27, Figure 10 on page 28, and Figure 11 on page 29 based on the platform where the Juniper Secure Connect application is installed.

Figure 8 on page 26 is a sample warning message on Windows platform if the application does not have a root certificate.

Figure 8: Sample Certificate Warning Message on Windows Platform



Warning: Potential Security Risk

Your VPN application (Juniper Secure Connect) is unable to validate the URL entered in the input field "Gateway Address". This may indicate that an attacker is trying to intercept your connection or that your administrator decided to use a self-signed certificate.

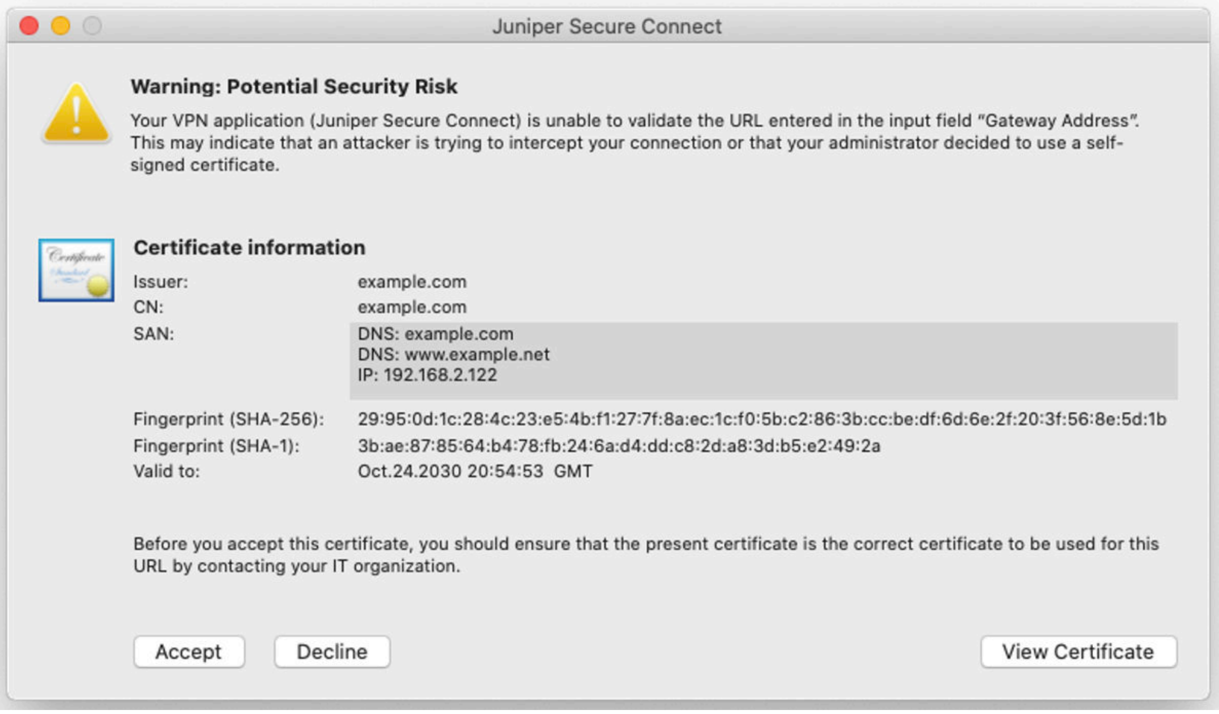
Certificate information

Issuer:	example.com
CN:	example.com
SAN:	DNS: example.com DNS: www.exaple.net.de IP: 192.168.2.122
Fingerprint (SHA-256):	40:23:87:90:81:62:F2:30:B6:31:C0:F4:7C:58:DD:D8:52:5A:55:9B:8E:9B:D0:36:9E:7A:B0:3D:A7:FA:1D:20
Fingerprint (SHA-1):	F2:33:AE:70:B1:DC:94:86:2D:BC:BB:F6:C4:07:7E:5A:DB:A2:D8:71
Valid to:	Oct. 5.2020 15:36:18 GMT

Before you accept this certificate, you should ensure that the present certificate is the correct certificate to be used for this URL by contacting your IT organization.

Figure 9 on page 27 is a sample warning message on macOS platform if the application does not have a root certificate.

Figure 9: Sample Certificate Warning Message on macOS Platform



Warning: Potential Security Risk

Your VPN application (Juniper Secure Connect) is unable to validate the URL entered in the input field "Gateway Address". This may indicate that an attacker is trying to intercept your connection or that your administrator decided to use a self-signed certificate.

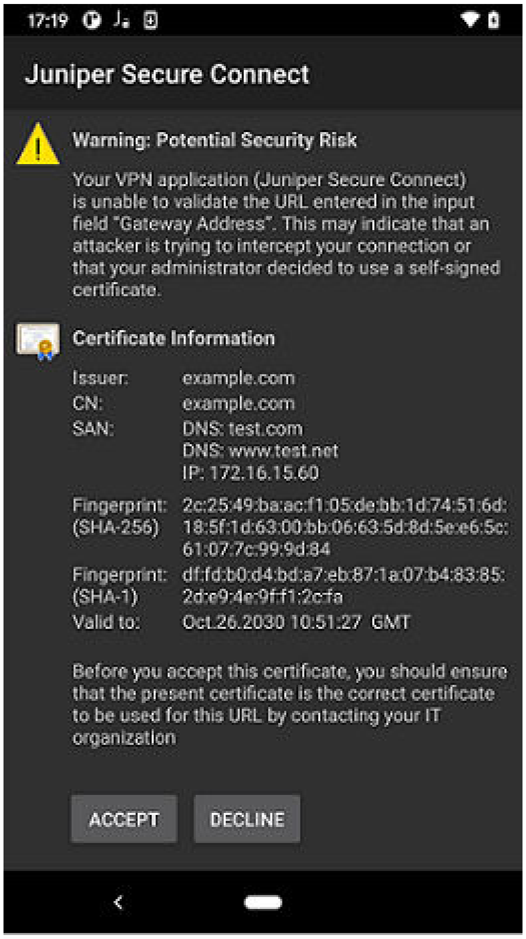
Certificate information

Issuer:	example.com
CN:	example.com
SAN:	DNS: example.com DNS: www.example.net IP: 192.168.2.122
Fingerprint (SHA-256):	29:95:0d:1c:28:4c:23:e5:4b:f1:27:7f:8a:ec:1c:f0:5b:c2:86:3b:cc:be:df:6d:6e:2f:20:3f:56:8e:5d:1b
Fingerprint (SHA-1):	3b:ae:87:85:64:b4:78:fb:24:6a:d4:dd:c8:2d:a8:3d:b5:e2:49:2a
Valid to:	Oct.24.2030 20:54:53 GMT

Before you accept this certificate, you should ensure that the present certificate is the correct certificate to be used for this URL by contacting your IT organization.

Figure 10 on page 28 is a sample warning message on Android platform if the application does not have a root certificate.

Figure 10: Sample Certificate Warning Message on Android Platform



Juniper Secure Connect

Warning: Potential Security Risk

Your VPN application (Juniper Secure Connect) is unable to validate the URL entered in the input field "Gateway Address". This may indicate that an attacker is trying to intercept your connection or that your administrator decided to use a self-signed certificate.

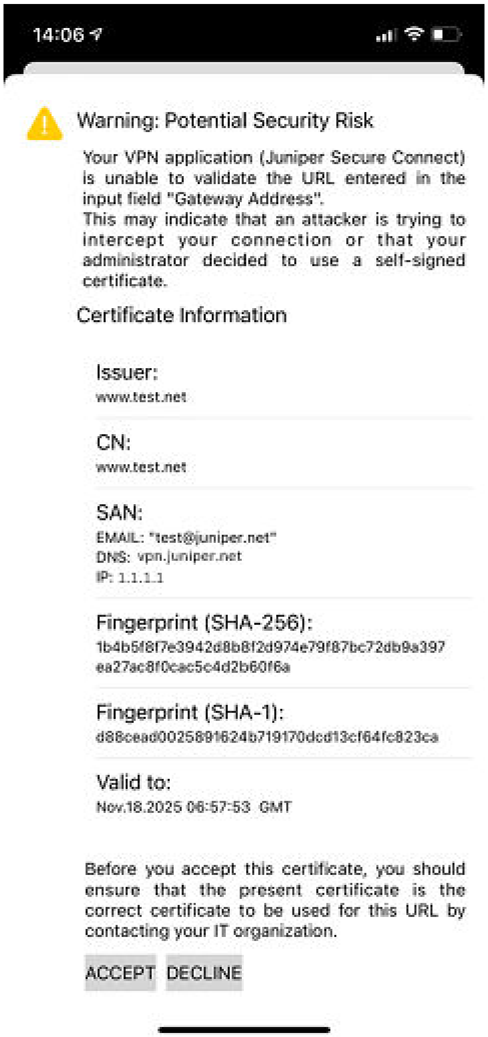
Certificate Information

Issuer:	example.com
CN:	example.com
SAN:	DNS: test.com DNS: www.test.net IP: 172.16.15.60
Fingerprint: (SHA-256)	2c:25:49:ba:ac:f1:05:de:bb:1d:74:51:6d: 18:5f:1d:63:00:bb:06:63:5d:8d:5e:e6:5c: 61:07:7c:99:9d:84
Fingerprint: (SHA-1)	df:fd:b0:d4:bd:a7:eb:87:1a:07:b4:83:85: 2d:e9:4e:9f:f1:2c:fa
Valid to:	Oct.26.2030 10:51:27 GMT

Before you accept this certificate, you should ensure that the present certificate is the correct certificate to be used for this URL by contacting your IT organization

Figure 11 on page 29 is a sample warning message on iOS platform if the application does not have a root certificate.

Figure 11: Sample Certificate Warning Message on iOS Platform



14:06

Warning: Potential Security Risk

Your VPN application (Juniper Secure Connect) is unable to validate the URL entered in the input field "Gateway Address".
This may indicate that an attacker is trying to intercept your connection or that your administrator decided to use a self-signed certificate.

Certificate Information

Issuer:
www.test.net

CN:
www.test.net

SAN:
EMAIL: "test@juniper.net"
DNS: vpn.juniper.net
IP: 1.1.1.1

Fingerprint (SHA-256):
1b4b5f8f7e3942d8b8f2d974e79f87bc72db9a397
ea27ac8f0cac5c4d2b60f6a

Fingerprint (SHA-1):
d88cead0025891624b719170dcd13cf64fc823ca

Valid to:
Nov.18.2025 06:57:53 GMT

Before you accept this certificate, you should ensure that the present certificate is the correct certificate to be used for this URL by contacting your IT organization.

The appearance of the warning message page depends on where the Juniper Secure Connect application is installed.

Details displayed on the warning message depend on the certificate that is configured on Juniper Secure Connect. Table 7 on page 29 shows the details in a sample warning message.

Table 7: Certificate Information

Certificate Information	Description
Issuer	Name of the certificate issuer.

Table 7: Certificate Information *(Continued)*

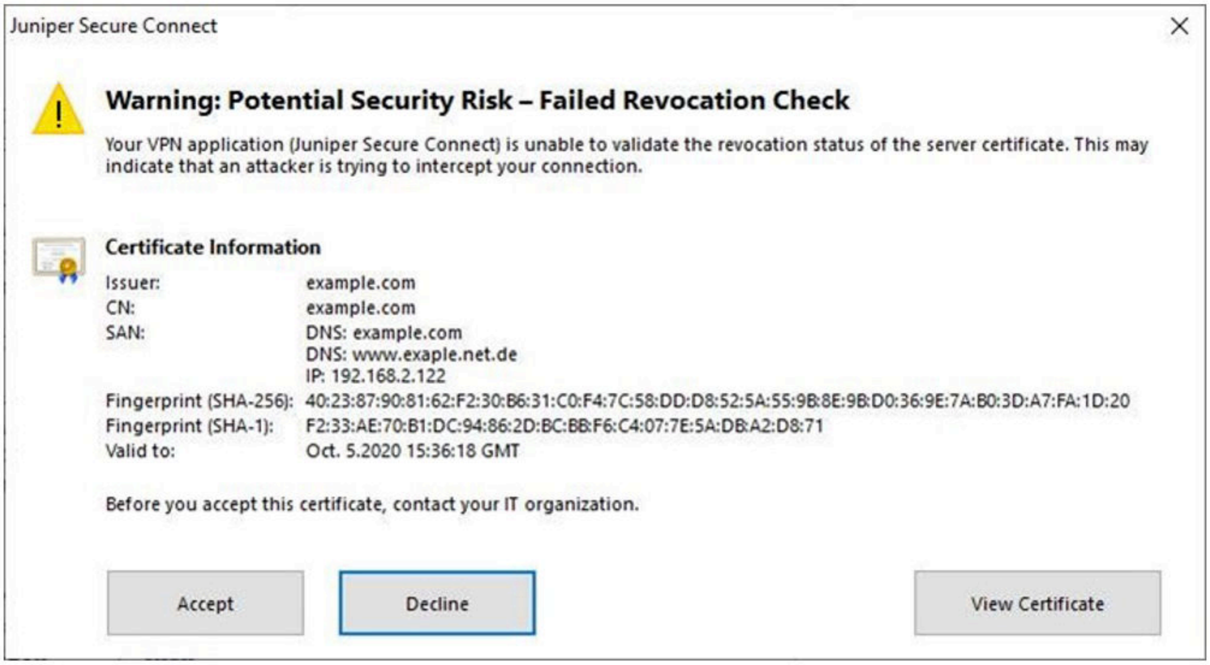
Certificate Information	Description
CN	Common name (CN) represents the subject name in the certificate.
SAN	Subject Alternative Name (SAN) represents the subject alternative name in the certificate.
Fingerprint	Represents the finger and thumbprint section in the certificate.

As a system administrator, you must inform your users what action they need to take when a warning message is displayed. The easiest way to validate your certificate as an administrator is to click on the warning message in the browser toolbar to display the certificate details as shown in Figure 4 on page 17 and Figure 5 on page 18 or load the correct root certificate on the client.

Users notice the following warning message if the application cannot reach the CRL (Certificate Revocation List) of the signed certificate loaded on the SRX Series Firewall.

WARNING: When you use a signed certificate and if the Juniper Secure Connect application cannot reach the Certificate Revocation List (CRL) to validate the gateway certificate, the application prompts the users with the warning message (as shown in Figure 12 on page 31, Figure 13 on page 31, Figure 14 on page 32, and Figure 15 on page 33) each time they connect until the CRL is accessible. Juniper Networks strongly recommends you or your user to report this error message to your IT organization to solve the CRL download failure.

Figure 12: Warning Message when Application Cannot Validate Gateway Certificate (Windows)



Warning: Potential Security Risk – Failed Revocation Check

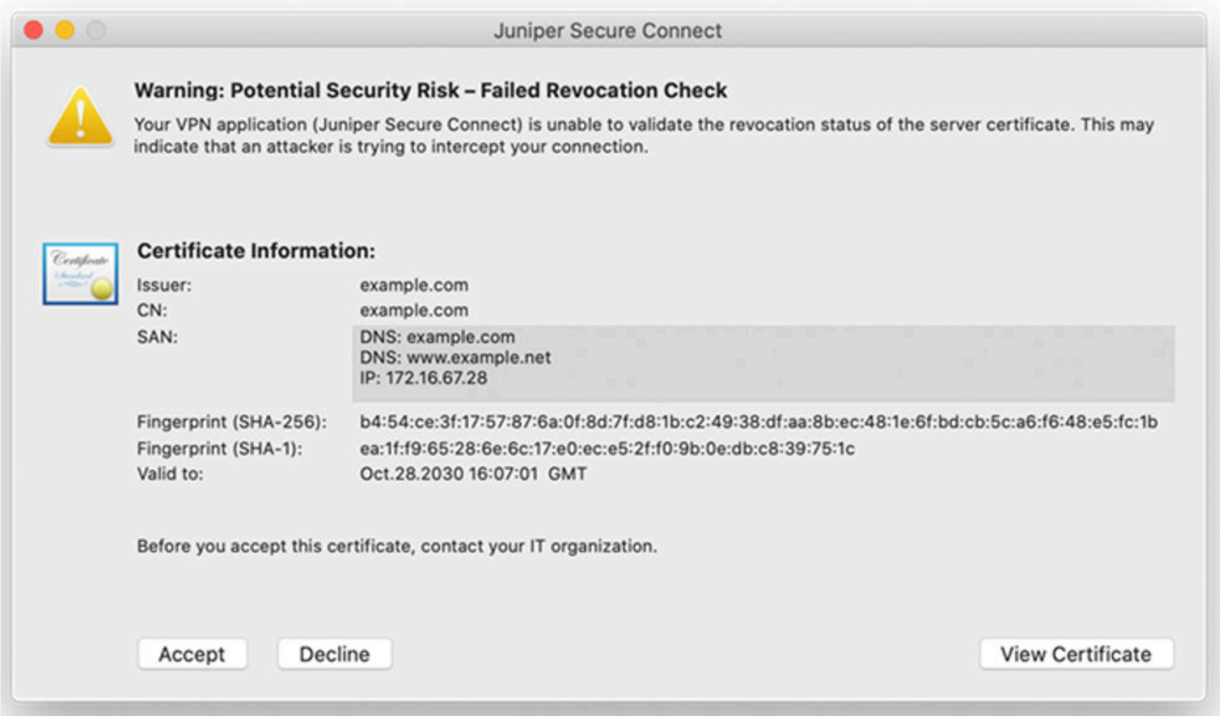
Your VPN application (Juniper Secure Connect) is unable to validate the revocation status of the server certificate. This may indicate that an attacker is trying to intercept your connection.

Certificate Information

Issuer:	example.com
CN:	example.com
SAN:	DNS: example.com DNS: www.exaple.net.de IP: 192.168.2.122
Fingerprint (SHA-256):	40:23:87:90:81:62:F2:30:B6:31:C0:F4:7C:58:DD:D8:52:5A:55:9B:8E:9B:D0:36:9E:7A:B0:3D:A7:FA:1D:20
Fingerprint (SHA-1):	F2:33:AE:70:B1:DC:94:86:2D:BC:BB:F6:C4:07:7E:5A:DB:A2:D8:71
Valid to:	Oct. 5.2020 15:36:18 GMT

Before you accept this certificate, contact your IT organization.

Figure 13: Warning Message when Application Cannot Validate Gateway Certificate (macOS)



Warning: Potential Security Risk – Failed Revocation Check

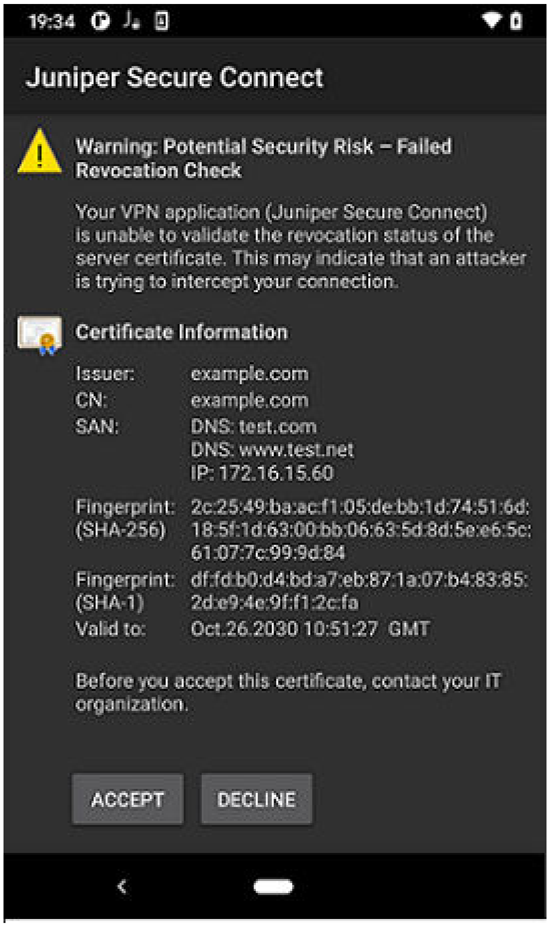
Your VPN application (Juniper Secure Connect) is unable to validate the revocation status of the server certificate. This may indicate that an attacker is trying to intercept your connection.

Certificate Information:

Issuer:	example.com
CN:	example.com
SAN:	DNS: example.com DNS: www.example.net IP: 172.16.67.28
Fingerprint (SHA-256):	b4:54:ce:3f:17:57:87:6a:0f:8d:7f:d8:1b:c2:49:38:df:aa:8b:ec:48:1e:6f:bd:cb:5c:a6:f6:48:e5:fc:1b
Fingerprint (SHA-1):	ea:1f:f9:65:28:6e:6c:17:e0:ec:e5:2f:f0:9b:0e:db:c8:39:75:1c
Valid to:	Oct.28.2030 16:07:01 GMT

Before you accept this certificate, contact your IT organization.

Figure 14: Warning Message when Application Cannot Validate Gateway Certificate (Android)



Juniper Secure Connect

Warning: Potential Security Risk – Failed Revocation Check

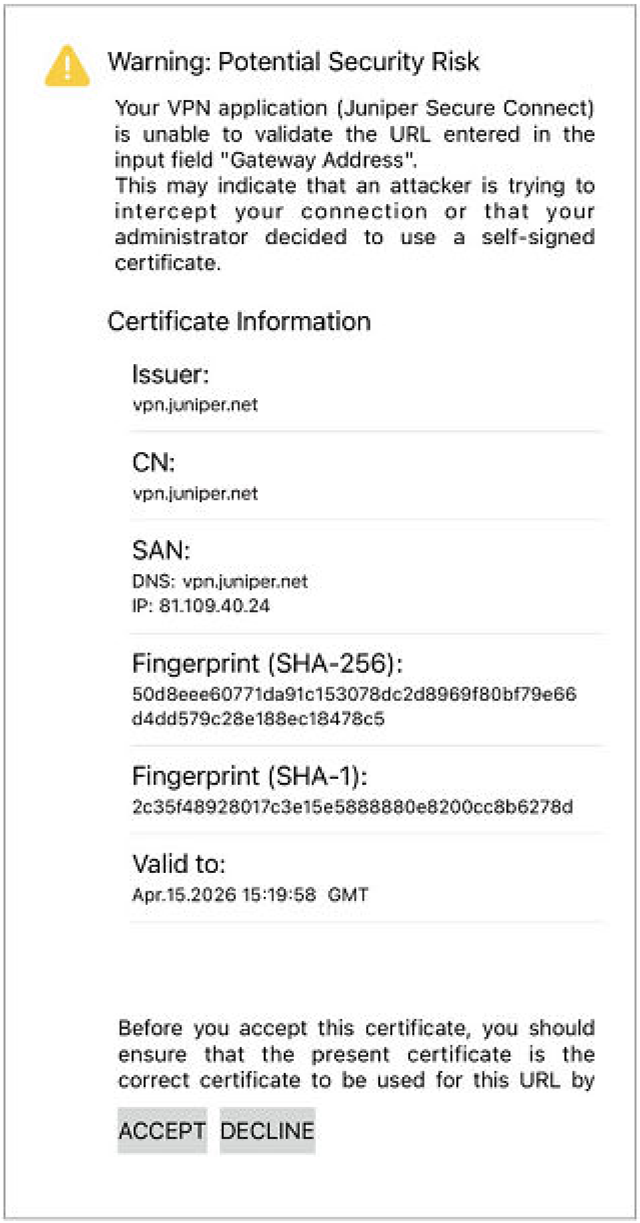
Your VPN application (Juniper Secure Connect) is unable to validate the revocation status of the server certificate. This may indicate that an attacker is trying to intercept your connection.

Certificate Information

Issuer:	example.com
CN:	example.com
SAN:	DNS: test.com DNS: www.test.net IP: 172.16.15.60
Fingerprint: (SHA-256)	2c:25:49:ba:ac:f1:05:de:bb:1d:74:51:6d: 18:5f:1d:63:00:bb:06:63:5d:8d:5e:e6:5c: 61:07:7c:99:9d:84
Fingerprint: (SHA-1)	df:fd:b0:d4:bd:a7:eb:87:1a:07:b4:83:85: 2d:e9:4e:9f:f1:2c:fa
Valid to:	Oct.26.2030 10:51:27 GMT

Before you accept this certificate, contact your IT organization.

Figure 15: Warning Message when Application Cannot Validate Gateway Certificate (iOS)



Warning: Potential Security Risk

Your VPN application (Juniper Secure Connect) is unable to validate the URL entered in the input field "Gateway Address".
This may indicate that an attacker is trying to intercept your connection or that your administrator decided to use a self-signed certificate.

Certificate Information

Issuer:
vpn.juniper.net

CN:
vpn.juniper.net

SAN:
DNS: vpn.juniper.net
IP: 81.109.40.24

Fingerprint (SHA-256):
50d8eee60771da91c153078dc2d8969f80bf79e66
d4dd579c28e188ec18478c5

Fingerprint (SHA-1):
2c35f48928017c3e15e5888880e8200cc8b6278d

Valid to:
Apr.15.2026 15:19:58 GMT

Before you accept this certificate, you should ensure that the present certificate is the correct certificate to be used for this URL by

RELATED DOCUMENTATION

Juniper Secure Connect Overview | 1

3

CHAPTER

Authentication in Juniper Secure Connect

SUMMARY

Read this topic to know more about different user authentication methods in Juniper Secure Connect.

IN THIS CHAPTER

Users can establish secure connectivity with Juniper Secure Connect either through local or external authentication. Both methods have the following certain restrictions:

- Local Authentication—In local authentication, the SRX Series Firewall validates the user credentials by checking them in the local database. In this method, the administrator can change or reset passwords. Users must remember the new password. This is not a preferred authentication method as it is not secure.

- External Authentication—In this method, users can authenticate with the same credentials that they use to access other resources on the network. In many cases, user credentials are the same as domain login credentials used for Active Directory or any other Lightweight Directory Access Protocol (LDAP) authentication system. This method simplifies user experience and improves the organization's security posture because you can maintain the authorization system with the regular security policy used by your organization.

  - Multi Factor Authentication—To add an extra layer of protection, you can also enable Multi Factor Authentication (MFA). In this method, a RADIUS proxy is used to send a notification message to a device such as the users' smart phone. Users must accept the notification message to complete the connection. See KB Article 73468.

  - LDAP Authentication using Juniper Secure Connect—Starting with Junos OS Release 23.1R1, we've introduced group-based controlled LDAP authorization. You can use LDAP to define one or more LDAP groups. Use the `allowed-groups` statement at the `[edit access ldap-options]` hierarchy level to specify the list of groups that LDAP authenticates. A user can belong to multiple LDAP groups. You can map the group to an address pool. Based on the LDAP group membership, the system assigns an IP addresses to the user.

  - SAML-based Authentication—SAML is an XML-based framework where the two parties, the identity provider (IdP) and the service provider, exchange identity information about the remote user. SAML enables Single Sign-On (SSO), allowing users to log in once and then seamlessly access multiple applications without having to reenter their credentials each time.

Table 8 on page 36 compares different authentication methods in Juniper Secure Connect.

Table 8: Juniper Secure Connect Authentication Types

Authentication Methods	Credentials (Username and Password)	End-User Certificate	Local Authentication	External Authentication Radius	External Authentication LDAP	External Authentication IdP
IKEv1 - pre-shared-key	Yes	No	Yes	Yes	Yes	No

Table 8: Juniper Secure Connect Authentication Types *(Continued)*

Authentication Methods	Credentials (Username and Password)	End-User Certificate	Local Authentication	External Authentication Radius	External Authentication LDAP	External Authentication IdP
IKEv2-EAP-MSCHAPv2	Yes	No	No	Yes	No	No
IKEv2-EAP-TLS	No	Yes	No	Yes	No	No
SAML-based Authentication (Proprietary IKEv2-EAP implementation)	Username only	No	No	No	No	Yes

Regardless of the authentication method, you can continue to use the username and password for external user authentication using the RADIUS server to download the initial configuration, even when implementing EAP-TLS authentication.

See the following topics to configure user authentication for Juniper Secure Connect.

- CLI Procedures
  - "Local User Authentication Using Pre-shared Key (CLI Procedure)" on page 74
  - "External User Authentication (CLI Procedure)" on page 91
  - "Example: Configuring LDAP Authentication for Juniper Secure Connect (CLI Procedure)" on page 109
  - "Certificate-Based Validation Using EAP-MSCHAPv2 Authentication (CLI Procedure)" on page 127
  - "Certificate-Based Validation Using EAP-TLS Authentication (CLI Procedure)" on page 145
- J-Web Procedures
  - "Local User Authentication Using Pre-shared Key" on page 164
  - "External User Authentication Using RADIUS" on page 173

- "Certificate-Based Validation Using EAP-MSCHAPv2 Authentication" on page 189
- "Certificate-Based Validation Using EAP-TLS Authentication" on page 208

RELATED DOCUMENTATION

Get Started with Juniper Secure Connect | 10

SAML Authentication in Juniper Secure Connect

SUMMARY

Read this topic to learn about Security Assertion Markup Language (SAML) based user authentication in Juniper Secure Connect.

IN THIS SECTION

SAML Overview

Security Assertion Markup Language (SAML) is an XML-based framework for exchanging authentication and authorization data between the service provider (SP) and the identity provider (IdP). SAML enables Single Sign-On (SSO) that allows users to log in once and then seamlessly access multiple applications without having to reenter their credentials each time.

Juniper Secure Connect supports remote user authentication using SAML version 2 (SAML 2.0). When you run a VPN service using the iked process, the SRX Series Firewalls supports this feature.

SAML Components for Juniper Secure Connect

Following are the key components in SAML for Juniper Secure Connect:

- Principal (User)—The user who requests for services such as the remote access VPN connection. Any remote user of the Juniper Secure Connect is the Principal. The browser available on the user's device (such as a Windows laptop) is used as an agent for SSO.

- Identity Provider (IdP)—The entity that authenticates users and provides identity assertions to the service provider. The IdP generates an authentication assertion to indicate that the user has been authenticated. Okta and Microsoft Azure are examples for IdPs.

- Service Provider (SP) —Entity that provides the service to the user. It relies on the assertions from the IdP to grant access to the user. In Juniper Secure Connect, the SRX Series Firewall functions as the SP delivering remote access VPN service.

- SAML Assertion—An XML-based message that carries user's authentication and authorization information. Assertions are used to transfer user identity information from the IdP to the SP.

- SAML Binding—Defines how the SAML messages are transmitted between the IdP and SP. SRX Series Firewall supports SP initiated SSO profile over HTTP Redirect and HTTP POST bindings.

- SAML Metadata—An XML-based data that describe the IdP and SP attributes such as entity ID, certificates, bindings, URLs, and so on. These entities interact with each other. SRX Series Firewalls allow you to import the IdP metadata and export SP metadata.

Table 9 on page 39 shows the list of SAML feature support in SRX Series Firewall.

Table 9: SAML Support in SRX Series Firewall

SAML Features	Support
SAML Version	• SAML 2.0 Not compatible with SAMLv1.
SAML Profiles	• Web SSO: Service provider-initiated SSO profile • SingleLogout: Service provider receives the user logout request and sends the logout response only to the IdP. Service provider doesn’t generate or send user logout request to IdP.
SAML Bindings	• HTTP Redirect: Service provider to IdP messages such as the authentication request and logout response use HTTP Redirect. • HTTP POST: Service provider accepts messages from IdP such as the logout request and assertion response using HTTP POST.

Table 9: SAML Support in SRX Series Firewall *(Continued)*

SAML Features	Support
Service Provider Hash Algorithms	• SHA-256, SHA-384, SHA-512 Default is SHA-256.
Assertion-cache	• Yes. The firewall can use the same assertion cache later for user authentication.
Support for High Availability	• Chassis cluster (L2 HA) • Multinode High Availability (L3 HA) No high availability support for authentication sessions that are in progress.

Benefits

- Improved user experience—SAML provides SSO capabilities in multi-application access scenarios. With a single login, in-addition to Juniper Secure Connect, you can connect to multiple applications offered by different service providers. You don't need to enter different credentials for different applications.

- Enhanced security—SAML provides enhanced security for the Juniper Secure Connect remote user by providing single point of authentication using a secure IdP. SAML doesn't share user credentials with the service provider. SAML transfers only the identity information to the service provider ensuring that the credentials are sent only to the IdP and not each and every service provider.

- Easy integration—As an open standard, SAML facilitates easy integration with any IdP for Juniper Secure Connect remote user authentication.

- Reduced cost—SAML allows the service provider to reduce the cost of maintaining multiple user account details.

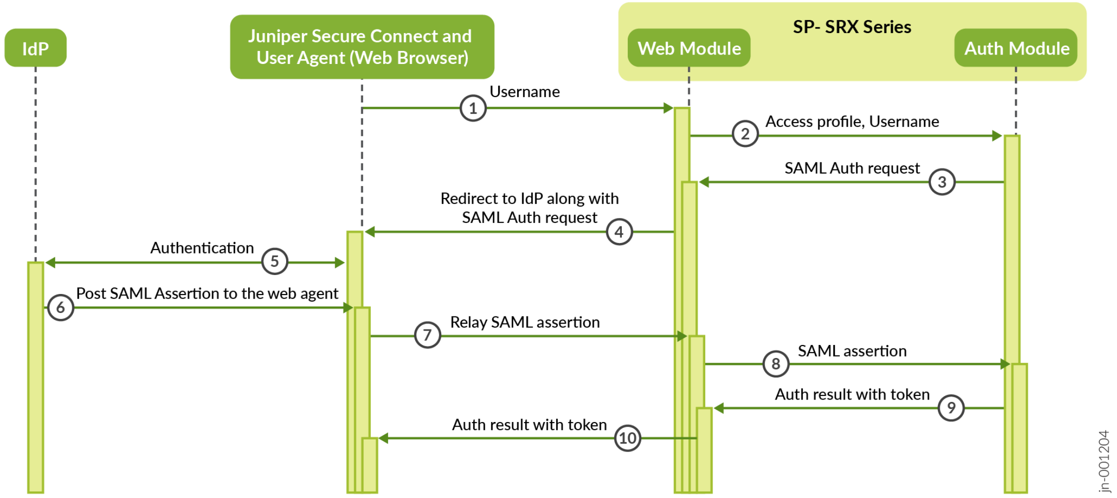
How SAML Works in Juniper Secure Connect

Consider the following points when configuring remote user authentication using SAML for Juniper Secure Connect.

- When you choose SAML for remote user authentication in Juniper Secure Connect, ensure you have an agreement with the IdP. You must be aware about the configuration settings related to the IdP that the service provider should be aware of.
- Set SAML as the authentication method for the access profile. See *authentication-order (Access Profile)*.
- Configure the SAML access parameters such as Identity Provider (IdP) and Service Provider (SP) settings. See *saml*.
- Specify the SAML settings for the access profile. See *saml (Access Profile)*.
- If you prefer not to cache SAML assertions from the IdP, set the preference in the SAML options. See *saml-options*.
- To authenticate Juniper Secure Connect remote user with SAML, both the remote access VPN profile and the IKE gateway AAA access profiles should be SAML-based.

Figure 16 on page 41 illustrates the SAML-based user authentication workflow in Juniper Secure Connect.

Figure 16: SAML Authentication Workflow with Juniper Secure Connect


IdP
Juniper Secure Connect and User Agent (Web Browser)
SP- SRX Series
Web Module
Auth Module
1 Username
2 Access profile, Username
3 SAML Auth request
4 Redirect to IdP along with SAML Auth request
5 Authentication
6 Post SAML Assertion to the web agent
7 Relay SAML assertion
8 SAML assertion
9 Auth result with token
10 Auth result with token
jn-001204

1. Juniper Secure Connect remote user sends a connection request to the SRX Series Firewalls, specifying a particular username and connection profile.

2. SRX Series Firewall checks the access profile to determine if the profile uses SAML as an authentication method. An access profile can contain multiple IdPs for different domains. The user's domain determines the selection of the IdP. For example, if the username is user1@domain1 and domain1 is configured within the access profile, the firewall selects the corresponding IdP for domain1. If domain1 is not configured, the firewall uses the IdP configured under the `any` domain. Similarly, if the username doesn't contain an email format, such as user1, the firewall selects the IdP configured under the `any` domain by default.

3. The firewall sends the SAML authentication request to Juniper Secure Connect.

4. Juniper Secure Connect launches a web-browser (user-agent) and redirects the SAML authentication request to the IdP.

5. The IdP authenticates the user.

6. If the authentication is successful, the IdP sends SAML assertion using an HTTP POST request.

7. The web-browser relays the SAML assertion to the SRX Series Firewall.

8. The SRX Series Firewall receives the SAML assertion and validates it.

9. When the SAML assertion is valid, the firewall sends the authentication result along with a valid SAML assertion token to Juniper Secure Connect.

Juniper Secure Connect establishes remote access VPN tunnel with the SRX Series Firewall after the SAML authentication.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
24.4R1	We've introduced support for SAML-based user authentication for Juniper Secure Connect in Junos OS Release 24.4R1.

RELATED DOCUMENTATION

Authentication in Juniper Secure Connect | 34

authentication-order (Access Profile)

saml

saml (Access Profile)

Configure SAML Authentication (CLI Procedure)

SUMMARY

In this configuration, you'll learn to setup Security Assertion Markup Language (SAML) based user authentication in Juniper Secure Connect.

IN THIS SECTION

Juniper Secure Connect supports remote user authentication using SAML v2 (SAML 2.0). In this configuration example, the SRX Series Firewall servers as the SAML service provider and authenticates the Juniper Secure Connect users using SAML IdP.

TIP:

Table 10: Readability Score and Time Estimates

Reading Time	Less than an hour
Configuration Time	Less than an hour

Example Prerequisites

Ensure you meet the following prerequisites:

- Understand the following main components in the example.

  - An active identity provider (IdP) user account. Okta and Microsoft Azure are examples of IdPs.

    In this example, we've used Okta as the IdP. For IdP settings, see "Functional Overview" on page 46. The step-by-step SAML 2.0 IdP configuration is out-of-scope of this documentation. The settings depend on your agreement with the IdP.

  - An SRX Series Firewall that acts a service provider (SP).

    This topic covers step-by-step configuration of SRX Series Firewall for SAML-based user authentication. See "Functional Overview" on page 46 and "Step-By-Step Configuration on vSRX" on page 52

  - Juniper Secure Connect application for Windows that supports SAML-based user authentication.

    See Juniper Secure Connect for Windows.

- Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

- Ensure that you've an account with your IdP before configuring the service provider. Confirm you've configured all necessary settings in your IdP application. Take a note of the following items on your IdP account:

  - Note the IdP entity ID.

  - Note the single sign-on (SSO) URL.

  - Note the single logout URL.

  - Download the signing certificate from the IdP and load it to the firewall.

    ```
    user@vsrx> request security pki ca-certificate load filename /<local-directory-path>/<idp-cert-filename> ca-profile <ca-profile-name>
    ```

    The example includes EXAMPLE-CA as the *ca-profile-name*.

  - Ensure you've created users in your IdP application.

- Ensure the firewall, which is the service provider, can reach the IdP SSO and single logout URLs using the Internet-facing interface.

- Ensure you've created the firewall (server-side) self-signed certificates for web-management and SSL profile. You can also use CA-signed certificates.
- Ensure you've CA-signed certificate for IKE.

Table 11: Hardware and Software Requirements

Hardware requirements	• One SRX Series Firewall that supports the feature. • Windows laptop with the latest Juniper Secure Connect application installed.
Software requirements	• Junos OS Release that supports the feature with `junos-ike` package to run VPN service with the iked process. • IdP details mentioned in the "Example Prerequisites" on page 44. In this example, we've used Okta as the IdP.

Before You Begin

Table 12: Resources, and Additional Information

Understand SAML for Juniper Secure Connect	• Understand how SAML works in Juniper Secure Connect. See SAML Authentication in Juniper Secure Connect. • Understand the Juniper Secure Connect application support. See Juniper Secure Connect Release Notes.
Know more	Learn about Junos configuration statements and CLI commands for SAML. See saml, authentication-order (access-profile), saml (Access Profile), saml-options, show network-access aaa saml assertion-cache, show network-access aaa statistics, request network-access aaa saml load-idp-metadata, request network-access aaa saml export-sp-metadata, clear network-access aaa saml assertion-cache, clear network-access aaa saml idp-metadata, and clear network-access aaa statistics

Functional Overview

Table 13: Functional Overview

Functional Component	Details
Certificates	
Self-signed certificate or CA-signed certificate for web-management	*jsc-web* is the PKI local certificate for web-authentication.
Self-signed certificate or CA-signed certificate for SSL profile	*jsc* is the server-side certificate for SSL profile.
CA-signed certificate for IKE	*IKE-CERT* is the signed-certificate for IKE. Use the CA certificate in the client laptop where you've installed your Juniper Secure Connect application.
Signed-certificate from IdP	SAML IdP certificate, *EXAMPLE-CA* is the signing certificate downloaded from IdP and copied to the firewall.
IKE	
IKE proposal	*JSC-IKE-PRO* is the IKEv2 proposal that defines the algorithms and keys used to establish the secure IKE connection with Juniper Secure Connect application.
IKE policy	*JSC-IKE-POL* is the IKEv2 policy that defines the IKE proposal to be used during IKE negotiation.
IKE gateway	*JSC-GW* is the IKEv2 gateway that uses the IKE policy. In Juniper Secure Connect, associate the IKE gateway with the access profile and the TCP encapsulation profile. We've used *example.com* as the IKE gateway domain name
IPsec	

Table 13: Functional Overview *(Continued)*

Functional Component	Details
IPsec proposal	*JSC-IPSEC-PRO* is the IPsec proposal that defines the IPsec protocol and algorithms used to establish the secure IKE connection with Juniper Secure Connect application.
IPsec policy	*JSC-IPSEC-POL* is the IPsec policy that defines the IPsec proposal to be used during IPsec negotiation.
SAML Access Profile	
SAML Authentication Order	The access profile *JSC-ACCESS* defines `saml` as the authentication method. It contains the address pool details for the Juniper Secure Connect and the associated SAML service provider name and IdP domain details.
SAML IdP	
SAML IdP name	*example-idp* is the name of the IdP used in this example. We've used *example.org* as the IdP domain name.
SAML IdP Entity ID	*http://www.example.org/abcd1234* is the unique entity which is a URI that identifies the IdP. The metadata XML file has the IdP entity-id information. Use it in the *entity-id* option at [`edit access saml identity-provider` *name* `settings`] hierarchy level.
SAML login URL	*https://5075942.example.org/app/5075942_srx1examplenet_1/abcd1234/sso/saml* is the single-signon-url on available on the IdP. Use it in the *single-signon-url-name* option at [`edit access saml identity-provider` *name* `settings signle-signon-url` *signle-signon-url*] hierarchy level.
SAML logout URL	*https://5075942.example.org* is the single-logout-url on available on the IdP. Use it in the *single-logout-url-name* option at [`edit access saml identity-provider` *name* `settings single-logout-url`] hierarchy level.

Table 13: Functional Overview *(Continued)*

Functional Component	Details
SAML IdP certificate	`EXAMPLE-CA` is the signing certificate available on the IdP. The SAML service provider uses this IdP certificate validating its users. Use it in the *idp-certificate-name* option at `[edit access saml identity-provider name settings idp-certificate]` hierarchy level.
SAML user attributes	*user1*, who is the Principal, requests access. SAML user attributes are name-value pairs that are IdP attributes. These attributes include user information such as firstname, lastname, or email configured on the IdP. The IdP sends this information to the service provider through the SAML assertion. During the firewall configuration, specify whether an attribute related to the Principal is mandatory or optional.
SAML service provider	
SAML service provider name	`vsrx-jsc` is the name of the service provider used in this example. We've used `example.net` as the service provider domain name for SAML.
SAML service provider Entity ID	`https://srx1.example.net` is the unique entity which is a URI that identifies the service provider. Use it in the *entity-id* option at `[edit access saml service-provider name]` hierarchy level. **TIP**: SAML domain names are case-sensitive. `Example.net` is different from `example.net` in SAML.
Remote Access	
Profile	`jsc-saml` is the remote access VPN profile with IPsec VPN, user access profile, and Secure Connect client configuration settings.
SSL	
Termination profile	`JSC-SSL-PRO` is the SSL termination profile for the remote access IPsec traffic encapsulation into a TLS connection.

Table 13: Functional Overview *(Continued)*

Functional Component	Details
Security Zones	
trust	Network segment facing the corporate resources such as the server.
untrust	Network segment facing the Internet. Note that IdP is reachable through this segment.
VPN	Network segment with the secure tunnel interface st0.0.

Table 13: Functional Overview *(Continued)*

Functional Component	Details
Security Policy	Allows you to select the type of data traffic. - *JSC-ALLOW-OUT*—Permits traffic from the trust zone to the vpn zone, where the match criteria is: - source-address: any - destination-address: any - application: any - *JSC-ALLOW-IN*—Permits traffic from the vpn zone to the trust zone, where the match criteria is: - source-address: any - destination-address: any - application: any - `default-permit`—Permits traffic from the trust zone to the trust zone, where the match criteria is: - source-address: any - destination-address: any - application: any - `default-permit`—Permits traffic from the trust zone to the untrust zone, where the match criteria is: - source-address: any - destination-address: any - application: any
Source NAT	Source NAT to allow traffic from the VPN client to reach the internal server.

Topology Overview

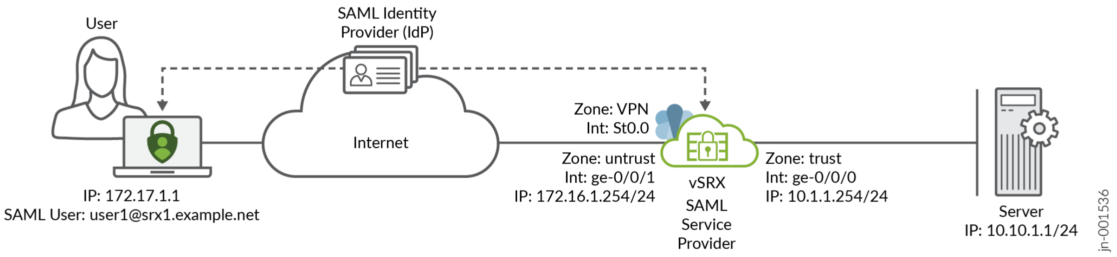
In this example, the Juniper Secure Connect client initiates remote access VPN connection establishment with the firewall, vSRX. The firewall sends SAML authentication request to Juniper Secure Connect which checks with the IdP for the user authentication. Once authentication completes, the firewall confirms the SAML assertion, and establishes remote access VPN tunnel.

Table 14: Topology Overview

Hostname	Role	Function
vsrx	• Remote access VPN server • SAML service provider	• In Juniper Secure Connect, the firewall establishes the remote access VPN tunnels. • In Juniper Secure Connect SAML-based user authentication, the firewall functions as the SAML service provider delivering remote access VPN service. This service provider relies on the IdP's assertions to grant user access.
Client	Remote access VPN client	In Juniper Secure Connect, a laptop or computer using the Juniper Secure Connect application initiates a VPN connection with the firewalls.
IdP	SAML IdP	In Juniper Secure Connect, the IdP authenticates users and provides identity assertions to the service provider. The IdP generates an authentication assertion to confirm user authentication. Okta serves as the IdP in this example.
Server	Server in the trust zone	The Juniper Secure Connect client tries to access the internal corporate server.

Topology Illustration

Figure 17: SAML-Based User Authentication in Juniper Secure Connect



Step-By-Step Configuration on vSRX

NOTE: For complete sample configurations on the DUT, see:

- "Appendix 2: Set Commands on vSRX" on page 63
- "Appendix 3: Show Configuration Output on vSRX" on page 66

This configuration is applicable for only vSRX. You must make the appropriate device-specific configuration changes.

1. Configure interfaces.

```
[edit]
user@vsrx# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.254/24
user@vsrx# set interfaces st0 unit 0 family inet
user@vsrx# set interfaces ge-0/0/1 unit 0 family inet address 172.16.1.254/24
```

2. Configure security zones.

```
[edit security zones]
user@vsrx# set security-zone trust host-inbound-traffic system-services all
user@vsrx# set security-zone trust host-inbound-traffic protocols all
user@vsrx# set security-zone trust interfaces ge-0/0/0.0
user@vsrx# set security-zone untrust host-inbound-traffic system-services all
```

```
user@vsrx# set security-zone untrust host-inbound-traffic protocols all
user@vsrx# set security-zone untrust interfaces ge-0/0/1.0
user@vsrx# set security-zone VPN interfaces st0.0
```

3. Configure security policies.

```
[edit security policies]
user@vsrx# set from-zone trust to-zone trust policy default-permit match source-address any
user@vsrx# set from-zone trust to-zone trust policy default-permit match destination-
address any
user@vsrx# set from-zone trust to-zone trust policy default-permit match application any
user@vsrx# set from-zone trust to-zone trust policy default-permit then permit
user@vsrx# set from-zone trust to-zone untrust policy default-permit match source-address
any
user@vsrx# set from-zone trust to-zone untrust policy default-permit match destination-
address any
user@vsrx# set from-zone trust to-zone untrust policy default-permit match application any
user@vsrx# set from-zone trust to-zone untrust policy default-permit then permit
user@vsrx# set from-zone trust to-zone VPN policy JSC-ALLOW-OUT match source-address any
user@vsrx# set from-zone trust to-zone VPN policy JSC-ALLOW-OUT match destination-address
any
user@vsrx# set from-zone trust to-zone VPN policy JSC-ALLOW-OUT match application any
user@vsrx# set from-zone trust to-zone VPN policy JSC-ALLOW-OUT then permit
user@vsrx# set from-zone VPN to-zone trust policy JSC-ALLOW-IN match source-address any
user@vsrx# set from-zone VPN to-zone trust policy JSC-ALLOW-IN match destination-address any
user@vsrx# set from-zone VPN to-zone trust policy JSC-ALLOW-IN match application any
user@vsrx# set from-zone VPN to-zone trust policy JSC-ALLOW-IN then permit
```

4. Configure source NAT.

```
[edit security nat]
user@vsrx# set source rule-set JSC-NAT from zone VPN
user@vsrx# set source rule-set JSC-NAT to zone trust
user@vsrx# set source rule-set JSC-NAT rule 1 match source-address 0.0.0.0/0
user@vsrx# set source rule-set JSC-NAT rule 1 then source-nat interface
```

5. Configure certificates.

```
[edit security pki]
user@vsrx# set ca-profile EXAMPLE-CA ca-identity EXAMPLE-CA
user@vsrx# set ca-profile EXAMPLE-CA revocation-check disable
```

```
user@vsrx# set ca-profile CERTAUTH ca-identity CERTAUTH
user@vsrx# set ca-profile CERTAUTH revocation-check disable
```

6. Configure web-management.

```
[edit system services]
user@vsrx# set web-management https pki-local-certificate jsc-web
```

7. Configure IKE proposal.

```
[edit security ike]
user@vsrx# set proposal JSC-IKE-PRO authentication-method rsa-signatures
user@vsrx# set proposal JSC-IKE-PRO dh-group group19
user@vsrx# set proposal JSC-IKE-PRO authentication-algorithm sha-256
user@vsrx# set proposal JSC-IKE-PRO encryption-algorithm aes-256-cbc
```

8. Configure IKE policy.

```
[edit security ike]
user@vsrx# set policy JSC-IKE-POL proposals JSC-IKE-PRO
user@vsrx# set policy JSC-IKE-POL certificate local-certificate IKE-CERT
```

9. Configure IKE gateway.

   a. Configure IKE gateway options.

```
[edit security ike]
user@vsrx# set gateway JSC-GW dynamic user-at-hostname "ra@example.com"
user@vsrx# set gateway JSC-GW dynamic ike-user-type shared-ike-id
user@vsrx# set gateway JSC-GW ike-policy JSC-IKE-POL
user@vsrx# set gateway JSC-GW version v2-only
```

   b. Configure external interface IP address for the clients to connect. You must enter this IP address (*https://172.16.1.254/<profile>*) for the Gateway Address field in the Juniper Secure Connect application.

```
[edit security ike]
user@vsrx# set gateway JSC-GW external-interface ge-0/0/1
user@vsrx# set gateway JSC-GW local-address 172.16.1.254
```

c. Configure dead peer detection (DPD).

```
[edit security ike]
user@vsrx# set gateway JSC-GW dead-peer-detection optimized
user@vsrx# set gateway JSC-GW dead-peer-detection interval 10
user@vsrx# set gateway JSC-GW dead-peer-detection threshold 5
```

d. Associate the gateway with the access profile and the TCP encapsulation profile.

```
[edit security ike]
user@vsrx# set gateway JSC-GW aaa access-profile JSC-ACCESS
user@vsrx# set gateway JSC-GW tcp-encap-profile JSC-ENCAP
```

10. Configure IPsec proposal.

```
[edit security ipsec]
user@vsrx# set proposal JSC-IPSEC-PRO protocol esp
user@vsrx# set proposal JSC-IPSEC-PRO encryption-algorithm aes-256-gcm
```

11. Configure IPsec policy.

```
[edit security ipsec]
user@vsrx# set policy JSC-IPSEC-POL proposals JSC-IPSEC-PRO
user@vsrx# set policy JSC-IPSEC-POL perfect-forward-secrecy keys group19
```

12. Configure IPsec VPN parameters and traffic selectors.

```
[edit security ipsec]
user@vsrx# set vpn JSC-VPN bind-interface st0.0
user@vsrx# set vpn JSC-VPN df-bit clear
user@vsrx# set vpn JSC-VPN ike gateway JSC-GW
user@vsrx# set vpn JSC-VPN ike ipsec-policy JSC-IPSEC-POL
user@vsrx# set vpn JSC-VPN traffic-selector ts-1 local-ip 10.1.1.1/32
user@vsrx# set vpn JSC-VPN traffic-selector ts-1 remote-ip 0.0.0.0/0
```

13. Configure remote access settings.

a. Configure remote access profile.

```
[edit security remote-access]
user@vsrx# set profile jsc-saml ipsec-vpn JSC-VPN
user@vsrx# set profile jsc-saml access-profile JSC-ACCESS
user@vsrx# set profile jsc-saml client-config JSC-CLIENT
```

b. Configure remote access client settings.

```
[edit security remote-access]
user@vsrx# set client-config JSC-CLIENT connection-mode manual
user@vsrx# set client-config JSC-CLIENT dead-peer-detection interval 60
user@vsrx# set client-config JSC-CLIENT dead-peer-detection threshold 5
user@vsrx# set client-config JSC-CLIENT no-eap-tls
```

14. Configure the firewall as the local gateway for remote access.

a. Set SAML as the authentication method for the access profile.

```
[edit access]
user@vsrx# set profile JSC-ACCESS authentication-order saml
```

b. Specify SAML settings for the access profile.

```
[edit access]
user@vsrx# set profile JSC-ACCESS saml service-provider vsrx-jsc
user@vsrx# set profile JSC-ACCESS saml identity-provider srx1.example.net idp-name
example-idp
user@vsrx# set profile JSC-ACCESS saml identity-provider any idp-name example-idp
```

c. Associate the network address pool with the access profile.Configure the address pool for assigning dynamic IPs the clients.

```
[edit access]
user@vsrx# set profile JSC-ACCESS address-assignment pool JSC-POOL
user@vsrx# set address-assignment pool JSC-POOL family inet network 10.1.3.0/24
user@vsrx# set address-assignment pool JSC-POOL family inet range JSC-RANGE low 10.1.3.10
user@vsrx# set address-assignment pool JSC-POOL inet range JSC-RANGE high 10.1.3.20
```

```
user@vsrx# set address-assignment pool JSC-POOL family inet xauth-attributes primary-dns
8.8.8.8/32
```

d. Configure firewall authentication.

```
[edit access]
user@vsrx# set firewall-authentication web-authentication default-profile JSC-ACCESS
```

e. Configure SSL termination profile for the firewall to act as an SSL proxy server, and terminate the SSL session from the client. The server certificate is a local certificate identifier. Server certificates are used to authenticate the identity of a server.

```
[edit services]
user@vsrx# set ssl termination profile JSC-SSL-PRO server-certificate jsc
```

f. Configure SSL VPN profile.

```
[edit security]
user@vsrx# set tcp-encap profile JSC-ENCAP ssl-profile JSC-SSL-PRO
user@vsrx# set tcp-encap profile JSC-ENCAP log
```

15. Configure the SAML access parameters such as IdP and SP settings.

```
[edit access]
user@vsrx# set saml service-provider vsrx-jsc entity-id https://srx1.example.net
user@vsrx# set saml service-provider vsrx-jsc assertion-waittime 60
user@vsrx# set saml identity-provider example-idp settings entity-id http://www.example.org/
abcd1234
user@vsrx# set saml identity-provider example-idp settings single-signon-url https://
5075942.example.org/app/5075942_srx1examplenet_1/abcd1234/sso/saml
user@vsrx# set saml identity-provider example-idp settings single-logout-url https://
5075942.example.org
user@vsrx# set saml identity-provider example-idp settings idp-certificate EXAMPLE-CA
user@vsrx# set saml identity-provider example-idp attribute-mapping username mail mandatory
```

Verification

IN THIS SECTION

This section provides a list of show commands that you can use to verify the feature in this example. .

Verify SAML-Based User Authentication in Juniper Secure Connect Application

Purpose

Connect Juniper Secure Connect application for remote access VPN using SAMl-based user authentication.

Action

Perform the following steps on your client:

1. Place the CA certificate in the client laptop at `C:\ProgramData\Juniper\SecureConnect\cacerts`.
2. Enter the **Connection Profile** as *`https://172.16.1.254/jsc-saml`* or *`https://srx1.juniper.net/jsc-saml`*. Then click the **Connection** toggle button to establish the VPN connection.
3. After the system downloads the configuration, you see a window, **User ID for SAML authentiation**, that prompts you for your SAML user ID. Enter your SAML user ID in the **User ID** field as *`user1@srx1.example.net`*.
4. The system redirects you to the IdP SSO URL in your default browser. Enter the username *`user1@srx1.example.net`* along with the correct password.

5. When you successfully complete the user authentication, accept the browser pop-up to launch the Juniper Secure Connect application.

6. Close the browser while the IKE connection runs in the background.

7. Observe that the Juniper Secure Connect application establishes the remote access VPN connection.

Meaning

The user, *user1@srx1.example.net* is authenticated with SAML-based user autehntication method and the remote access VPN connection established. Notice that the username is in the email format defined in the IdP's mandatory attribute-mapping.

Verify SAML Assertion Cache Entries

```
user@vsrx> show network-access aaa saml assertion-cache
  Username            Remaining Validity
  user1@srx1.example.net 6h 52m 40s
```

Purpose

Run the command to display SAML assertion cache entries.

Action

From operational mode, run the command `show network-access aaa saml assertion-cache` on vSRX.

Meaning

Shows SAML authentication assertions cache information with the domain name configured in the access profile IdP settings and the SAML authenticated username.

Verify Subscriber-Specific AAA Statistics

```
user@vsrx> show network-access aaa subscribers
Username                 Logical system/Routing instance   Client type    Session-ID
user1@srx1.example.net   default:default                   xauth          6
```

Purpose

Run the command to display subscriber username.

Action

From operational mode, run the command `show network-access aaa subscribers` on vSRX.

Meaning

Displays information about active subscriber sessions.

Verify SAML Authentication Statistics

```
user@vsrx> show network-access aaa statistics saml
SAML Authentication statistics
    Authentication request received       21
    Authentication response sent          21
    Request hit cache                     0
    Request sent to IdP                   6
    Assertion received                    5
    Assertion timeout                     1
    Assertion parse fail                  0
    Assertion sanity fail                 0
    Assertion signature verify fail       0
    Assertion decryption fail             0
    Assertion node missing                0
    Assertion attributes missing          0
    Assertion username mismatch           0
    Logout request received               0
    Logout response sent                  0
    Logout parse fail                     0
    Logout sanity fail                    0
    Logout signature verify fail          0
    Memory allocation fail                0
```

Purpose

Run the command to display SAML authentication statistics.

Action

From operational mode, run the command `show network-access aaa statistics saml` on vSRX.

Meaning

Displays SAML authentication statistics.

Verify IKE SA

```
user@vsrx> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
1       UP     a5872b7d9c649c0b  3264d25485c6827a  IKEv2          172.17.1.1
```

Purpose

Run the command to display information about IKE security associations (SA).

Action

From operational mode, run the command `show security ike security-associations` on vSRX.

Meaning

Shows the firewall's IKE mode as IKEv2 and has SA with 172.17.1.1 which is the Juniper Secure Connect client.

Verify IPsec SA

```
user@vsrx> show security ipsec security-associations
  Total active tunnels: 1     Total IPsec sas: 1
  ID      Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <500001 ESP:aes-gcm-256/aes256-gcm 0xdb912536 3429/ unlim - root 10954 172.17.1.1
  >500001 ESP:aes-gcm-256/aes256-gcm 0x52a3f7de 3429/ unlim - root 10954 172.17.1.1
```

Purpose

Run the command to display information about IPsec SA.

Action

From operational mode, run the command `show security ipsec security-associations` on vSRX.

Meaning

Shows that the firewall has one active IPsec tunnel SA with 172.17.1.1 which is the Juniper Secure Connect client.

Verify IKE Active Peer

```
user@vsrx> show security ike active-peer
Remote Address                      Port     Peer IKE-ID                                AAA
username                        Assigned IP
172.17.1.1                          10954    ra@example.com
user1@srx1.example.net              10.1.3.10
```

Purpose

Run the command to display the connected IKE peers.

Action

From operational mode, run the command `show security ike active-peer` on vSRX.

Meaning

Shows that the firewall has one active IKE peer 172.17.1.1 which is the Juniper Secure Connect client. The firewall also displays the peer IKE ID and the authenticated remote username and IP address assigned to the user.

Appendix 1: Troubleshoot Juniper Secure Connect

If you encounter any issue with SAML-based user authentication, follow these steps to troubleshoot the problem:

1. The feature works with the iked process. Ensure you install the junos-ike package by using the command `request system software add optional://junos-ike.tgz`.

2. Enable traceoptions for PKI, IKE, IPsec, and remote access options. For example, run the command `set security pki traceoptions file pki.log` to enable traceoptions on PKI. Check the syslogs and trace logs.
3. Check whether the SAML assertion cache is disabled. If the SAML assertion cache is disabled, we recommend enabling it to cache SAML assertions from the IdP. See saml-options.
4. Ensure that the assertion cache contains a valid entry for the user. The assertion cache must include a valid user entry to support SAML-based user authentication. If the cache does not have a valid entry, perform a manual disconnect and reconnect of the VPN connection in the Juniper Secure Connect application. This action prompts the application to authenticate the user again and repopulate the assertion cache. See show network-access aaa saml assertion-cache.
5. If the syslog reports `AUTHD_SAML_AUTH_FAILED` because of an assertion wait timeout, extend the assertion timeout using the command `set access saml service-provider yoursaml assertion-waittime` *`waittime`*.
6. To reload IdP metadata, see request network-access aaa saml load-idp-metadata.
7. To export service provider metadata, see request network-access aaa saml export-sp-metadata.
8. If you notice that the IKE session times out, extend the session using the command `set security ike session half-open timeout` *`timeout`*.

Appendix 2: Set Commands on vSRX

Set command output on vSRX.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.254/24
set interfaces st0 unit 0 family inet
set interfaces ge-0/0/1 unit 0 family inet address 172.16.1.254/24

set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone VPN interfaces st0.0

set security policies from-zone trust to-zone trust policy default-permit match source-address
any
set security policies from-zone trust to-zone trust policy default-permit match destination-
address any
set security policies from-zone trust to-zone trust policy default-permit match application any
set security policies from-zone trust to-zone trust policy default-permit then permit
set security policies from-zone trust to-zone untrust policy default-permit match source-address any
set security policies from-zone trust to-zone untrust policy default-permit match destination-address any
set security policies from-zone trust to-zone untrust policy default-permit match application any
set security policies from-zone trust to-zone untrust policy default-permit then permit
set security policies from-zone trust to-zone VPN policy JSC-ALLOW-OUT match source-address any
set security policies from-zone trust to-zone VPN policy JSC-ALLOW-OUT match destination-address any
set security policies from-zone trust to-zone VPN policy JSC-ALLOW-OUT match application any
set security policies from-zone trust to-zone VPN policy JSC-ALLOW-OUT then permit
set security policies from-zone VPN to-zone trust policy JSC-ALLOW-IN match source-address any
set security policies from-zone VPN to-zone trust policy JSC-ALLOW-IN match destination-address any
set security policies from-zone VPN to-zone trust policy JSC-ALLOW-IN match application any
set security policies from-zone VPN to-zone trust policy JSC-ALLOW-IN then permit

set security nat source rule-set jsc from zone VPN
set security nat source rule-set jsc to zone trust
set security nat source rule-set jsc rule 1 match source-address 0.0.0.0/0
set security nat source rule-set jsc rule 1 then source-nat interface

set security ike proposal JSC-IKE-PRO authentication-method rsa-signatures
set security ike proposal JSC-IKE-PRO dh-group group19
set security ike proposal JSC-IKE-PRO authentication-algorithm sha-256
set security ike proposal JSC-IKE-PRO encryption-algorithm aes-256-cbc

set security ike policy JSC-IKE-POL proposals JSC-IKE-PRO
set security ike policy JSC-IKE-POL certificate local-certificate IKE-KEY

set security ike gateway JSC-GW dynamic user-at-hostname "ra@example.com"
set security ike gateway JSC-GW dynamic ike-user-type shared-ike-id
set security ike gateway JSC-GW ike-policy JSC-IKE-POL
user@vsrx# set security ike gateway JSC-GW version v2-only

set security ike gateway JSC-GW external-interface ge-0/0/1
set security ike gateway JSC-GW local-address 172.16.1.254

set security ike gateway JSC-GW dead-peer-detection optimized
set security ike gateway JSC-GW dead-peer-detection interval 10
set security ike gateway JSC-GW dead-peer-detection threshold 5
set security ike gateway JSC-GW aaa access-profile JSC-ACCESS
set security ike gateway JSC-GW tcp-encap-profile JSC-ENCAP

set security ipsec proposal JSC-IPSEC-PRO protocol esp
set security ipsec proposal JSC-IPSEC-PRO encryption-algorithm aes-256-gcm

set security ipsec policy JSC-IPSEC-POL proposals JSC-IPSEC-PRO
set security ipsec policy JSC-IPSEC-POL perfect-forward-secrecy keys group19

set security ipsec vpn JSC-VPN bind-interface st0.0
set security ipsec vpn JSC-VPN df-bit clear
set security ipsec vpn JSC-VPN ike gateway JSC-GW
set security ipsec vpn JSC-VPN ike ipsec-policy JSC-IPSEC-POL
set security ipsec vpn JSC-VPN traffic-selector ts-1 local-ip 10.1.1.1/32
set security ipsec vpn JSC-VPN traffic-selector ts-1 remote-ip 0.0.0.0/0

set security remote-access profile jsc-saml ipsec-vpn JSC-VPN
set security remote-access profile jsc-saml access-profile JSC-ACCESS
set security remote-access profile jsc-saml client-config JSC-CLIENT

set security remote-access client-config JSC-CLIENT connection-mode manual
set security remote-access client-config JSC-CLIENT dead-peer-detection interval 60
set security remote-access client-config JSC-CLIENT dead-peer-detection threshold 5
set security remote-access client-config JSC-CLIENT no-eap-tls

set access profile JSC-ACCESS authentication-order saml
set access profile JSC-ACCESS saml service-provider vsrx-jsc
set access profile JSC-ACCESS saml identity-provider srx1.example.net idp-name example-idp
set access profile JSC-ACCESS saml identity-provider any idp-name example-idp
set access profile JSC-ACCESS address-assignment pool JSC-POOL

set access address-assignment pool JSC-POOL family inet network 10.1.3.0/24
set access address-assignment pool JSC-POOL family inet range JSC-RANGE low 10.1.3.10
set access address-assignment pool JSC-POOL inet range JSC-RANGE high 10.1.3.20
set access address-assignment pool JSC-POOL family inet xauth-attributes primary-dns 8.8.8.8/32

set access firewall-authentication web-authentication default-profile JSC-ACCESS

set services ssl termination profile JSC-SSL-PRO server-certificate jsc

set security tcp-encap profile JSC-ENCAP ssl-profile JSC-SSL-PRO
set security tcp-encap profile JSC-ENCAP log
set access saml service-provider vsrx-jsc entity-id https://srx1.example.net
set access saml service-provider vsrx-jsc assertion-waittime 60
set access saml identity-provider example-idp settings entity-id http://www.example.org/abcd1234
set access saml identity-provider example-idp settings single-signon-url https://
5075942.example.org/app/5075942_srx1examplenet_1/abcd1234/sso/saml
set access saml identity-provider example-idp settings single-logout-url https://
5075942.example.org
set access saml identity-provider example-idp settings idp-certificate EXAMPLE-CA
set access saml identity-provider example-idp attribute-mapping username mail mandatory
```

Appendix 3: Show Configuration Output on vSRX

Show command output on vSRX.

From configuration mode, confirm your configuration by entering the following commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@vsrx# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.1.1.254/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 172.16.1.254/24;
        }
    }
}
st0 {
    unit 0 {
        family inet;
    }
}
```

```
[edit]
user@vsrx# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
security-zone VPN {
    interfaces {
        st0.0;
    }
}
```

```
[edit]
user@vsrx# show security policies
from-zone trust to-zone trust {
    policy default-permit {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone trust to-zone untrust {
    policy default-permit {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone trust to-zone VPN {
    policy JSC-ALLOW-OUT {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone VPN to-zone trust {
    policy JSC-ALLOW-IN {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

```
[edit]
user@vsrx# show security nat
source {
    rule-set JSC-NAT {
        from zone VPN;
        to zone trust;
        rule 1 {
            match {
                source-address 0.0.0.0/0;
            }
            then {
                source-nat {
                    interface;
                }
            }
        }
    }
}
```

```
[edit]
user@vsrx# show system services
…
web-management {
    https {
        pki-local-certificate jsc-web;
    }
}
```

```
[edit]
user@vsrx# show security pki
ca-profile EXAMPLE-CA {
    ca-identity EXAMPLE-CA;
    revocation-check {
        disable;
    }
}
ca-profile CERTAUTH {
    ca-identity CERTAUTH;
    revocation-check {
        disable;
    }
}
```

```
[edit]
user@vsrx# show security ike
proposal JSC-IKE-PRO {
    authentication-method rsa-signatures;
    dh-group group19;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
}
policy JSC-IKE-POL {
    proposals JSC-IKE-PRO;
    certificate {
        local-certificate IKE-CERT;
    }
}
gateway JSC-GW {
    ike-policy JSC-IKE-POL;
    dynamic {
        user-at-hostname "ra@example.com";
        ike-user-type shared-ike-id;
    }
    dead-peer-detection {
        optimized;
        interval 10;
        threshold 5;
    }
    external-interface ge-0/0/1;
    local-address 172.16.1.254;
    aaa {
        access-profile JSC-ACCESS;
    }
    version v2-only;
    tcp-encap-profile JSC-ENCAP;
}
```

```
[edit]
user@vsrx# show security ipsec
proposal JSC-IPSEC-PRO {
    protocol esp;
    encryption-algorithm aes-256-gcm;
}
policy JSC-IPSEC-POL {
    perfect-forward-secrecy {
        keys group19;
    }
    proposals JSC-IPSEC-PRO;
}
vpn JSC-VPN {
    bind-interface st0.0;
    df-bit clear;
    ike {
        gateway JSC-GW;
        ipsec-policy JSC-IPSEC-POL;
    }
    traffic-selector ts-1 {
        local-ip 10.1.1.1/32;
        remote-ip 0.0.0.0/0;
    }
}
```

```
[edit]
user@vsrx# show security tcp-encap
profile JSC-ENCAP {
    ssl-profile JSC-SSL-PRO;
    log;
}
```

```
[edit]
user@vsrx# show services
ssl {
    termination {
        profile JSC-SSL-PRO {
            server-certificate jsc;
        }
    }
}
```

```
[edit]
user@vsrx# show security remote-access
profile jsc-saml {
    ipsec-vpn JSC-VPN;
    access-profile JSC-ACCESS;
    client-config JSC-CLIENT;
}
client-config JSC-CLIENT {
    connection-mode manual;
    dead-peer-detection {
        interval 60;
        threshold 5;
    }
    no-eap-tls;
}
```

```
[edit]
user@vsrx# show access
profile JSC-ACCESS {
    authentication-order saml;
    address-assignment {
        pool JSC-POOL;
    }
    saml {
        service-provider vsrx-jsc;
        identity-provider srx1.example.net {
            idp-name example-idp;
        }
        identity-provider any {
            idp-name example-idp;
        }
    }
}
address-assignment {
    pool JSC-POOL {
        family inet {
            network 10.1.3.0/24;
            range jsc-range {
                low 10.1.3.10;
                high 10.1.3.20;
            }
            xauth-attributes {
                primary-dns 8.8.8.8/32;
            }
        }
    }
}
saml {
    service-provider vsrx-jsc {
        entity-id https://srx1.example.net;
        assertion-waittime 60;
    }
    identity-provider example-idp {
        settings {
            entity-id http://www.example.org/abcd1234;
            single-signon-url https://5075942.example.org/app/5075942_srx1examplenet_1/
abcd1234/sso/saml;
            single-logout-url https://5075942.example.org;
            idp-certificate EXAMPLE-CA;
        }
        attribute-mapping {
            username mail mandatory;
        }
    }
}
firewall-authentication {
    web-authentication {
        default-profile JSC-ACCESS;
    }
}
```

Local User Authentication Using Pre-shared Key (CLI Procedure)

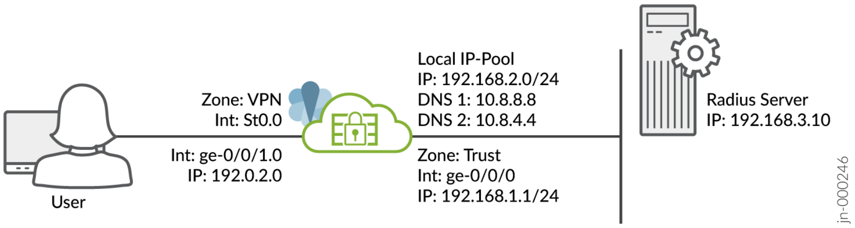
IN THIS SECTION

Overview

In this configuration, you use the username and password for local user authentication. This configuration option does not allow you to change or recover your credentials without interacting with the firewall administrator, hence we do not recommend this authentication method. Instead, we recommend you to use "External User Authentication Using RADIUS" on page 173 method.

We assume that you have completed the basic setup of your SRX Series Firewalls, including interfaces, zones, and security policies as illustrated in the Figure 18 on page 74.

Figure 18: Topology



For information about prerequisites, see "System Requirements for Juniper Secure Connect" on page 11.

You must ensure that the SRX Series Firewall uses either a signed certificate or a self-signed certificate instead of the default system-generated certificate. Before you start configuring Juniper Secure Connect, you must bind the certificate to the SRX Series Firewall by executing the following command:

```
user@host# set system services web-management https pki-local-certificate <cert_name>
```

For example:

```
user@host# set system services web-management https pki-local-certificate SRX_Certificate
```

Where *SRX_Certificate* is the self-signed certificate.

CLI Quick Configuration

To quickly configure this example on your SRX Series Firewalls, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
[edit]
user@host#

set security ike proposal JUNIPER_SECURE_CONNECT authentication-method pre-shared-keys
set security ike proposal JUNIPER_SECURE_CONNECT dh-group group19
set security ike proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-cbc
set security ike proposal JUNIPER_SECURE_CONNECT lifetime-seconds 28800
set security ike policy JUNIPER_SECURE_CONNECT mode aggressive

set security ike policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT
set security ike policy JUNIPER_SECURE_CONNECT pre-shared-key ascii-text "$9$yYJeMXVwgUjq7-
jqmfn6rev"

set security ike gateway JUNIPER_SECURE_CONNECT dynamic hostname ra.example.com
set security ike gateway JUNIPER_SECURE_CONNECT dynamic ike-user-type shared-ike-id
set security ike gateway JUNIPER_SECURE_CONNECT ike-policy JUNIPER_SECURE_CONNECT
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection optimized
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection interval 10
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
set security ike gateway JUNIPER_SECURE_CONNECT version v1-only
set security ike gateway JUNIPER_SECURE_CONNECT aaa access-profile Juniper_Secure_Connect
set security ike gateway JUNIPER_SECURE_CONNECT tcp-encap-profile SSL-VPN
set security ike gateway JUNIPER_SECURE_CONNECT external-interface ge-0/0/1



set security ipsec proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-gcm
set security ipsec proposal JUNIPER_SECURE_CONNECT lifetime-seconds 3600
set security ipsec policy JUNIPER_SECURE_CONNECT perfect-forward-secrecy keys group19
set security ipsec policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT

set security ipsec vpn JUNIPER_SECURE_CONNECT bind-interface st0.0
set security ipsec vpn JUNIPER_SECURE_CONNECT ike gateway JUNIPER_SECURE_CONNECT
set security ipsec vpn JUNIPER_SECURE_CONNECT ike ipsec-policy JUNIPER_SECURE_CONNECT
set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 local-ip 0.0.0.0/0
set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 remote-ip 0.0.0.0/0
set security remote-access profile ra.example.com ipsec-vpn JUNIPER_SECURE_CONNECT
set security remote-access profile ra.example.com access-profile Juniper_Secure_Connect
set security remote-access profile ra.example.com client-config JUNIPER_SECURE_CONNECT
set security remote-access client-config JUNIPER_SECURE_CONNECT connection-mode manual
set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-detection interval 60
set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5


set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet network
192.168.2.0/24
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet range Range low
192.168.2.11
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet range Range high
192.168.2.100
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet xauth-attributes
primary-dns 10.8.8.8/32
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet xauth-attributes
primary-wins 192.168.4.10/32
set access profile Juniper_Secure_Connect address-assignment pool Juniper_Secure_Connect_Addr-
Pool
set access firewall-authentication web-authentication default-profile Juniper_Secure_Connect
set access profile Juniper_Secure_Connect client Bob firewall-user password
"$9$abGjqTz6uORmfORhSMWJGD"

set services ssl termination profile Juniper_SCC-SSL-Term-Profile server-certificate
JUNIPER_SECURE_CONNECT(RSA)
set security tcp-encap profile SSL-VPN ssl-profile Juniper_SCC-SSL-Term-Profile
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match source-
address any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match
destination-address any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match
application any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 then permit
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 then log
session-close
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match source-
address any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match
destination-address any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match
application any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 then permit
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 then log
session-close

set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.0/24
set interfaces ge-0/0/1 unit 0 family inet address 198.51.100.0/24
set interfaces st0 unit 0 family inet

set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone VPN host-inbound-traffic system-services all
set security zones security-zone VPN host-inbound-traffic protocols all
set security zones security-zone VPN interface st0.0
set security zones security-zone VPN interfaces ge-0/0/1.0
```

Step-by-Step-Procedure

To configure VPN settings using the command line interface:

1. Log in to your SRX Series Firewall using the command line interface (CLI).
2. Enter the configuration mode.
3. Configure remote access VPN.

   Condition

For deploying Juniper Secure Connect, you must create a self-signed certificate and bind the certificate to the SRX Series Firewall. For more information, see Preparing Juniper Secure Connect Configuration.

IKE Configuration:

a. Configure IKE proposal.

   - Define IKE proposal authentication method, Diffie-Hellman group, and authentication algorithm.

   - Configure **pre-shared-keys** as the authentication method.

     Enter the key in ASCII format. We do not support hexadecimal format for remote-access VPN.

```
user@host# set security ike proposal JUNIPER_SECURE_CONNECT authentication-method pre-shared-keys
user@host# set security ike proposal JUNIPER_SECURE_CONNECT dh-group group19
user@host# set security ike proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-cbc
user@host# set security ike proposal JUNIPER_SECURE_CONNECT lifetime-seconds 28800
```

   See proposal (Security IKE).

b. Configure IKE policy.

   Set the IKE Phase 1 policy mode, reference to the IKE proposal, and IKE Phase 1 policy authentication method.

```
user@host# set security ike policy JUNIPER_SECURE_CONNECT mode aggressive
user@host# set security ike policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT
user@host# set security ike policy JUNIPER_SECURE_CONNECT pre-shared-key ascii-text "$9$yYJeMXVwgUjq7-jqmfn6rev"
```

   See policy (Security IKE).

c. Configure IKE gateway options. See dynamic.

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dynamic hostname ra.example.com
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dynamic ike-user-type shared-ike-id
```

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT ike-policy
JUNIPER_SECURE_CONNECT
```

If you do not configure the DPD values and the version information, the Junos OS assigns the default value for these options. See dead-peer-detection.

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection optimized
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection interval 10
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
user@host# set security ike gateway JUNIPER_SECURE_CONNECT version v1-only
user@host# set security ike gateway JUNIPER_SECURE_CONNECT aaa access-profile
Juniper_Secure_Connect
user@host# set security ike gateway JUNIPER_SECURE_CONNECT tcp-encap-profile SSL-VPN
```

Configure external interface IP address for the clients to connect. You must enter this same IP address (in this example: 192.0.2.0) for the **Gateway Address** field in the Juniper Secure Connect application. See gateway.

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT external-interface ge-0/0/1
```

IPsec Configuration:

a. Configure IPsec proposal.

```
user@host# set security ipsec proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-
gcm
user@host# set security ipsec proposal JUNIPER_SECURE_CONNECT lifetime-seconds 3600
```

See proposal (Security IPsec).

b. Configure IPsec policy.

- Specify IPsec phase 2 PFS to use Diffie-Hellman group 19.

- Specify IPsec Phase 2 proposal reference.

```
user@host# set security ipsec policy JUNIPER_SECURE_CONNECT perfect-forward-secrecy keys
group19
user@host# set security ipsec policy JUNIPER_SECURE_CONNECT proposals
JUNIPER_SECURE_CONNECT
```

See policy (Security IPsec).

IPsec VPN Configuration:

a. Configure IPsec VPN parameters. See vpn (Security).

```
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT bind-interface st0.0
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT ike gateway JUNIPER_SECURE_CONNECT
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT ike ipsec-policy
JUNIPER_SECURE_CONNECT
```

b. Configure VPN traffic selectors. See traffic-selector.

```
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 local-ip
0.0.0.0/0
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 remote-ip
0.0.0.0/0
```

4. Configure the remote user client options.

a. Configure remote access profile. See remote-access.

```
user@host# set security remote-access profile ra.example.com ipsec-vpn
JUNIPER_SECURE_CONNECT
user@host# set security remote-access profile ra.example.com access-profile
Juniper_Secure_Connect
user@host# set security remote-access profile ra.example.com client-config
JUNIPER_SECURE_CONNECT
```

b. Configure remote access client configuration. See client-config.

```
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT connection-mode
manual
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-
detection interval 60
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-
detection threshold 5
```

Table 15 on page 81 summarizes the remote user settings options.

Table 15: Remote User Settings Options

Remote User Settings	Description
connection-mode	To establish the client connection manually or automatically, configure the appropriate option. • If you configure **manual** option, then in the Juniper Secure Connect application, to establish a connection, you must either click the toggle button or select **Connection > Connect** from the menu. • If you configure **Always** option, then Juniper Secure Connect automatically establishes the connection. *Known Limitation:* **Android device**: If you use or select **Always**, then the configuration is downloaded from the first used SRX device. If the first SRX Series Firewall configuration changes or if you connect to a new SRX device, the configuration does not get downloaded to the Juniper Secure Connect application. This means that once you connect in the **Always** mode using the Android device, any configuration changes in the SRX Series Firewall do not take effect on Juniper Secure Connect.
dead-peer-detection	Dead Peer Detection (DPD) is enabled by default to allow the client to detect if the SRX Series Firewall is reachable and if the device is not reachable, disable the connection till reachability is restored.

Table 15: Remote User Settings Options *(Continued)*

Remote User Settings	Description
default -profile	If you configure a VPN connection profile as a **default-profile**, then you must enter only the gateway address in the Juniper Secure Connect application. It is optional to enter the realm name in Juniper Secure Connect application, as the application automatically selects default profile as realm name. In this example, enter *ra.example.com* in the **Gateway Address** field of the Juniper Secure Connect application. **NOTE**: Starting in Junos OS Release 23.1R1, we've hidden the `default-profile` option at the `[edit security remote-access]` hierarchy level. In releases before Junos OS Release 23.1R1, you use this option to specify one of the remote-access profiles as the default profile in Juniper Secure Connect. But with changes to the format of remote-access profile names, we no longer require the `default-profile` option. We've deprecated `default-profile` option—rather than immediately removing it—to provide backward compatibility and a chance to make your existing configuration conform to the changed configuration. You'll receive a warning message if you continue to use the `default-profile` option in your configuration. However existing deployments are not affected if you modify the current configuration. See default-profile (Juniper Secure Connect).

5. Configure the local gateway.

   a. Create address pool for client dynamic-IP assignment. See address-assignment (Access).

      - Enter the network address that you use for the address assignment.

      - Enter your DNS server address. Enter WINS server details, if required. Create the address range to assign IP addresses to the clients.

      - Enter the name, and the lower and higher limits.

```
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
network 192.168.2.0/24
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
range Range low 192.168.2.11
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
range Range high 192.168.2.100
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
xauth-attributes primary-dns 10.8.8.8/32
```

```
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
xauth-attributes primary-wins 192.168.4.10/32
```

b. Create access profile. 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.

```
user@host# set access profile Juniper_Secure_Connect address-assignment pool
Juniper_Secure_Connect_Addr-Pool
user@host# set access firewall-authentication web-authentication default-profile
Juniper_Secure_Connect
```

Enter a username and password for SRX local authentication of client credentials.

```
user@host# set access profile Juniper_Secure_Connect client Bob firewall-user password
"$9$abGjqTz6uORmfORhSMWJGD"
```

c. Create SSL termination profile. SSL termination is a process where the SRX Series Firewalls acts as an SSL proxy server, and terminates the SSL session from the client. 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. The server certificate is a local certificate identifier. Server certificates are used to authenticate the identity of a server.

```
user@host# set services ssl termination profile Juniper_SCC-SSL-Term-Profile server-
certificate JUNIPER_SECURE_CONNECT(RSA)
```

d. Create SSL VPN profile. See tcp-encap.

```
user@host# set security tcp-encap profile SSL-VPN ssl-profile Juniper_SCC-SSL-Term-Profile
```

e. Create firewall policies.

Create the security policy to permit traffic from the trust zone to the VPN zone.

```
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 match source-address any
user@host# set security policies from-zone trust to-zone VPN policy
```

```
JUNIPER_SECURE_CONNECT-1 match destination-address any
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 match application any
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 then permit
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 then log session-close
```

Create the security policy to permit traffic from the VPN zone to the trust zone.

```
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 match source-address any
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 match destination-address any
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 match application any
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 then permit
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 then log session-close
```

6. Configure Ethernet interface information.

   ```
   user@host# set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.0/24
   user@host# set interfaces ge-0/0/1 unit 0 family inet address 198.51.100.0/24
   ```

   Configure st0 interface with the family set as inet.

   ```
   user@host# set interfaces st0 unit 0 family inet
   ```

7. Configure security zones.

   For `host-inbound-traffic` the required minimum configuration:

   a. `system-services` - On the *VPN* zone, select `ike` to allow VPN service and `https` to allow HTTPS connection to push the initial configuration to Juniper Secure Connect Application. On the *trust* zone, select `https`.

   b. `protocols` - None for the basic configuration.

      See system-services and protocols.

In the configuration example we mention *all* `system-services` and `protocols`. But, we recommend you to allow only necessary services and protocols.

```
user@host# set security zones security-zone trust host-inbound-traffic system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-0/0/0.0
user@host# set security zones security-zone VPN host-inbound-traffic system-services all
user@host# set security zones security-zone VPN host-inbound-traffic protocols all
user@host# set security zones security-zone VPN interface st0.0
user@host# set security zones security-zone VPN interfaces ge-0/0/1.0
```

8. Remote access configuration with remote user and local gateway is configured successfully.
9. Launch the Juniper Secure Connect application and provide the same IP address that you configured for external IP address in the **Gateway Address** field in the Juniper Secure Connect application.

   In this example, you've configured 192.0.2.0 as the external interface IP address for the clients to connect. You must enter this same IP address (192.0.2.0) for the Gateway Address field in the Juniper Secure Connect application.

Result

From operational mode, confirm your configuration by entering the `show security`, `show access`, and `show services` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host> show security
   ike {
       proposal JUNIPER_SECURE_CONNECT {

           authentication-method pre-shared-keys;
           dh-group group19;
           encryption-algorithm aes-256-cbc;
           lifetime-seconds 28800;
       }
       policy JUNIPER_SECURE_CONNECT {
           mode aggressive;
;
           proposals JUNIPER_SECURE_CONNECT;
           pre-shared-key ascii-text "$9$lifv87wYojHm-VHmfT/9evW"; ## SECRET-DATA
       }
       gateway JUNIPER_SECURE_CONNECT {
           ike-policy JUNIPER_SECURE_CONNECT;
```

```
            dynamic {
                hostname ra.example.com;
                ike-user-type shared-ike-id;
            }
            dead-peer-detection {
                optimized;
                interval 10;
                threshold 5;
            }
            external-interface ge-0/0/1;

            aaa {
                access-profile Juniper_Secure_Connect;
            }
            version v1-only;
            tcp-encap-profile SSL-VPN;
        }
    }
    ipsec {
        proposal JUNIPER_SECURE_CONNECT {

            encryption-algorithm aes-256-gcm;
            lifetime-seconds 3600;
        }
        policy JUNIPER_SECURE_CONNECT {

            perfect-forward-secrecy {
                keys group19;
            }
            proposals JUNIPER_SECURE_CONNECT;
        }
        vpn JUNIPER_SECURE_CONNECT {
            bind-interface st0.0;

            ike {
                gateway JUNIPER_SECURE_CONNECT;
                ipsec-policy JUNIPER_SECURE_CONNECT;
            }
            traffic-selector ts-1 {
                local-ip 0.0.0.0/0;
                remote-ip 0.0.0.0/0;
            }
        }
    }
    remote-access {
        profile ra.example.com {
            ipsec-vpn JUNIPER_SECURE_CONNECT;
            access-profile Juniper_Secure_Connect;
            client-config JUNIPER_SECURE_CONNECT;
        }
        client-config JUNIPER_SECURE_CONNECT {
            connection-mode manual;
            dead-peer-detection {
                interval 60;
                threshold 5;
            }
        }

    }
    policies {
        from-zone trust to-zone VPN {
            policy JUNIPER_SECURE_CONNECT-1 {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
        }
        from-zone VPN to-zone trust {
            policy JUNIPER_SECURE_CONNECT-2 {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
```

```
                   }
               }
           }
       }
   }
   tcp-encap {
       profile SSL-VPN {
           ssl-profile Juniper_SCC-SSL-Term-Profile;
       }
   }
```

```
[edit]
user@host> show access
  access {
      profile Juniper_Secure_Connect {
          client Bob {
              firewall-user {
                  password "$9$m5z6p0IreW9AeWLxwsP5Q"; ## SECRET-DATA
              }
          }
          address-assignment {
              pool Juniper_Secure_Connect_Addr-Pool;
          }
      }
      address-assignment {
          pool Juniper_Secure_Connect_Addr-Pool {
              family inet {
                  network 192.168.2.0/24;
                  range Range {
                      low 192.168.2.11;
                      high 192.168.2.100;
                  }
                  xauth-attributes {
                      primary-dns 10.8.8.8/32;
                      primary-wins 192.168.4.10/32;
                  }
              }
          }
      }
      firewall-authentication {
          web-authentication {
              default-profile Juniper_Secure_Connect;
          }
      }
  }
```

```
[edit]
user@host> show services
   ssl {
       termination {
           profile Juniper_SCC-SSL-Term-Profile {
               server-certificate JUNIPER_SECURE_CONNECT(RSA);
           }
       }
   }
```

Make sure that you already have a server certificate to attach with the SSL termination profile.

```
[edit]
user@host> show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 192.0.2.0/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 198.51.100.0/24;
        }
    }
}
st0 {
    unit 1 {
        family inet;
    }
}
```

```
[edit]
user@host> show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone VPN {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
        ge-0/0/1.0;
    }
}
```

When you are done configuring the feature on your device, enter commit from configuration mode.

RELATED DOCUMENTATION

External User Authentication (CLI Procedure) | 91

Certificate-Based Validation Using EAP-MSCHAPv2 Authentication (CLI Procedure) | 127

Certificate-Based Validation Using EAP-TLS Authentication (CLI Procedure) | 145

External User Authentication (CLI Procedure)

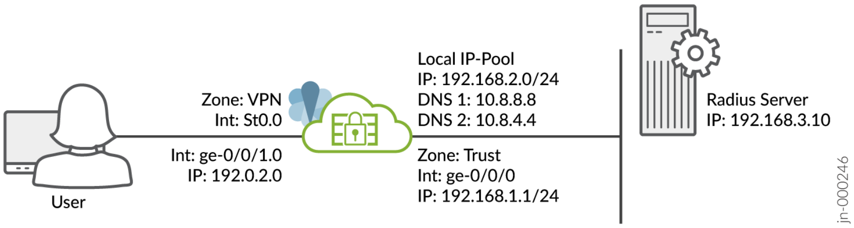
IN THIS SECTION

Overview

This configuration is more secure as it allows you to use the same username and password as your domain login as well as change or recover your credentials without interacting with the firewall administrator. It also adds less workload on the administrator as the password must be changed frequently. We recommend you to use this configuration for authenticating the user.

We assume that you have completed the basic setup of your SRX Series Firewalls, including interfaces, zones, and security policies as illustrated in the Figure 19 on page 91.

Figure 19: Topology



For information about prerequisites, see "System Requirements for Juniper Secure Connect" on page 11.

You must ensure that the SRX Series Firewall uses either a signed certificate or a self-signed certificate instead of the default system-generated certificate. Before you start configuring Juniper Secure Connect, you must bind the certificate to the SRX Series Firewall by executing the following command:

```
user@host# set system services web-management https pki-local-certificate <cert_name>
```

For example:

```
user@host# set system services web-management https pki-local-certificate SRX_Certificate
```

Where *SRX_Certificate* is the certificate obtained from CA or self-signed certificate.

CLI Quick Configuration

To quickly configure this example on your SRX Series Firewalls, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
[edit]
user@host#
set security ike proposal JUNIPER_SECURE_CONNECT authentication-method pre-shared-keys
set security ike proposal JUNIPER_SECURE_CONNECT dh-group group19

set security ike proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-gcm
set security ike proposal JUNIPER_SECURE_CONNECT lifetime-seconds 28800
set security ike policy JUNIPER_SECURE_CONNECT mode aggressive
set security ike policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT
set security ike policy JUNIPER_SECURE_CONNECT pre-shared-key ascii-text "$9$yYJeMXVwgUjq7-jqmfn6rev"
set security ike gateway JUNIPER_SECURE_CONNECT dynamic hostname ra.example.com
set security ike gateway JUNIPER_SECURE_CONNECT dynamic ike-user-type group-ike-id
set security ike gateway JUNIPER_SECURE_CONNECT ike-policy JUNIPER_SECURE_CONNECT
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection optimized
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection interval 10
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
set security ike gateway JUNIPER_SECURE_CONNECT version v1-only
set security ike gateway JUNIPER_SECURE_CONNECT aaa access-profile Juniper_Secure_Connect
set security ike gateway JUNIPER_SECURE_CONNECT tcp-encap-profile SSL-VPN
set security ike gateway JUNIPER_SECURE_CONNECT external-interface ge-0/0/0
set security ike gateway JUNIPER_SECURE_CONNECT local-address 192.0.2.0

set security ipsec proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-gcm
set security ipsec proposal JUNIPER_SECURE_CONNECT lifetime-seconds 3600
set security ipsec policy JUNIPER_SECURE_CONNECT perfect-forward-secrecy keys group19
set security ipsec policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT
set security ipsec vpn JUNIPER_SECURE_CONNECT bind-interface st0.0

set security ipsec vpn JUNIPER_SECURE_CONNECT ike gateway JUNIPER_SECURE_CONNECT
set security ipsec vpn JUNIPER_SECURE_CONNECT ike ipsec-policy JUNIPER_SECURE_CONNECT
set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 local-ip 0.0.0.0/0
set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 remote-ip 0.0.0.0/0
set security remote-access profile ra.example.com ipsec-vpn JUNIPER_SECURE_CONNECT
set security remote-access profile ra.example.com access-profile Juniper_Secure_Connect
set security remote-access profile ra.example.com client-config JUNIPER_SECURE_CONNECT
set security remote-access profile ra.example.com options multi-access
set security remote-access client-config JUNIPER_SECURE_CONNECT connection-mode manual
set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-detection interval 60
set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5


set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet network
192.168.2.0/24
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet range Range low
192.168.2.11
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet range Range high
192.168.2.100
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet xauth-attributes
primary-dns 10.8.8.8/32
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet xauth-attributes
primary-wins 192.168.4.10/32
set access profile Juniper_Secure_Connect authentication-order radius
set access profile Juniper_Secure_Connect address-assignment pool Juniper_Secure_Connect_Addr-
Pool
set access profile Juniper_Secure_Connect radius-server 192.168.3.10 port 1812
set access profile Juniper_Secure_Connect radius-server 192.168.3.10 secret "$9$JSUi.QF/
0BEP5BEcyW8ZUj"
set access profile Juniper_Secure_Connect radius-server 192.168.3.10 timeout 5
set access profile Juniper_Secure_Connect radius-server 192.168.3.10 retry 3
set access firewall-authentication web-authentication default-profile Juniper_Secure_Connect

set services ssl termination profile Juniper_SCC-SSL-Term-Profile server-certificate
```

```
JUNIPER_SECURE_CONNECT(RSA)
set security tcp-encap profile SSL-VPN ssl-profile Juniper_SCC-SSL-Term-Profile
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match source-
address any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match
destination-address any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match
application any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 then permit
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 then log
session-close
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match source-
address any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match
destination-address any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match
application any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 then permit
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 then log
session-close

set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.0/24
set interfaces ge-0/0/1 unit 0 family inet address 198.51.100.0/24
set interfaces st0 unit 0 family inet

set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone vpn host-inbound-traffic system-services all
set security zones security-zone vpn host-inbound-traffic protocols all
set security zones security-zone VPN interface st0.0
set security zones security-zone vpn interfaces ge-0/0/1.0
```

Step-by-Step-Procedure

To configure VPN settings using the command line interface:

1. Log in to your SRX Series Firewall using the command line interface (CLI).
2. Enter the configuration mode.
3. Configure remote access VPN.

For deploying Juniper Secure Connect, you must create a self-signed certificate and bind the certificate to the SRX Series Firewall. For more information, see "Get Started with Juniper Secure Connect" on page 10.

IKE Configuration:

a. Configure IKE proposal.

   - Define IKE proposal authentication method, Diffie-Hellman group, and authentication algorithm.

   - Configure **pre-shared-keys** as the authentication method. Enter the preshared key in ASCII format. We do not support hexadecimal format for remote-access VPN.

```
user@host# set security ike proposal JUNIPER_SECURE_CONNECT authentication-method pre-shared-keys
user@host# set security ike proposal JUNIPER_SECURE_CONNECT dh-group group19
user@host# set security ike proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-gcm
user@host# set security ike proposal JUNIPER_SECURE_CONNECT lifetime-seconds 28800
```

   See proposal (Security IKE).

b. Configure IKE policy.

   Set the IKE Phase 1 policy mode, reference to the IKE proposal, and IKE Phase 1 policy authentication method.

```
user@host# set security ike policy JUNIPER_SECURE_CONNECT mode aggressive

user@host# set security ike policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT
user@host# set security ike policy JUNIPER_SECURE_CONNECT pre-shared-key ascii-text
"$9$yYJeMXVwgUjq7-jqmfn6rev"
```

   See policy (Security IKE).

c. Configure IKE gateway options. See dynamic.

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dynamic hostname ra.example.com
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dynamic ike-user-type group-ike-id
```

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT ike-policy
JUNIPER_SECURE_CONNECT
```

If you do not configure the DPD values and the version information, the Junos OS assigns the default value for these options. See dead-peer-detection.

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection optimized
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection interval 10
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
user@host# set security ike gateway JUNIPER_SECURE_CONNECT version v1-only
user@host# set security ike gateway JUNIPER_SECURE_CONNECT aaa access-profile
Juniper_Secure_Connect
user@host# set security ike gateway JUNIPER_SECURE_CONNECT tcp-encap-profile SSL-VPN
```

Configure external interface IP address for the clients to connect. You must enter this same IP address (in this example: https://192.0.2.0/) for the Gateway Address field in the Juniper Secure Connect application. See gateway.

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT external-interface ge-0/0/0
user@host# set security ike gateway JUNIPER_SECURE_CONNECT local-address 192.0.2.0
```

IPsec Configuration:

a. Configure IPsec proposal.

```
user@host# set security ipsec proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-
gcm
user@host# set security ipsec proposal JUNIPER_SECURE_CONNECT lifetime-seconds 3600
```

See proposal (Security IPsec).

b. Configure IPsec policy.

- Specify IPsec phase 2 PFS to use Diffie-Hellman group 19.

- Specify IPsec Phase 2 proposal reference.

```
user@host# set security ipsec policy JUNIPER_SECURE_CONNECT perfect-forward-secrecy keys
group19
user@host# set security ipsec policy JUNIPER_SECURE_CONNECT proposals
JUNIPER_SECURE_CONNECT
```

See policy (Security IPsec).

IPsec VPN Configuration:

a. Configure IPsec VPN parameters. See vpn (Security).

```
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT bind-interface st0.0

user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT ike gateway JUNIPER_SECURE_CONNECT
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT ike ipsec-policy
JUNIPER_SECURE_CONNECT
```

b. Configure VPN traffic selectors. See traffic-selector.

```
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 local-ip
0.0.0.0/0
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 remote-ip
0.0.0.0/0
```

4. Configure the remote user client options.

a. Configure remote access profile. See remote-access.

```
user@host# set security remote-access profile ra.example.com ipsec-vpn
JUNIPER_SECURE_CONNECT
user@host# set security remote-access profile ra.example.com access-profile
Juniper_Secure_Connect
user@host# set security remote-access profile ra.example.com client-config
JUNIPER_SECURE_CONNECT
```

b. Configure multi device user access for remote acess.

   To configure multidevice user access, ensure that the following prerequisites are met:

   - Secure Connect client version is supported.

   - Each of the remote devices (computers or smart devices) has a unique hostname.

   - To reduce license consumption, you can configure idle timeout options using `set security ipsec vpn` *`vpn-name`*`ike idle-time` command to disconnect inactive connections.

   - Supports only *group-ike-id*.

   You can clear all the IKE associations of a user using the command `clear security ike active-peer aaa-username` *`user-name`*.

   The multi device user access feature does not work with static IP address assignment using radius attribute Framed-IP-Address. The user's first connection will succeed, but the subsequent connections may fail.

   The authd process assigns the static address, providing the user with a configured IP address for their first connection. For subsequent connections, the authd process selects a free IP from the pool using the `set access address-assignment pool family [inet|inet6] host ip-address user-name` command.

```
user@host# set security remote-access profile ra.example.com options multi-access
```

c. Configure remote access client configuration. See client-config.

```
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT connection-mode manual
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-detection interval 60
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
```

Table 16 on page 99 summarizes the remote user settings options.

Table 16: Remote User Settings Options

Remote User Settings	Description
connection-mode	To establish the client connection manually or automatically, configure the appropriate option. • If you configure **manual** option, then in the Juniper Secure Connect application, to establish a connection, you must either click the toggle button or select **Connection > Connect** from the menu. • If you configure **Always** option, then Juniper Secure Connect automatically establishes the connection. *Known Limitation:* **Android device**: If you use or select **Always**, then the configuration is downloaded from the first used SRX device. If the first SRX Series Firewall configuration changes or if you connect to a new SRX device, the configuration does not get downloaded to the Juniper Secure Connect application. This means that once you connect in the **Always** mode using the Android device, any configuration changes in the SRX Series Firewall do not take effect on Juniper Secure Connect.
dead-peer-detection	Dead Peer Detection (DPD) is enabled by default to allow the client to detect if the SRX Series Firewall is reachable and if the device is not reachable, disable the connection till reachability is restored.

Table 16: Remote User Settings Options *(Continued)*

Remote User Settings	Description
default -profile	If you configure a VPN connection profile as a **default-profile**, then you must enter only the gateway address in the Juniper Secure Connect application. It is optional to enter the realm name in Juniper Secure Connect application, as the application automatically selects default profile as realm name. In this example, enter *ra.example.com* in the **Gateway Address** field of the Juniper Secure Connect application. **NOTE**: Starting in Junos OS Release 23.1R1, we've hidden the `default-profile` option at the `[edit security remote-access]` hierarchy level. In releases before Junos OS Release 23.1R1, you use this option to specify one of the remote-access profiles as the default profile in Juniper Secure Connect. But with changes to the format of remote-access profile names, we no longer require the `default-profile` option. We've deprecated `default-profile` option—rather than immediately removing it—to provide backward compatibility and a chance to make your existing configuration conform to the changed configuration. You'll receive a warning message if you continue to use the `default-profile` option in your configuration. However existing deployments are not affected if you modify the current configuration. See default-profile (Juniper Secure Connect).

5. Configure the local gateway.

   a. Create address pool for client dynamic-IP assignment. See address-assignment (Access).

      - Enter the network address that you use for the address assignment.
      - Enter your DNS server address. Enter WINS server details, if required. Create the address range to assign IP addresses to the clients.
      - Enter the name, and the lower and higher limits.

```
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
network 192.168.2.0/24
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
range Range low 192.168.2.11
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
range Range high 192.168.2.100
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
xauth-attributes primary-dns 10.8.8.8/32
```

```
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
xauth-attributes primary-wins 192.168.4.10/32
```

b. Create access profile.

   For external user authentication, provide Radius Server IP Address, the Radius Secret, and Source Address for the radius communications to be sourced from. Configure radius for the authentication order.

```
user@host# set access profile Juniper_Secure_Connect authentication-order radius
user@host# set access profile Juniper_Secure_Connect address-assignment pool
Juniper_Secure_Connect_Addr-Pool
user@host# set access profile Juniper_Secure_Connect radius-server 192.168.3.10 port 1812
user@host# set access profile Juniper_Secure_Connect radius-server 192.168.3.10 secret
"$9$JSUi.QF/0BEP5BEcyW8ZUj"
user@host# set access profile Juniper_Secure_Connect radius-server 192.168.3.10 timeout 5
user@host# set access profile Juniper_Secure_Connect radius-server 192.168.3.10 retry 3
user@host# set access firewall-authentication web-authentication default-profile
Juniper_Secure_Connect
```

c. Create SSL termination profile. SSL termination is a process where the SRX Series Firewalls acts as an SSL proxy server, and terminates the SSL session from the client. 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. The server certificate is a local certificate identifier. Server certificates are used to authenticate the identity of a server.

```
user@host# set services ssl termination profile Juniper_SCC-SSL-Term-Profile server-
certificate JUNIPER_SECURE_CONNECT(RSA)
```

d. Create SSL VPN profile. See tcp-encap.

```
user@host# set security tcp-encap profile SSL-VPN ssl-profile Juniper_SCC-SSL-Term-Profile
```

e. Create firewall policies.

   Create the security policy to permit traffic from the trust zone to the VPN zone.

```
user@host# set security policies from-zone trust to-zone VPN policy
```

```
JUNIPER_SECURE_CONNECT-1 match source-address any
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 match destination-address anyuser@host# set security policies
from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match application any
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 then permit
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 then log session-close
```

Create the security policy to permit traffic from the VPN zone to the trust zone.

```
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 match source-address any
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 match destination-address any
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 match application any
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 then permit
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 then log session-close
```

6. Configure Ethernet interface information.

```
user@host# set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/1 unit 0 family inet address 198.51.100.0/24
```

Configure st0 interface with the family set as inet.

```
user@host# set interfaces st0 unit 0 family inet
```

7. Configure security zones.

```
user@host# set security zones security-zone trust host-inbound-traffic system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-0/0/0.0
user@host# set security zones security-zone vpn host-inbound-traffic system-services all
```

```
user@host# set security zones security-zone vpn host-inbound-traffic protocols all
user@host# set security zones security-zone VPN interface st0.0
user@host# set security zones security-zone vpn interfaces ge-0/0/1.0
```

8. Remote access configuration with remote user and local gateway is configured successfully.
9. Launch the Juniper Secure Connect application and provide the same IP address that you configured for external IP address in the Gateway Address field in the Juniper Secure Connect application.

   In this example, you've configured 192.0.2.0 as the external interface IP address for the clients to connect. You must enter this same IP address (192.0.2.0) for the Gateway Address field in the Juniper Secure Connect application.

Result

From operational mode, confirm your configuration by entering the `show security`, `show access`, and `show services` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host> show security
   ike {
       proposal JUNIPER_SECURE_CONNECT {
           authentication-method pre-shared-keys;
           dh-group group19;
           encryption-algorithm aes-256-gcm;
           lifetime-seconds 28800;
       }
       policy JUNIPER_SECURE_CONNECT {
           mode aggressive;
           proposals JUNIPER_SECURE_CONNECT;
           pre-shared-key ascii-text "$9$oWZDk5Qnp0I.P0IEcvMaZU"; ## SECRET-DATA
       }
       gateway JUNIPER_SECURE_CONNECT {
           ike-policy JUNIPER_SECURE_CONNECT;
           dynamic {
               hostname ra.example.com;
               ike-user-type group-ike-id;
           }
           dead-peer-detection {
               optimized;
               interval 10;
               threshold 5;
           }
           external-interface ge-0/0/1;
```

```
            aaa {
                access-profile Juniper_Secure_Connect;
            }
            version v1-only;
            tcp-encap-profile SSL-VPN;
        }
    }
    ipsec {
        proposal JUNIPER_SECURE_CONNECT {


            encryption-algorithm aes-256-gcm;
            lifetime-seconds 3600;
        }
        policy JUNIPER_SECURE_CONNECT {
            perfect-forward-secrecy {
                keys group19;
            }
            proposals JUNIPER_SECURE_CONNECT;
        }
        vpn JUNIPER_SECURE_CONNECT {
            bind-interface st0.0;
            ike {
                gateway JUNIPER_SECURE_CONNECT;
                ipsec-policy JUNIPER_SECURE_CONNECT;
            }
            traffic-selector ts-1 {
                local-ip 0.0.0.0/0;
                remote-ip 0.0.0.0/0;
            }
        }
    }
    remote-access {
        profile ra.example.com {

            ipsec-vpn JUNIPER_SECURE_CONNECT;
            access-profile Juniper_Secure_Connect;
            client-config JUNIPER_SECURE_CONNECT;
        }
        client-config JUNIPER_SECURE_CONNECT {
            connection-mode manual;
            dead-peer-detection {
                interval 60;
                threshold 5;
            }
        }

    }
    policies {
        from-zone trust to-zone VPN {
            policy JUNIPER_SECURE_CONNECT-1 {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
        }
        from-zone VPN to-zone trust {
            policy JUNIPER_SECURE_CONNECT-2 {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
        }
    }
    tcp-encap {
        profile SSL-VPN {
            ssl-profile Juniper_SCC-SSL-Term-Profile;
```

```
       }
   }
```

```
[edit]
user@host> show access
  access {
      profile Juniper_Secure_Connect {
          authentication-order radius;
          address-assignment {
              pool Juniper_Secure_Connect_Addr-Pool;
          }
          radius-server {
              192.168.3.10 {
                  port 1812;
                  secret "$9$JSUi.QF/0BEP5BEcyW8ZUj"; ## SECRET-DATA
                  timeout 5;
                  retry 3;
              }
          }
      }
      address-assignment {
          pool Juniper_Secure_Connect_Addr-Pool {
              family inet {
                  network 192.168.2.0/24;
                  range Range {
                      low 192.168.2.11;
                      high 192.168.2.100;
                  }
                  xauth-attributes {
                      primary-dns 10.8.8.8/32;
                      primary-wins 192.168.4.10/32;
                  }
              }
          }
      }
      firewall-authentication {
          web-authentication {
              default-profile Juniper_Secure_Connect;
          }
      }
  }
```

```
[edit]
user@host> show services
   ssl {
       termination {
           profile Juniper_SCC-SSL-Term-Profile {
               server-certificate JUNIPER_SECURE_CONNECT(RSA);
           }
       }
   }
```

Make sure that you already have a server certificate to attach with the SSL termination profile.

```
[edit]
user@host> show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 192.0.2.0/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 198.51.100.0/24;
        }
    }
}
st0 {
    unit 1 {
        family inet;
    }
}
```

```
[edit]
user@host> show security zones
```

```
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone vpn {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
        ge-0/0/1.0;
    }
}
```

When you are done configuring the feature on your device, enter commit from configuration mode.

RELATED DOCUMENTATION

Local User Authentication Using Pre-shared Key (CLI Procedure) | **74**

Certificate-Based Validation Using EAP-MSCHAPv2 Authentication (CLI Procedure) | **127**

Certificate-Based Validation Using EAP-TLS Authentication (CLI Procedure) | **145**

Example: Configuring LDAP Authentication for Juniper Secure Connect (CLI Procedure)

IN THIS SECTION

Overview

LDAP helps in authentication of users. You can define one or more LDAP groups and use a specific local IP pool for address assignment based on group membership when you use LDAP as an authentication option. If you don't specify the local IP pool per group, Junos OS assigns an IP address from the local IP pool configured in the access profile.

To configure user groups, include the `allowed-groups` statement at the `[edit access ldap-options]` hierarchy level. These group names match the names in your LDAP directory.

Consider the following LDAP groups such as group1, group2, and group3. You can assign group1 to address pool Juniper_Secure_Connect_Addr-Pool. You can assign group2 to address pool poolB. You can assign group3 to address pool poolC.

1. User1 belongs to group1. User1's group matches one of the configured groups, User1 is authenticated. Based on the group membership, the system assigns IP address to User1 from following address pool Juniper_Secure_Connect_Addr-Pool.

2. User2 belongs to group2. User2's group matches one of the configured groups, User2 is authenticated. Based on the group membership, the system assigns IP address to User2 from following address pool poolB.

3. User3 belongs to group3. User3's group matches one of the configured groups, User3 is authenticated. Based on the group membership, the system assigns IP address to User3 from following address pool poolC.

4. User4's group doesn't match either of the configured groups.

Table-1 describes LDAP server response when the `ldap-options` is configured at the global access level and within the access profile. The priority of profile configuration is higher than global configuration.

Table 17: LDAP access groups at global level and within access profile

Username	Configured Matched group	LDAP server returned groups	Address pool	Action
User1	group1	group1, group2, group3	Juniper_Secure_Connect_Addr-Pool	Accept (Matching configured groups)
User2	group2	group1, group2, group3	poolB	Accept (Matching configured groups)
User3	group3	group1, group2, group3	poolC	Accept (Matching configured groups)
User4	group4	groupX, groupY, groupZ	poolD	Reject (Not matching configured matched groups)

NOTE: This example uses LDAP as the authentication option where the user belongs to a single group.

Requirements

This example uses the following hardware and software components:

- Any SRX Series Firewall
- Junos OS Release 23.1R1

Before you begin:

- ldap options, see ladp-options
- Enable LDAP authentication with TLS/SSL for secure connections, see Enabling LDAP Authentication with TLS/SSL for Secure Connections.

For information about prerequisites, see "System Requirements for Juniper Secure Connect" on page 11.

You must ensure that the SRX Series Firewall uses either a signed certificate or a self-signed certificate instead of the default system-generated certificate. Before you start configuring Juniper Secure Connect, you must bind the certificate to the SRX Series Firewall by executing the following command:

```
user@host# set system services web-management https pki-local-certificate <cert_name>
```

For example:

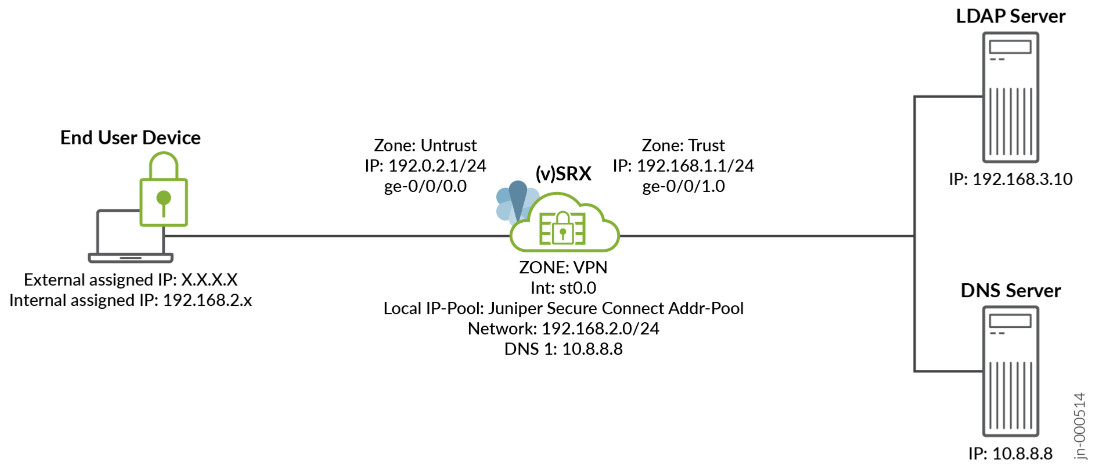
```
user@host# set system services web-management https pki-local-certificate SRX_Certificate
```

Where SRX_Certificate is the certificate obtained from CA or self-signed certificate.

Topology

The below figure shows the topology in this example.

Figure 1: Configuring LDAP authentication for Juniper Secure Connect



Configuration

IN THIS SECTION

In this example, we use LDAP as the authentication option where the user belongs to a single group.

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set security ike proposal JUNIPER_SECURE_CONNECT authentication-method pre-shared-keys
set security ike proposal JUNIPER_SECURE_CONNECT dh-group group19
set security ike proposal JUNIPER_SECURE_CONNECT authentication-algorithm sha-384
set security ike proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-cbc
set security ike proposal JUNIPER_SECURE_CONNECT lifetime-seconds 28800

set security ike policy JUNIPER_SECURE_CONNECT mode aggressive
set security ike policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT
set security ike policy JUNIPER_SECURE_CONNECT pre-shared-key ascii-text
"$9$vWL8xd24Zk.5bs.5QFAtM8X7bsgoJDHq4o"

set security ike gateway JUNIPER_SECURE_CONNECT dynamic hostname ra.example.com
set security ike gateway JUNIPER_SECURE_CONNECT dynamic ike-user-type shared-ike-id
set security ike gateway JUNIPER_SECURE_CONNECT ike-policy JUNIPER_SECURE_CONNECT
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection optimized
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection interval 10
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
set security ike gateway JUNIPER_SECURE_CONNECT version v1-only
set security ike gateway JUNIPER_SECURE_CONNECT aaa access-profile JUNIPER_SECURE_CONNECT
set security ike gateway JUNIPER_SECURE_CONNECT tcp-encap-profile SSL-VPN
set security ike gateway JUNIPER_SECURE_CONNECT external-interface ge-0/0/0
set security ipsec proposal JUNIPER_SECURE_CONNECT authentication-algorithm hmac-sha-256-128
set security ipsec proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-cbc
set security ipsec proposal JUNIPER_SECURE_CONNECT lifetime-seconds 3600

set security ipsec policy JUNIPER_SECURE_CONNECT perfect-forward-secrecy keys group19
set security ipsec policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT

set security ipsec vpn JUNIPER_SECURE_CONNECT bind-interface st0.0
set security ipsec vpn JUNIPER_SECURE_CONNECT ike gateway JUNIPER_SECURE_CONNECT
set security ipsec vpn JUNIPER_SECURE_CONNECT ike ipsec-policy JUNIPER_SECURE_CONNECT
set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts1 local-ip 0.0.0.0/0
set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts1 remote-ip 0.0.0.0/0

set security remote-access profile ra.example.com ipsec-vpn JUNIPER_SECURE_CONNECT
set security remote-access profile ra.example.com access-profile JUNIPER_SECURE_CONNECT
set security remote-access profile ra.example.com client-config JUNIPER_SECURE_CONNECT
set security remote-access client-config JUNIPER_SECURE_CONNECT connection-mode manual
set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-detection interval 10
set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5

set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet network
192.168.2.0/24
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet xauth-attributes
primary-dns 10.8.8.8/32
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet xauth-attributes
primary-wins 192.168.3.10/32

set access profile JUNIPER_SECURE_CONNECT authentication-order ldap
set access profile JUNIPER_SECURE_CONNECT  ldap-options base-distinguished-name
CN=Users,DC=juniper,DC=net
set access profile JUNIPER_SECURE_CONNECT  ldap-options search search-filter CN=
set access profile JUNIPER_SECURE_CONNECT ldap-options search admin-search distinguished-name
CN=Administrator,CN=Users,DC=juniper,DC=net
set access profile JUNIPER_SECURE_CONNECT ldap-options search admin-search password
"$9$Bmf1hreK8x7Vrl24ZGiHkqmPQ36/t0OR"
set access profile JUNIPER_SECURE_CONNECT ldap-options allowed-groups group1 address-assignment
pool Juniper_Secure_Connect_Addr-Pool
set access profile JUNIPER_SECURE_CONNECT ldap-server 192.168.3.10
set access firewall-authentication web-authentication default-profile JUNIPER_SECURE_CONNECT

set services ssl termination profile Juniper_SCC-SSL-Term-Profile server-certificate
JUNIPER_SECURE_CONNECT(RSA)
```

```
set security tcp-encap profile SSL-VPN ssl-profile Juniper_SCC-SSL-Term-Profile
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match source-
address any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match
destination-address any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match
application any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 then permit
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 then log
session-close
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match source-
address any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match
destination-address any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match
application any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 then permit
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 then log
session-close

set interfaces ge-0/0/0 description untrust
set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.1/24
set interfaces ge-0/0/1 description trust
set interfaces ge-0/0/1 unit 0 family inet address 192.168.1.1/24
set interfaces st0 unit 0 family inet

set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services https
set security zones security-zone untrust host-inbound-traffic system-services tcp-encap
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone trust interfaces ge-0/0/1.0
set security zones security-zone vpn interface st0.0
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy.

1. Configure one or more Internet Key Exchange (IKE) proposals; then you associate these proposals with an IKE policy. Configure IKE gateway options.

   ```
   user@host# set security ike proposal JUNIPER_SECURE_CONNECT authentication-method pre-shared-
   keys
   ```

```
user@host# set security ike proposal JUNIPER_SECURE_CONNECT dh-group group19
user@host# set security ike proposal JUNIPER_SECURE_CONNECT authentication-algorithm sha-384
user@host# set security ike proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-cbc
user@host# set security ike proposal JUNIPER_SECURE_CONNECT lifetime-seconds 28800

user@host# set security ike policy JUNIPER_SECURE_CONNECT mode aggressive
user@host# set security ike policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT
user@host# set security ike policy JUNIPER_SECURE_CONNECT pre-shared-key ascii-text
"$9$vWL8xd24Zk.5bs.5QFAtM8X7bsgoJDHq4o"

user@host# set security ike gateway JUNIPER_SECURE_CONNECT dynamic hostname ra.example.com
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dynamic ike-user-type shared-ike-id
user@host# set security ike gateway JUNIPER_SECURE_CONNECT ike-policy JUNIPER_SECURE_CONNECT
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection optimized
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection interval 10
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
user@host# set security ike gateway JUNIPER_SECURE_CONNECT version v1-only
user@host# set security ike gateway JUNIPER_SECURE_CONNECT aaa access-profile
JUNIPER_SECURE_CONNECT
user@host# set security ike gateway JUNIPER_SECURE_CONNECT tcp-encap-profile SSL-VPN
user@host# set security ike gateway JUNIPER_SECURE_CONNECT external-interface ge-0/0/0
```

2. Configure one or more IPsec proposals; then you associate these proposals with an IPsec policy. Configure IPsec VPN parameters and traffic selectors.

```
user@host# set security ipsec proposal JUNIPER_SECURE_CONNECT authentication-algorithm hmac-
sha-256-128
user@host# set security ipsec proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-cbc
user@host# set security ipsec proposal JUNIPER_SECURE_CONNECT lifetime-seconds 3600

user@host# set security ipsec policy JUNIPER_SECURE_CONNECT perfect-forward-secrecy keys
group19
user@host# set security ipsec policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT

user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT bind-interface st0.0
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT ike gateway JUNIPER_SECURE_CONNECT
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT ike ipsec-policy
JUNIPER_SECURE_CONNECT
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts1 local-ip
0.0.0.0/0
```

```
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts1 remote-ip
0.0.0.0/0
```

3. Configure a remote access profile and client configuration.

```
user@host# set security remote-access profile ra.example.com ipsec-vpn JUNIPER_SECURE_CONNECT
user@host# set security remote-access profile ra.example.com access-profile
JUNIPER_SECURE_CONNECT
user@host# set security remote-access profile ra.example.com client-config
JUNIPER_SECURE_CONNECT
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT connection-mode
manual
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-
detection interval 10
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-
detection threshold 5
```

4. Specify the LDAP server for external authentication order.

```
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
network 192.168.2.0/24
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
xauth-attributes primary-dns 10.8.8.8/32
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
xauth-attributes primary-wins 192.168.3.10/32

user@host# set access profile JUNIPER_SECURE_CONNECT authentication-order ldap
user@host# set access profile JUNIPER_SECURE_CONNECT  ldap-options base-distinguished-name
CN=Users,DC=juniper,DC=net
user@host# set access profile JUNIPER_SECURE_CONNECT  ldap-options search search-filter CN=
user@host# set access profile JUNIPER_SECURE_CONNECT ldap-options search admin-search
distinguished-name CN=Administrator,CN=Users,DC=juniper,DC=net
user@host# set access profile JUNIPER_SECURE_CONNECT ldap-options search admin-search
password "$9$Bmf1hreK8x7Vrl24ZGiHkqmPQ36/t0OR"
user@host# set access profile JUNIPER_SECURE_CONNECT ldap-options allowed-groups group1
address-assignment pool Juniper_Secure_Connect_Addr-Pool
user@host# set access profile JUNIPER_SECURE_CONNECT ldap-server 192.168.3.10
user@host# set access firewall-authentication web-authentication default-profile
JUNIPER_SECURE_CONNECT
```

5. Create SSL termination profile. SSL termination is a process where the SRX Series Firewalls acts as an SSL proxy server, and terminates the SSL session from the client. 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. The server certificate is a local certificate identifier. Server certificates are used to authenticate the identity of a server.

   ```
   user@host# set services ssl termination profile Juniper_SCC-SSL-Term-Profile server-
   certificate JUNIPER_SECURE_CONNECT(RSA)
   ```

   Create SSL VPN profile. See tcp-encap.

   ```
   user@host# set security tcp-encap profile SSL-VPN ssl-profile Juniper_SCC-SSL-Term-Profile
   ```

6. Create firewall policies.

   Create the security policy to permit traffic from the trust zone to the VPN zone.

   ```
   user@host# set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1
   match source-address any
   user@host# set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1
   match destination-address anyuser@host# set security policies from-zone trust to-zone VPN
   policy JUNIPER_SECURE_CONNECT-1 match application any
   user@host# set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1
   then permit
   user@host# set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1
   then log session-close
   ```

   Create the security policy to permit traffic from the VPN zone to the trust zone.

   ```
   user@host# set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2
   match source-address any
   user@host# set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2
   match destination-address any
   user@host# set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2
   match application any
   user@host# set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2
   then permit
   user@host# set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2
   then log session-close
   ```

7. Configure Ethernet interface information.

```
user@host# set interfaces ge-0/0/0 description untrust
user@host# set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.1/24
user@host# set interfaces ge-0/0/1 description trust
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.168.1.1/24
```

   Configure st0 interface with the family set as inet.

```
user@host# set interfaces st0 unit 0 family inet
```

8. Configure security zones.

```
user@host# set security zones security-zone untrust host-inbound-traffic system-services ike
user@host# set security zones security-zone untrust host-inbound-traffic system-services https
user@host# set security zones security-zone untrust host-inbound-traffic system-services tcp-encap
user@host# set security zones security-zone untrust interfaces ge-0/0/0.0
user@host# set security zones security-zone trust interfaces ge-0/0/1.0
user@host# set security zones security-zone vpn interface st0.0
```

Results

Check the results of the configuration:

```
[edit security ike]
proposal JUNIPER_SECURE_CONNECT {
    authentication-method pre-shared-keys;
    dh-group group19;
    authentication-algorithm sha-384;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 28800;
}
policy JUNIPER_SECURE_CONNECT {
    mode aggressive;
    proposals JUNIPER_SECURE_CONNECT;
    pre-shared-key ascii-text “$9$vWL8xd24Zk.5bs.5QFAtM8X7bsgoJDHq4o"; ## SECRET-DATA
}
```

```
gateway JUNIPER_SECURE_CONNECT {
    dynamic {
        hostname ra.example.com;
        ike-user-type shared-ike-id;
    }
    ike-policy JUNIPER_SECURE_CONNECT;
    dead-peer-detection {
        optimized;
        interval 10;
        threshold 5;
    }
    version v1-only;
    aaa {
        access-profile JUNIPER_SECURE_CONNECT;
    }
    tcp-encap-profile SSL-VPN;
    external-interface ge-0/0/0;
}
```

```
[edit security ipsec]
proposal JUNIPER_SECURE_CONNECT {
    authentication-algorithm hmac-sha-256-128;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 3600;
}
policy JUNIPER_SECURE_CONNECT {
    perfect-forward-secrecy {
        keys group19;
    }
    proposals JUNIPER_SECURE_CONNECT;
}
vpn JUNIPER_SECURE_CONNECT {
    bind-interface st0.0;
    ike {
        gateway JUNIPER_SECURE_CONNECT;
        ipsec-policy JUNIPER_SECURE_CONNECT;
    }
    traffic-selector ts1 {
        local-ip 0.0.0.0/0;
        remote-ip 0.0.0.0/0;
    }
}
```

```
[edit security remote-access]
profile ra.example.com {
    ipsec-vpn JUNIPER_SECURE_CONNECT;
    access-profile JUNIPER_SECURE_CONNECT;
    client-config JUNIPER_SECURE_CONNECT;
}
client-config JUNIPER_SECURE_CONNECT {
    connection-mode manual;
    dead-peer-detection {
        interval 10;
        threshold 5;
    }
}
```

```
[edit access]
address-assignment {
    pool Juniper_Secure_Connect_Addr-Pool {
        family inet {
            network 192.168.2.0/24;
            xauth-attributes {
                primary-dns 10.8.8.8/32;
                primary-wins 192.168.3.10/32;
            }
        }
    }
}
profile JUNIPER_SECURE_CONNECT {
    authentication-order ldap;
    ldap-options {
        base-distinguished-name DC=juniper,DC=net;
        search {
            search-filter CN=
            admin-search {
                distinguished-name CN=Administrator,CN=Users,DC=juniper,DC=net;
                password "$9$Bmf1hreK8x7Vrl24ZGiHkqmPQ36/t0OR"; ## SECRET-DATA
            }
        }
        allowed-groups {
            group1 {
                address-assignment {
                    pool Juniper_Secure_Connect_Addr-Pool;
                }
            }
        }
    }
    ldap-server 192.168.3.10;
}
firewall-authentication {
    web-authentication {
        default-profile JUNIPER_SECURE_CONNECT;
    }
}
```

```
[edit services]
ssl {
    termination {
        profile Juniper_SCC-SSL-Term-Profile {
            server-certificate JUNIPER_SECURE_CONNECT(RSA);
        }
    }
}
```

Make sure that you already have a server certificate to attach with the SSL termination profile.

```
[edit security]
tcp-encap {
    profile SSL-VPN {
        ssl-profile Juniper_SCC-SSL-Term-Profile;
    }
}
policies {
    from-zone trust to-zone VPN {
        policy JUNIPER_SECURE_CONNECT-1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
    }
    from-zone VPN to-zone trust {
        policy JUNIPER_SECURE_CONNECT-2 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
                log {
                    session-close;
                }
            }
        }
   }
}
```

```
[edit interfaces]
ge-0/0/0 {
    description untrust;
    unit 0 {
        family inet {
            address 192.0.2.1/24;
        }
    }
}
ge-0/0/1 {
    description trust;
    unit 0 {
        family inet {
            address 192.168.1.1/24;
        }
    }
}
st0 {
    unit 0 {
        family inet;
    }
}
```

```
[edit security zones]
security-zone untrust {
    host-inbound-traffic {
        system-services (ike | https | tcp-encap);
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone trust {
    interfaces {
        ge-0/0/1.0;
    }
}
security-zone vpn {
    interfaces {
        st0.0;
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, enter the following show commands.

Verify IPsec, IKE, and Group Information

IN THIS SECTION

Purpose

Display the possible outcomes list based on the LDAP server response when you use JUNIPER_SECURE_CONNECT access profile and configure `ldap-options` within the profile.

Action

From operational mode, enter these commands:

```
user@host> show network-access address-assignment pool Juniper_Secure_Connect_Addr-Pool
IP address/prefix       Hardware address     Host/User      Type
192.168.2.3              FF:FF:C0:A8:02:03    user1          xauth
```

```
user@host> show security ike security-associations detail
IKE peer 192.0.2.100, Index 6771534, Gateway Name: JUNIPER_SECURE_CONNECT
  Role: Responder, State: UP
  Initiator cookie: f174398039244783, Responder cookie: ffb63035b9f3f098
  Exchange type: Aggressive, Authentication method: Pre-shared-keys
  Local: 192.0.2.1:500, Remote: 192.0.2.100:10952
  Lifetime: Expires in 28746 seconds
  Reauth Lifetime: Disabled
  IKE Fragmentation: Disabled, Size: 0
  Remote Access Client Info: Juniper Secure Connect
  Peer ike-id: ra.example.com
  AAA assigned IP: 192.168.2.3
  Algorithms:
   Authentication        : hmac-sha384-192
   Encryption            : aes256-cbc
   Pseudo random function: hmac-sha384
   Diffie-Hellman group  : DH-group-19
  Traffic statistics:
   Input  bytes  :                 2058
   Output bytes  :                 1680
   Input  packets:                   12
   Output packets:                   10
   Input  fragmentated packets:       0
   Output fragmentated packets:       0
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 1

    Negotiation type: Quick mode, Role: Responder, Message ID: 0
    Local: 192.0.2.1:500, Remote: 192.0.2.100:10952
    Local identity: 192.0.2.1
    Remote identity: ra.example.com
    Flags: IKE SA is created
```

```
user@host> show security ike active-peer detail
Peer address: 192.0.2.100, Port: 10952,
Peer IKE-ID : ra.example.com
AAA username: user1
Assigned network attributes:
IP Address      : 192.168.2.3 ,   netmask         : 255.255.255.0
DNS Address     : 10.8.8.8 ,   DNS2 Address    : 0.0.0.0
WINS Address    : 192.168.3.10 ,   WINS2 Address   : 0.0.0.0

Previous Peer address   : 0.0.0.0, Port               : 0
Active IKE SA indexes   : 6771534
IKE SA negotiated       : 1
IPSec tunnels active    : 1, IPSec Tunnel IDs   : 67108869

DPD Config Mode    : optimized
DPD Config Interval: 10
DPD Config Treshold: 5
DPD Config P1SA IDX: 6771534
DPD Flags          : REMOTE_ACCESS

DPD Stats Req sent: 0, DPD Stats Resp rcvd: 0
DPD Statistics          : DPD TTL                 :5    DPD seq-no               :515423892
DPD Statistics          : DPD triggerd p1SA       :0    DPD Reserved             :0
```

```
user@host> show security ipsec security-associations detail
ID: 67108869 Virtual-system: root, VPN Name: JUNIPER_SECURE_CONNECT
  Local Gateway: 192.0.2.1, Remote Gateway: 192.0.2.100
  Traffic Selector Name: ts1
  Local Identity: ipv4(0.0.0.0-255.255.255.255)
  Remote Identity: ipv4(192.168.2.3)
  Version: IKEv1
  DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.0
  Port: 500, Nego#: 4, Fail#: 0, Def-Del#: 0 Flag: 0x24608f29
  Multi-sa, Configured SAs# 1, Negotiated SAs#: 1
  Tunnel events:
    Tue Mar 28 2023 11:34:36: IPSec SA negotiation successfully completed (1 times)
    Tue Mar 28 2023 11:34:36: Tunnel is ready. Waiting for trigger event or peer to trigger
negotiation (1 times)
    Tue Mar 28 2023 11:34:35: IKE SA negotiation successfully completed (1 times)
  Direction: inbound, SPI: f74fcaad, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 3435 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2838 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
  Direction: outbound, SPI: 8605b13f, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 3435 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2838 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
```

Meaning

Command output provides details of matched group.

Certificate-Based Validation Using EAP-MSCHAPv2 Authentication (CLI Procedure)

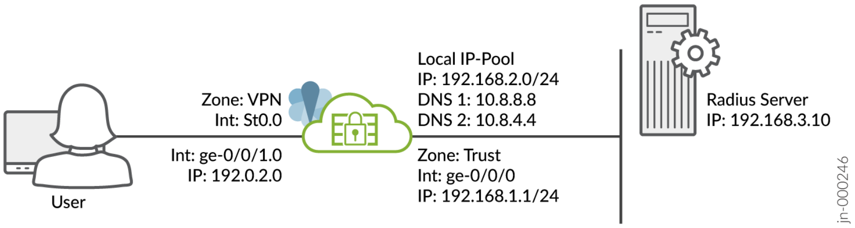
IN THIS SECTION

Overview

In this topic, you will see that the EAP-MSCHAPv2 authentication method uses the username and the password for authenticating the user using the RADIUS server. You use these credentials to download the initial configuration from the SRX Series Firewall and authenticate the user using the RADIUS server during remote access VPN setup at the IKE negotiation process.

We assume that you have completed the basic setup of your SRX Series Firewalls, including interfaces, zones, and security policies as illustrated in the Figure 20 on page 127.

Figure 20: Topology



For information about prerequisites, see "System Requirements for Juniper Secure Connect" on page 11.

Ensure that you have a Public Key Infrastructure (PKI) configured as the backend authentication. In this case, you only need to install the root certificate of the CA on each client. Note that local authentication is not supported in this scenario.

You must ensure that the SRX Series Firewall uses either a signed certificate or a self-signed certificate instead of the default system-generated certificate. Before you start configuring Juniper Secure Connect, you must bind the certificate to the SRX Series Firewall by executing the following command:

```
user@host# set system services web-management https pki-local-certificate <cert_name>
```

For example:

```
user@host# set system services web-management https pki-local-certificate SRX_Certificate
```

Where *SRX_Certificate* is the self-signed certificate.

CLI Quick Configuration

To quickly configure this example on your SRX Series Firewalls, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
[edit]
user@host#
set security ike proposal JUNIPER_SECURE_CONNECT authentication-method rsa-signatures
set security ike proposal JUNIPER_SECURE_CONNECT dh-group group19
set security ike proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-gcm
set security ike proposal JUNIPER_SECURE_CONNECT lifetime-seconds 28800
set security ike policy JUNIPER_SECURE_CONNECT mode main
set security ike policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT
set security ike policy JUNIPER_SECURE_CONNECT certificate local-certificate SRX_Certificate

set security ike gateway JUNIPER_SECURE_CONNECT dynamic hostname ra.example.com
set security ike gateway JUNIPER_SECURE_CONNECT dynamic ike-user-type shared-ike-id
set security ike gateway JUNIPER_SECURE_CONNECT ike-policy JUNIPER_SECURE_CONNECT
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection optimized
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection interval 10
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
set security ike gateway JUNIPER_SECURE_CONNECT version v2-only
set security ike gateway JUNIPER_SECURE_CONNECT aaa access-profile Juniper_Secure_Connect
set security ike gateway JUNIPER_SECURE_CONNECT tcp-encap-profile SSL-VPN
set security ike gateway JUNIPER_SECURE_CONNECT external-interface ge-0/0/0
set security ike gateway JUNIPER_SECURE_CONNECT local-address 192.0.2.0

set security ipsec proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-gcm
set security ipsec proposal JUNIPER_SECURE_CONNECT lifetime-seconds 3600

set security ipsec policy JUNIPER_SECURE_CONNECT perfect-forward-secrecy keys group19
set security ipsec policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT

set security ipsec vpn JUNIPER_SECURE_CONNECT bind-interface st0.0


set security ipsec vpn JUNIPER_SECURE_CONNECT ike gateway JUNIPER_SECURE_CONNECT
set security ipsec vpn JUNIPER_SECURE_CONNECT ike ipsec-policy JUNIPER_SECURE_CONNECT
set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 local-ip 0.0.0.0/0
set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 remote-ip 0.0.0.0/0
set security remote-access profile ra.example.com ipsec-vpn JUNIPER_SECURE_CONNECT
set security remote-access profile ra.example.com access-profile Juniper_Secure_Connect
set security remote-access profile ra.example.com client-config JUNIPER_SECURE_CONNECT
set security remote-access client-config JUNIPER_SECURE_CONNECT connection-mode manual
set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-detection interval 60
set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
set security remote-access client-config JUNIPER_SECURE_CONNECT no-eap-tls
set security remote-access client-config JUNIPER_SECURE_CONNECT certificate warn-before-expiry 60

set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet network
192.168.2.0/24
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet range Range low
192.168.2.11
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet range Range high
192.168.2.100
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet xauth-attributes
primary-dns 10.8.8.8/32
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet xauth-attributes
primary-wins 192.168.4.10/32
set access profile Juniper_Secure_Connect authentication-order radius
set access profile Juniper_Secure_Connect address-assignment pool Juniper_Secure_Connect_Addr-
Pool
set access profile Juniper_Secure_Connect radius-server 192.168.3.10 port 1812
set access profile Juniper_Secure_Connect radius-server 192.168.3.10 secret
"$9$ggaGjmfzCtOHqtO1RlegoJ"
set access profile Juniper_Secure_Connect radius-server 192.168.3.10 timeout 5
set access profile Juniper_Secure_Connect radius-server 192.168.3.10 retry 3
set access firewall-authentication web-authentication default-profile Juniper_Secure_Connect
set security pki ca-profile jweb-CA ca-identity jweb-CA
set security pki ca-profile jweb-CA enrollment url http://juniper-ca.example.com/certsrv/
set security pki ca-profile jweb-CA enrollment retry 0
set security pki ca-profile jweb-CA enrollment retry-interval 0
set security pki ca-profile jweb-CA revocation-check disable

set services ssl termination profile Juniper_SCC-SSL-Term-Profile server-certificate
JUNIPER_SECURE_CONNECT(RSA)
set security tcp-encap profile SSL-VPN ssl-profile Juniper_SCC-SSL-Term-Profile

set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match source-
address any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match
destination-address any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match
application any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 then permit
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 then log
session-close
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match source-
address any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match
destination-address any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match
application any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 then permit
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 then log
session-close

set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.0/24
set interfaces ge-0/0/1 unit 0 family inet address 198.51.100.0/24
set interfaces st0 unit 0 family inet

set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone vpn host-inbound-traffic system-services all
set security zones security-zone vpn host-inbound-traffic protocols all
set security zones security-zone VPN interface st0.0
set security zones security-zone vpn interfaces ge-0/0/1.0
```

Step-by-Step-Procedure

To configure VPN settings using the command line interface:

1. Log in to your SRX Series Firewall using the command line interface (CLI).
2. Enter the configuration mode.
3. Configure remote access VPN.

   For deploying Juniper Secure Connect, you must create a self-signed certificate and bind the certificate to the SRX Series Firewall. For more information, see "Get Started with Juniper Secure Connect" on page 10.

   IKE Configuration:

   a. Configure IKE proposal.

      - Configure `rsa-signatures` as authentication method to configure certificate-based authentication.

      - Define IKE proposal authentication method, Diffie-Hellman group, and authentication algorithm.

      ```
      user@host# set security ike proposal JUNIPER_SECURE_CONNECT authentication-method rsa-
      signatures
      user@host# set security ike proposal JUNIPER_SECURE_CONNECT dh-group group19

      user@host# set security ike proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-
      gcm
      user@host# set security ike proposal JUNIPER_SECURE_CONNECT lifetime-seconds 28800
      ```

      See proposal (Security IKE).

   b. Configure IKE policy. Set the IKE Phase 1 policy mode, reference to the IKE proposal, and IKE Phase 1 policy authentication method. See policy (Security IKE).

      ```
      user@host# set security ike policy JUNIPER_SECURE_CONNECT mode main

      user@host# set security ike policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT
      user@host# set security ike policy JUNIPER_SECURE_CONNECT certificate local-certificate
      SRX_Certificate
      ```

To load a local certificate, specify a particular local certificate using the `set security ike policy` *`policy-name`* `certificate local-certificate` *`certificate-id`* command when the local device has multiple loaded certificates. You can select one of the already externally signed local certificates. In this example, *SRX_Certificate* is the existing local certificate that is loaded for `JUNIPER_SECURE_CONNECT` policy.

If you don't have an existing local certificate, you can create one by following these steps:

- Manually load a certificate authority (CA) digital certificate from a specified location. See request security pki ca-certificate load (Security).

  ```
  user@host> request security pki ca-certificate load ca-profile ca-profile-name
  filename path/filename
  ```

- Manually load a local digital certificate from a specified location. See request security pki local-certificate load.

  ```
  user@host> request security pki local-certificate load filename local-certificate-name
  key key-name certificate-id SRX_Certificate
  ```

After creating a local certificate, you can attach the certificate to an IKE policy using the `set security ike policy` *`policy-name`* `certificate local-certificate` *`certificate-id`* command.

c. Configure IKE gateway options. See dynamic.

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dynamic hostname ra.example.com
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dynamic ike-user-type shared-
ike-id
user@host# set security ike gateway JUNIPER_SECURE_CONNECT ike-policy
JUNIPER_SECURE_CONNECT
```

If you do not configure the DPD values and the version information, the Junos OS assigns the default value for these options. See dead-peer-detection.

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection optimized
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection interval 10
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
user@host# set security ike gateway JUNIPER_SECURE_CONNECT version v2-only
user@host# set security ike gateway JUNIPER_SECURE_CONNECT aaa access-profile
```

```
Juniper_Secure_Connect
user@host# set security ike gateway JUNIPER_SECURE_CONNECT tcp-encap-profile SSL-VPN
```

Configure external interface IP address for the clients to connect. You must enter this same IP address (in this example: https://192.0.2.0) for the **Gateway Address** field in the Juniper Secure Connect application. See gateway.

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT external-interface ge-0/0/0
user@host# set security ike gateway JUNIPER_SECURE_CONNECT local-address 192.0.2.0
```

IPsec Configuration:

a. Configure IPsec proposal.

   Specify the IPsec phase 2 proposal protocol, encryption algorithm, and other phase 2 options.

```
user@host# set security ipsec proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-
gcm
user@host# set security ipsec proposal JUNIPER_SECURE_CONNECT lifetime-seconds 3600
```

   See proposal (Security IPsec).

b. Configure IPsec policy.

   - Specify IPsec phase 2 PFS to use Diffie-Hellman group 19.

   - Specify IPsec Phase 2 proposal reference.

```
user@host# set security ipsec policy JUNIPER_SECURE_CONNECT perfect-forward-secrecy keys
group19
user@host# set security ipsec policy JUNIPER_SECURE_CONNECT proposals
JUNIPER_SECURE_CONNECT
```

   See policy (Security IPsec).

IPsec VPN Configuration:

a. Configure IPsec VPN parameters. See vpn (Security).

```
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT bind-interface st0.0
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT ike gateway JUNIPER_SECURE_CONNECT
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT ike ipsec-policy
JUNIPER_SECURE_CONNECT
```

b. Configure VPN traffic selectors. See traffic-selector.

```
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 local-ip
0.0.0.0/0
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 remote-ip
0.0.0.0/0
```

4. Configure the remote user client options.

a. Configure remote access profile. See remote-access.

```
user@host# set security remote-access profile ra.example.com ipsec-vpn
JUNIPER_SECURE_CONNECT
user@host# set security remote-access profile ra.example.com access-profile
Juniper_Secure_Connect
user@host# set security remote-access profile ra.example.com client-config
JUNIPER_SECURE_CONNECT
```

b. Configure remote access client configuration. See client-config.

```
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT connection-mode
manual
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-
detection interval 60
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-
detection threshold 5
```

Table 18 on page 135 summarizes the remote user settings options.

Table 18: Remote User Settings Options

Remote User Settings	Description
connection-mode	To establish the client connection manually or automatically, configure the appropriate option. • If you configure **manual** option, then in the Juniper Secure Connect application, to establish a connection, you must either click the toggle button or select **Connection > Connect** from the menu. • If you configure **Always** option, then Juniper Secure Connect automatically establishes the connection. *Known Limitation:* **Android device**: If you use or select **Always**, then the configuration is downloaded from the first used SRX device. If the first SRX Series Firewall configuration changes or if you connect to a new SRX device, the configuration does not get downloaded to the Juniper Secure Connect application. This means that once you connect in the **Always** mode using the Android device, any configuration changes in the SRX Series Firewall do not take effect on Juniper Secure Connect.
dead-peer-detection	Dead Peer Detection (DPD) is enabled by default to allow the client to detect if the SRX Series Firewall is reachable and if the device is not reachable, disable the connection till reachability is restored.

Table 18: Remote User Settings Options *(Continued)*

Remote User Settings	Description
default -profile	If you configure a VPN connection profile as a **default-profile**, then you must enter only the gateway address in the Juniper Secure Connect application. It is optional to enter the realm name in Juniper Secure Connect application, as the application automatically selects default profile as realm name. In this example, enter *ra.example.com* in the **Gateway Address** field of the Juniper Secure Connect application. **NOTE**: Starting in Junos OS Release 23.1R1, we've hidden the `default-profile` option at the `[edit security remote-access]` hierarchy level. In releases before Junos OS Release 23.1R1, you use this option to specify one of the remote-access profiles as the default profile in Juniper Secure Connect. But with changes to the format of remote-access profile names, we no longer require the `default-profile` option. We've deprecated `default-profile` option—rather than immediately removing it—to provide backward compatibility and a chance to make your existing configuration conform to the changed configuration. You'll receive a warning message if you continue to use the `default-profile` option in your configuration. However existing deployments are not affected if you modify the current configuration. See default-profile (Juniper Secure Connect).

Configure `no-eap-tls` option to configure EAP-MSCHAPv2 authentication method to validate the user certificates.

```
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT no-eap-tls
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT certificate
warn-before-expiry 60
```

5. Configure the local gateway.

   a. Create address pool for client dynamic-IP assignment. See address-assignment (Access).

   - Enter the network address that you use for the address assignment.
   - Enter your DNS server address. Enter WINS server details, if required. Create the address range to assign IP addresses to the clients.
   - Enter the name, and the lower and higher limits.

```
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
```

```
network 192.168.2.0/24
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
range Range low 192.168.2.11
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
range Range high 192.168.2.100
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
xauth-attributes primary-dns 10.8.8.8/32
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
xauth-attributes primary-wins 192.168.4.10/32
```

b. Create access profile.

   For external user authentication, provide Radius Server IP Address, the Radius Secret, and Source Address for the radius communications to be sourced from. Configure radius for the authentication order.

```
user@host# set access profile Juniper_Secure_Connect authentication-order radius
user@host# set access profile Juniper_Secure_Connect address-assignment pool
Juniper_Secure_Connect_Addr-Pool
user@host# set access profile Juniper_Secure_Connect radius-server 192.168.3.10 port 1812
user@host# set access profile Juniper_Secure_Connect radius-server 192.168.3.10 secret
"$9$ggaGjmfzCtOHqtO1RlegoJ"
user@host# set access profile Juniper_Secure_Connect radius-server 192.168.3.10 timeout 5
user@host# set access profile Juniper_Secure_Connect radius-server 192.168.3.10 retry 3
user@host# set access firewall-authentication web-authentication default-profile
Juniper_Secure_Connect
```

c. Configure public key infrastructure (PKI) attributes. See pki.

```
user@host# set security pki ca-profile jweb-CA ca-identity jweb-CA
user@host# set security pki ca-profile jweb-CA enrollment url http://juniper-
ca.example.com/certsrv/
user@host# set security pki ca-profile jweb-CA enrollment retry 0
user@host# set security pki ca-profile jweb-CA enrollment retry-interval 0
user@host# set security pki ca-profile jweb-CA revocation-check disable
```

d. Create SSL termination profile. SSL termination is a process where the SRX Series Firewalls acts as an SSL proxy server, and terminates the SSL session from the client. 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. The server certificate is a local certificate identifier. Server certificates are used to authenticate the identity of a server.

```
user@host# set services ssl termination profile Juniper_SCC-SSL-Term-Profile server-
certificate JUNIPER_SECURE_CONNECT(RSA)
```

e. Create SSL VPN profile. See tcp-encap.

```
user@host# set security tcp-encap profile SSL-VPN ssl-profile Juniper_SCC-SSL-Term-Profile
```

f. Create firewall policies.

Create the security policy to permit traffic from the trust zone to the VPN zone.

```
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 match source-address any
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 match destination-address any
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 match application any
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 then permit
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 then log session-close
```

Create the security policy to permit traffic from the VPN zone to the trust zone.

```
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 match source-address any
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 match destination-address any
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 match application any
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 then permit
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 then log session-close
```

6. Configure Ethernet interface information.

```
user@host# set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/1 unit 0 family inet address 198.51.100.0/24
```

   Configure st0 interface with the family set as inet.

```
user@host# set interfaces st0 unit 0 family inet
```

7. Configure security zones.

```
user@host# set security zones security-zone trust host-inbound-traffic system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-0/0/0.0
user@host# set security zones security-zone vpn host-inbound-traffic system-services all
user@host# set security zones security-zone vpn host-inbound-traffic protocols all
user@host# set security zones security-zone VPN interface st0.0
user@host# set security zones security-zone vpn interfaces ge-0/0/1.0
```

8. Remote access configuration with remote user and local gateway is configured successfully.
9. Launch the Juniper Secure Connect application and provide the same IP address that you configured for external IP address in the Gateway Address field in the Juniper Secure Connect application.

   In this example, you've configured https://192.0.2.0/ as the external interface IP address for the clients to connect. You must enter this same IP address (https://192.0.2.0/) for the **Gateway Address** field in the Juniper Secure Connect application.

Result

From operational mode, confirm your configuration by entering the `show security`, `show access`, and `show security pki` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host> show security
   ike {
       proposal JUNIPER_SECURE_CONNECT {

           authentication-method rsa-signatures;
```

```
            dh-group group19;           encryption-algorithm aes-256-gcm;
            lifetime-seconds 28800;
        }
        policy JUNIPER_SECURE_CONNECT {
            mode main;

            proposals JUNIPER_SECURE_CONNECT;
            certificate {
                local-certificate SRX_Certificate;

            }
        }
        gateway JUNIPER_SECURE_CONNECT {
            ike-policy JUNIPER_SECURE_CONNECT;
            dynamic {
                hostname ra.example.com;
                ike-user-type shared-ike-id;
            }
            dead-peer-detection {
                optimized;
                interval 10;
                threshold 5;
            }
            external-interface ge-0/0/1;

            aaa {
                access-profile Juniper_Secure_Connect;
            }
            version v2-only;

            tcp-encap-profile SSL-VPN;
        }
    }
    ipsec {
        proposal JUNIPER_SECURE_CONNECT {


            encryption-algorithm aes-256-gcm;
            lifetime-seconds 3600;
        }
        policy JUNIPER_SECURE_CONNECT {
            perfect-forward-secrecy {
                keys group19;
            }
            proposals JUNIPER_SECURE_CONNECT;
        }
        vpn JUNIPER_SECURE_CONNECT {
            bind-interface st0.0;

            ike {
                gateway JUNIPER_SECURE_CONNECT;
                ipsec-policy JUNIPER_SECURE_CONNECT;
            }
            traffic-selector ts-1 {
                local-ip 0.0.0.0/0;
                remote-ip 0.0.0.0/0;
            }
        }
    }
    remote-access {
        profile ra.example.com {

            ipsec-vpn JUNIPER_SECURE_CONNECT;
            access-profile Juniper_Secure_Connect;
            client-config JUNIPER_SECURE_CONNECT;
        }
        client-config JUNIPER_SECURE_CONNECT {
            connection-mode manual;
            dead-peer-detection {
                interval 60;
                threshold 5;
            }
            no-eap-tls;
            certificate {
                warn-before-expiry 60;
            }
        }

    }

    policies {
        from-zone trust to-zone VPN {
            policy JUNIPER_SECURE_CONNECT-1 {
                match {
                    source-address any;
                    destination-address any;
```

```
                   application any;
               }
               then {
                   permit;
                   log {
                       session-close;
                   }
               }
           }
       }
       from-zone VPN to-zone trust {
           policy JUNIPER_SECURE_CONNECT-2 {
               match {
                   source-address any;
                   destination-address any;
                   application any;
               }
               then {
                   permit;
                   log {
                       session-close;
                   }
               }
           }
       }
   }
```

```
[edit]
user@host> show access
  access {
      profile Juniper_Secure_Connect {
          authentication-order radius;
          address-assignment {
              pool Juniper_Secure_Connect_Addr-Pool;
          }
          radius-server {
              192.168.3.10 {
                  port 1812;
                  secret "$9$ggaGjmfzCtOHqtO1RlegoJ"; ## SECRET-DATA
                  timeout 5;
                  retry 3;
              }
          }
      }
      address-assignment {
          pool Juniper_Secure_Connect_Addr-Pool {
              family inet {
                  network 192.168.2.0/24;
                  range Range {
                      low 192.168.2.11;
                      high 192.168.2.100;
                  }
                  xauth-attributes {
                      primary-dns 10.8.8.8/32;
                      primary-wins 192.168.4.10/32;
                  }
              }
          }
      }
      firewall-authentication {
          web-authentication {
              default-profile Juniper_Secure_Connect;
          }
      }
  }
```

```
[edit]
user@host> show security pki
   pki {
       ca-profile jweb-CA {
           ca-identity jweb-CA;
           enrollment {
               url http://juniper-ca.example.com/certsrv/;
               retry 0;
               retry-interval 0;
           }
           revocation-check {
               disable;
           }
       }
   }
```

```
[edit]
user@host> show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 192.0.2.0/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 198.51.100.0/24;
        }
    }
}
st0 {
    unit 1 {
        family inet;
    }
}
```

```
[edit]
user@host> show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
```

```
security-zone vpn {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
        ge-0/0/1.0;
    }
}
```

When you are done configuring the feature on your device, enter commit from configuration mode.

RELATED DOCUMENTATION

Local User Authentication Using Pre-shared Key (CLI Procedure) | **74**

External User Authentication (CLI Procedure) | **91**

Certificate-Based Validation Using EAP-TLS Authentication (CLI Procedure) | **145**

Certificate-Based Validation Using EAP-TLS Authentication (CLI Procedure)

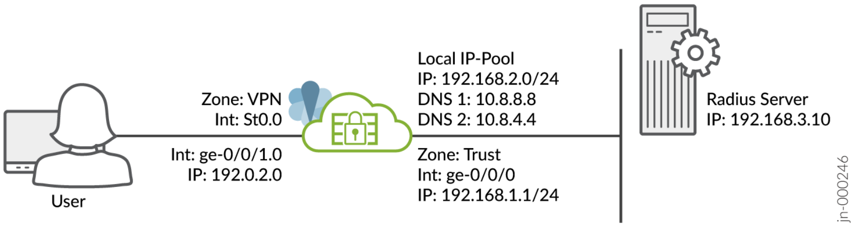
IN THIS SECTION

Overview

In this configuration, you use the EAP-TLS authentication method to validate the user certificates. You continue to use the username and password for external user authentication using the RADIUS server to download the initial configuration from the SRX Series Firewall.

We assume that you have completed the basic setup of your SRX Series Firewalls, including interfaces, zones, and security policies as illustrated in the Figure 21 on page 146.

Figure 21: Topology



For information about prerequisites, see "System Requirements for Juniper Secure Connect" on page 11.

Ensure that you have a Public Key Infrastructure (PKI) configured as the backend authentication. In this case, you need to install the root certificate of the CA on each client as well as a user specific certificate on each client device. Note that local authentication is not supported in this scenario.

You must ensure that the SRX Series Firewall uses either a signed certificate or a self-signed certificate instead of the default system-generated certificate. Before you start configuring Juniper Secure Connect, you must bind the certificate to the SRX Series Firewall by executing the following command:

```
user@host# set system services web-management https pki-local-certificate <cert_name>
```

For example:

```
user@host# set system services web-management https pki-local-certificate SRX_Certificate
```

Where *SRX_Certificate* is the self-signed certificate.

CLI Quick Configuration

To quickly configure this example on your SRX Series Firewalls, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
[edit]
user@host#
set security ike proposal JUNIPER_SECURE_CONNECT authentication-method rsa-signatures
set security ike proposal JUNIPER_SECURE_CONNECT dh-group group19
set security ike proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-gcm
set security ike proposal JUNIPER_SECURE_CONNECT lifetime-seconds 28800
set security ike policy JUNIPER_SECURE_CONNECT mode main
set security ike policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT
set security ike policy JUNIPER_SECURE_CONNECT certificate local-certificate SRX_Certificate

set security ike gateway JUNIPER_SECURE_CONNECT dynamic hostname ra.example.com
set security ike gateway JUNIPER_SECURE_CONNECT dynamic ike-user-type shared-ike-id
set security ike gateway JUNIPER_SECURE_CONNECT ike-policy JUNIPER_SECURE_CONNECT
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection optimized
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection interval 10
set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
set security ike gateway JUNIPER_SECURE_CONNECT version v2-only
set security ike gateway JUNIPER_SECURE_CONNECT aaa access-profile Juniper_Secure_Connect
set security ike gateway JUNIPER_SECURE_CONNECT tcp-encap-profile SSL-VPN
set security ike gateway JUNIPER_SECURE_CONNECT external-interface ge-0/0/0
set security ike gateway JUNIPER_SECURE_CONNECT local-address 192.0.2.0
set security ipsec proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-gcm
set security ipsec proposal JUNIPER_SECURE_CONNECT lifetime-seconds 3600
set security ipsec policy JUNIPER_SECURE_CONNECT perfect-forward-secrecy keys group19
set security ipsec policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT

set security ipsec vpn JUNIPER_SECURE_CONNECT bind-interface st0.0

set security ipsec vpn JUNIPER_SECURE_CONNECT ike gateway JUNIPER_SECURE_CONNECT
set security ipsec vpn JUNIPER_SECURE_CONNECT ike ipsec-policy JUNIPER_SECURE_CONNECT
set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 local-ip 0.0.0.0/0
set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 remote-ip 0.0.0.0/0

set security remote-access profile ra.example.com ipsec-vpn JUNIPER_SECURE_CONNECT
set security remote-access profile ra.example.com access-profile Juniper_Secure_Connect
set security remote-access profile ra.example.com client-config JUNIPER_SECURE_CONNECT
set security remote-access client-config JUNIPER_SECURE_CONNECT connection-mode manual
set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-detection interval 60
set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
set security remote-access client-config JUNIPER_SECURE_CONNECT certificate warn-before-expiry 60


set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet network
192.168.2.0/24
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet range Range low
192.168.2.11
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet range Range high
192.168.2.100
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet xauth-attributes
primary-dns 10.8.8.8/32
set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet xauth-attributes
primary-wins 192.168.4.10/32
set access profile Juniper_Secure_Connect authentication-order radius
set access profile Juniper_Secure_Connect address-assignment pool Juniper_Secure_Connect_Addr-
Pool
set access profile Juniper_Secure_Connect radius-server 192.168.3.10 port 1812
set access profile Juniper_Secure_Connect radius-server 192.168.3.10 secret
"$9$ggaGjmfzCtOHqtO1RlegoJ"
set access profile Juniper_Secure_Connect radius-server 192.168.3.10 timeout 5
set access profile Juniper_Secure_Connect radius-server 192.168.3.10 retry 3
set access firewall-authentication web-authentication default-profile Juniper_Secure_Connect

set security pki ca-profile jweb-CA ca-identity jweb-CA
set security pki ca-profile jweb-CA enrollment url http://juniper-ca.example.com/certsrv/
set security pki ca-profile jweb-CA enrollment retry 0
set security pki ca-profile jweb-CA enrollment retry-interval 0
set security pki ca-profile jweb-CA revocation-check disable

set services ssl termination profile Juniper_SCC-SSL-Term-Profile server-certificate
JUNIPER_SECURE_CONNECT(RSA)
set security tcp-encap profile SSL-VPN ssl-profile Juniper_SCC-SSL-Term-Profile

set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match source-
address any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match
destination-address any
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 match
application any
```

```
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 then permit
set security policies from-zone trust to-zone VPN policy JUNIPER_SECURE_CONNECT-1 then log
session-close
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match source-
address any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match
destination-address any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 match
application any
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 then permit
set security policies from-zone VPN to-zone trust policy JUNIPER_SECURE_CONNECT-2 then log
session-close

set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.0/24
set interfaces ge-0/0/1 unit 0 family inet address 198.51.100.0/24
set interfaces st0 unit 0 family inet

set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone vpn host-inbound-traffic system-services all
set security zones security-zone vpn host-inbound-traffic protocols all
set security zones security-zone VPN interface st0.0
set security zones security-zone vpn interfaces ge-0/0/1.0
```

Step-by-Step-Procedure

To configure VPN settings using the command line interface:

1. Log in to your SRX Series Firewall using the command line interface (CLI).
2. Enter the configuration mode.
3. Configure remote access VPN.

   For deploying Juniper Secure Connect, you must create a self-signed certificate and bind the certificate to the SRX Series Firewall. For more information, see "Get Started with Juniper Secure Connect" on page 10.

   IKE Configuration:

   a. Configure IKE proposal.

      Configure `rsa-signatures` as authentication method to configure certificate-based authentication.

Enable this option for the authentication process. IKEv2 requires EAP for user authentication. SRX Series Firewall cannot act as an EAP server. An external RADIUS server must be used for IKEv2 EAP to do the EAP authentication. SRX will act as a pass-through authenticator relaying EAP messages between the Juniper Secure Connect client and the RADIUS server.

EAP-TLS is enabled by default when you select the certificate-based authentication method.

Define IKE proposal authentication method, Diffie-Hellman group, and authentication algorithm.

```
user@host# set security ike proposal JUNIPER_SECURE_CONNECT authentication-method rsa-signatures
user@host# set security ike proposal JUNIPER_SECURE_CONNECT dh-group group19
user@host# set security ike proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-gcm
user@host# set security ike proposal JUNIPER_SECURE_CONNECT lifetime-seconds 28800
```

See proposal (Security IKE).

b. Configure IKE policy.

   Set the IKE Phase 1 policy mode, reference to the IKE proposal, and IKE Phase 1 policy authentication method.

```
user@host# set security ike policy JUNIPER_SECURE_CONNECT mode main
user@host# set security ike policy JUNIPER_SECURE_CONNECT proposals JUNIPER_SECURE_CONNECT
user@host# set security ike policy JUNIPER_SECURE_CONNECT certificate local-certificate SRX_Certificate
```

   See policy (Security IKE).

   To load a local certificate, specify a particular local certificate using the `set security ike policy` *`policy-name`* `certificate local-certificate` *`certificate-id`* command when the local device has multiple loaded certificates. You can select one of the already externally signed local certificates. In this example, *SRX_Certificate* is the existing local certificate that is loaded for `JUNIPER_SECURE_CONNECT` policy.

   If you don't have an existing local certificate, you can create one by following these steps:

   - Manually load a certificate authority (CA) digital certificate from a specified location. See request security pki ca-certificate load (Security).

```
user@host> request security pki ca-certificate load ca-profile ca-profile-name filename path/filename
```

- Manually load a local digital certificate from a specified location. See request security pki local-certificate load.

  ```
  user@host> request security pki local-certificate load filename local-certificate-name
  key key-name certificate-id SRX_Certificate
  ```

After creating a local certificate, you can attach the certificate to an IKE policy using the `set security ike policy` *`policy-name`* `certificate local-certificate` *`certificate-id`* command.

c. Configure IKE gateway options. See dynamic.

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dynamic hostname ra.example.com
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dynamic ike-user-type shared-
ike-id
user@host# set security ike gateway JUNIPER_SECURE_CONNECT ike-policy
JUNIPER_SECURE_CONNECT
```

If you do not configure the DPD values and the version information, the Junos OS assigns the default value for these options. See dead-peer-detection.

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection optimized
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection interval 10
user@host# set security ike gateway JUNIPER_SECURE_CONNECT dead-peer-detection threshold 5
user@host# set security ike gateway JUNIPER_SECURE_CONNECT version v2-only
user@host# set security ike gateway JUNIPER_SECURE_CONNECT aaa access-profile
Juniper_Secure_Connect

user@host# set security ike gateway JUNIPER_SECURE_CONNECT tcp-encap-profile SSL-VPN
```

Configure external interface IP address for the clients to connect. You must enter this same IP address (in this example: https://192.0.2.0) for the **Gateway Address** field in the Juniper Secure Connect application. See gateway.

```
user@host# set security ike gateway JUNIPER_SECURE_CONNECT external-interface ge-0/0/0
user@host# set security ike gateway JUNIPER_SECURE_CONNECT local-address 192.0.2.0
```

IPsec Configuration:

a. Configure IPsec proposal.

Specify the IPsec phase 2 proposal protocol, encryption algorithm, and other phase 2 options.

```
user@host# set security ipsec proposal JUNIPER_SECURE_CONNECT encryption-algorithm aes-256-
gcm
user@host# set security ipsec proposal JUNIPER_SECURE_CONNECT lifetime-seconds 3600
```

See proposal (Security IPsec).

b. Configure IPsec policy.

- Specify IPsec phase 2 PFS to use Diffie-Hellman group 19.
- Specify IPsec Phase 2 proposal reference.

```
user@host# set security ipsec policy JUNIPER_SECURE_CONNECT perfect-forward-secrecy keys
group19
user@host# set security ipsec policy JUNIPER_SECURE_CONNECT proposals
JUNIPER_SECURE_CONNECT
```

See policy (Security IPsec).

IPsec VPN Configuration:

a. Configure IPsec VPN parameters. See vpn (Security).

```
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT bind-interface st0.0
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT ike gateway JUNIPER_SECURE_CONNECT
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT ike ipsec-policy
JUNIPER_SECURE_CONNECT
```

b. Configure VPN traffic selectors. See traffic-selector.

```
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 local-ip
0.0.0.0/0
```

```
user@host# set security ipsec vpn JUNIPER_SECURE_CONNECT traffic-selector ts-1 remote-ip
0.0.0.0/0
```

4. Configure the remote user client options.

   a. Configure remote access profile. See remote-access.

```
user@host# set security remote-access profile ra.example.com ipsec-vpn
JUNIPER_SECURE_CONNECT
user@host# set security remote-access profile ra.example.com access-profile
Juniper_Secure_Connect
user@host# set security remote-access profile ra.example.com client-config
JUNIPER_SECURE_CONNECT
```

   b. Configure remote access client configuration. See client-config.

```
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT connection-mode
manual
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-
detection interval 60
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT dead-peer-
detection threshold 5
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT certificate
warn-before-expiry 60
user@host#
```

Table 19 on page 154 summarizes the remote user settings options.

Table 19: Remote User Settings Options

Remote User Settings	Description
connection-mode	To establish the client connection manually or automatically, configure the appropriate option. • If you configure **manual** option, then in the Juniper Secure Connect application, to establish a connection, you must either click the toggle button or select **Connection > Connect** from the menu. • If you configure **Always** option, then Juniper Secure Connect automatically establishes the connection. *Known Limitation:* **Android device**: If you use or select **Always**, then the configuration is downloaded from the first used SRX device. If the first SRX Series Firewall configuration changes or if you connect to a new SRX device, the configuration does not get downloaded to the Juniper Secure Connect application. This means that once you connect in the **Always** mode using the Android device, any configuration changes in the SRX Series Firewall do not take effect on Juniper Secure Connect.
dead-peer-detection	Dead Peer Detection (DPD) is enabled by default to allow the client to detect if the SRX Series Firewall is reachable and if the device is not reachable, disable the connection till reachability is restored.

Table 19: Remote User Settings Options *(Continued)*

Remote User Settings	Description
default -profile	If you configure a VPN connection profile as a **default-profile**, then you must enter only the gateway address in the Juniper Secure Connect application. It is optional to enter the realm name in Juniper Secure Connect application, as the application automatically selects default profile as realm name. In this example, enter *ra.example.com* in the **Gateway Address** field of the Juniper Secure Connect application. **NOTE**: Starting in Junos OS Release 23.1R1, we've hidden the `default-profile` option at the `[edit security remote-access]` hierarchy level. In releases before Junos OS Release 23.1R1, you use this option to specify one of the remote-access profiles as the default profile in Juniper Secure Connect. But with changes to the format of remote-access profile names, we no longer require the `default-profile` option. We've deprecated `default-profile` option—rather than immediately removing it—to provide backward compatibility and a chance to make your existing configuration conform to the changed configuration. You'll receive a warning message if you continue to use the `default-profile` option in your configuration. However existing deployments are not affected if you modify the current configuration. See default-profile (Juniper Secure Connect).

5. Configure the local gateway.

   a. Create address pool for client dynamic-IP assignment. See address-assignment (Access).

   - Enter the network address that you use for the address assignment.
   - Enter your DNS server address. Enter WINS server details, if required. Create the address range to assign IP addresses to the clients.
   - Enter the name, and the lower and higher limits.

```
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
network 192.168.2.0/24
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
range Range low 192.168.2.11
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
range Range high 192.168.2.100
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
xauth-attributes primary-dns 10.8.8.8/32
```

```
user@host# set access address-assignment pool Juniper_Secure_Connect_Addr-Pool family inet
xauth-attributes primary-wins 192.168.4.10/32
```

b. Create access profile.

For external user authentication, provide Radius Server IP Address, the Radius Secret, and Source Address for the radius communications to be sourced from. Configure radius for the authentication order.

```
user@host# set access profile Juniper_Secure_Connect authentication-order radius
user@host# set access profile Juniper_Secure_Connect address-assignment pool
Juniper_Secure_Connect_Addr-Pool
user@host# set access profile Juniper_Secure_Connect radius-server 192.168.3.10 port 1812
user@host# set access profile Juniper_Secure_Connect radius-server 192.168.3.10 secret
"$9$ggaGjmfzCtOHqtO1RlegoJ"
user@host# set access profile Juniper_Secure_Connect radius-server 192.168.3.10 timeout 5
user@host# set access profile Juniper_Secure_Connect radius-server 192.168.3.10 retry 3
user@host# set access firewall-authentication web-authentication default-profile
Juniper_Secure_Connect
```

c. Configure public key infrastructure (PKI) attributes. See pki.

```
user@host#
user@host# set security pki ca-profile jweb-CA ca-identity jweb-CA
user@host# set security pki ca-profile jweb-CA enrollment url http://juniper-
ca.example.com/certsrv/
user@host# set security pki ca-profile jweb-CA enrollment retry 0
user@host# set security pki ca-profile jweb-CA enrollment retry-interval 0
user@host# set security pki ca-profile jweb-CA revocation-check disable
```

d. Create SSL termination profile. SSL termination is a process where the SRX Series Firewalls acts as an SSL proxy server, and terminates the SSL session from the client. 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. The server certificate is a local certificate identifier. Server certificates are used to authenticate the identity of a server.

```
user@host# set services ssl termination profile Juniper_SCC-SSL-Term-Profile server-
certificate JUNIPER_SECURE_CONNECT(RSA)
```

e. Create SSL VPN profile. See tcp-encap

```
user@host# set security tcp-encap profile SSL-VPN ssl-profile Juniper_SCC-SSL-Term-Profile
```

f. Create firewall policies.

Create the security policy to permit traffic from the trust zone to the VPN zone.

```
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 match source-address any
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 match destination-address any
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 match application any
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 then permit
user@host# set security policies from-zone trust to-zone VPN policy
JUNIPER_SECURE_CONNECT-1 then log session-close
```

Create the security policy to permit traffic from the VPN zone to the trust zone.

```
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 match source-address any
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 match destination-address any
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 match application any
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 then permit
user@host# set security policies from-zone VPN to-zone trust policy
JUNIPER_SECURE_CONNECT-2 then log session-close
```

6. Configure Ethernet interface information.

```
user@host# set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.0/24
user@host# set interfaces ge-0/0/1 unit 0 family inet address 198.51.100.0/24
```

Configure st0 interface with the family set as inet.

```
user@host# set interfaces st0 unit 0 family inet
```

7. Configure security zones.

```
user@host# set security zones security-zone trust host-inbound-traffic system-services all
user@host# set security zones security-zone trust host-inbound-traffic protocols all
user@host# set security zones security-zone trust interfaces ge-0/0/0.0
user@host# set security zones security-zone vpn host-inbound-traffic system-services all
user@host# set security zones security-zone vpn host-inbound-traffic protocols all
user@host# set security zones security-zone VPN interface st0.0
user@host# set security zones security-zone vpn interfaces ge-0/0/1.0
```

8. Remote access configuration with remote user and local gateway is configured successfully.
9. Launch the Juniper Secure Connect application and provide the same IP address that you configured for external IP address in the Gateway Address field in the Juniper Secure Connect application.

   In this example, you've configured https://192.0.2.0/ as the external interface IP address for the clients to connect. You must enter this same IP address (https://192.0.2.0/) for the **Gateway Address** field in the Juniper Secure Connect application.

Result

From operational mode, confirm your configuration by entering the `show security`, `show access`, and `show security pki` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host> show security
   ike {
       proposal JUNIPER_SECURE_CONNECT {

           authentication-method rsa-signatures;
           dh-group group19;           encryption-algorithm aes-256-gcm;
           lifetime-seconds 28800;
       }
       policy JUNIPER_SECURE_CONNECT {
           mode main;
 ;
           proposals JUNIPER_SECURE_CONNECT;
```

```
            certificate {
                local-certificate SRX_Certificate;
            }
        }
        gateway JUNIPER_SECURE_CONNECT {
            ike-policy JUNIPER_SECURE_CONNECT;
            dynamic {
                hostname ra.example.com;
                ike-user-type shared-ike-id;
            }
            dead-peer-detection {
                optimized;
                interval 10;
                threshold 5;
            }
            external-interface ge-0/0/1;

            aaa {
                access-profile Juniper_Secure_Connect;
            }
            version v2-only;

            tcp-encap-profile SSL-VPN;
        }
    }
    ipsec {
        proposal JUNIPER_SECURE_CONNECT {


            encryption-algorithm aes-256-gcm;
            lifetime-seconds 3600;
        }
        policy JUNIPER_SECURE_CONNECT {

            perfect-forward-secrecy {
                keys group19;
            }
            proposals JUNIPER_SECURE_CONNECT;
        }
        vpn JUNIPER_SECURE_CONNECT {
            bind-interface st0.0;
            ike {
                gateway JUNIPER_SECURE_CONNECT;
                ipsec-policy JUNIPER_SECURE_CONNECT;
            }
            traffic-selector ts-1 {
                local-ip 0.0.0.0/0;
                remote-ip 0.0.0.0/0;
            }
        }
    }
    remote-access {
        profile ra.example.com {

            ipsec-vpn JUNIPER_SECURE_CONNECT;
            access-profile Juniper_Secure_Connect;
            client-config JUNIPER_SECURE_CONNECT;
        }
        client-config JUNIPER_SECURE_CONNECT {
            connection-mode manual;
            dead-peer-detection {
                interval 60;
                threshold 5;
            }
            certificate {
                warn-before-expiry 60;
            }
        }
           }

    policies {
        from-zone trust to-zone VPN {
            policy JUNIPER_SECURE_CONNECT-1 {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
        }
```

```
       from-zone VPN to-zone trust {
           policy JUNIPER_SECURE_CONNECT-2 {
               match {
                   source-address any;
                   destination-address any;
                   application any;
               }
               then {
                   permit;
                   log {
                       session-close;
                   }
               }
           }
       }
   }
```

```
[edit]
user@host> show access
  access {
      profile Juniper_Secure_Connect {
          authentication-order radius;
          address-assignment {
              pool Juniper_Secure_Connect_Addr-Pool;
          }
          radius-server {
              192.168.3.10 {
                  port 1812;
                  secret "$9$/2EhAuBcyKxNbIENbs2GU/Ct"; ## SECRET-DATA
                  timeout 5;
                  retry 3;
              }
          }
      }
      address-assignment {
          pool Juniper_Secure_Connect_Addr-Pool {
              family inet {
                  network 192.168.2.0/24;
                  range Range {
                      low 192.168.2.11;
                      high 192.168.2.100;
                  }
                  xauth-attributes {
                      primary-dns 10.8.8.8/32;
                      primary-wins 192.168.4.10/32;
                  }
              }
          }
      }
      firewall-authentication {
          web-authentication {
              default-profile Juniper_Secure_Connect;
          }
      }
  }
```

```
[edit]
user@host> show security pki
   pki {
       ca-profile jweb-CA {
           ca-identity jweb-CA;
           enrollment {
               url http://juniper-ca.example.com/certsrv/;
               retry 0;
               retry-interval 0;
           }
           revocation-check {
               disable;
           }
       }
   }
```

```
[edit]
user@host> show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 192.0.2.0/24;
        }
    }
}
```

```
ge-0/0/1 {
    unit 0 {
        family inet {
            address 198.51.100.0/24;
        }
    }
}
st0 {
    unit 1 {
        family inet;
    }
}
```

```
[edit]
user@host> show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone vpn {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
        ge-0/0/1.0;
    }
}
```

When you are done configuring the feature on your device, enter commit from configuration mode.

RELATED DOCUMENTATION

- Local User Authentication Using Pre-shared Key (CLI Procedure) | 74
- External User Authentication (CLI Procedure) | 91
- Certificate-Based Validation Using EAP-MSCHAPv2 Authentication (CLI Procedure) | 127

Local User Authentication Using Pre-shared Key

SUMMARY

In this configuration, you use the username and password for local user authentication. This configuration option does not allow you to change or recover your credentials without interacting with the firewall administrator, hence we do not recommended this authentication method. Instead, we recommend you to use "External User Authentication Using RADIUS" on page 173 method.

IN THIS SECTION

We assume that you have completed the basic setup of your SRX Series Firewalls, including interfaces, zones, and security policies as illustrated in the "Juniper Secure Connect Deployment Setup" on page 5.

For information about prerequisites, see "System Requirements for Juniper Secure Connect" on page 11.

NOTE: You must ensure that the SRX Series Firewall uses either a signed certificate or a self-signed certificate instead of the default system-generated certificate. Before you start configuring Juniper Secure Connect, it is important that you read the instructions in "Get Started with Juniper Secure Connect" on page 10.

Configure Juniper Secure Connect VPN Settings

To configure VPN settings using the J-Web interface:

1. Log in to your SRX Series Firewall using J-Web interface.

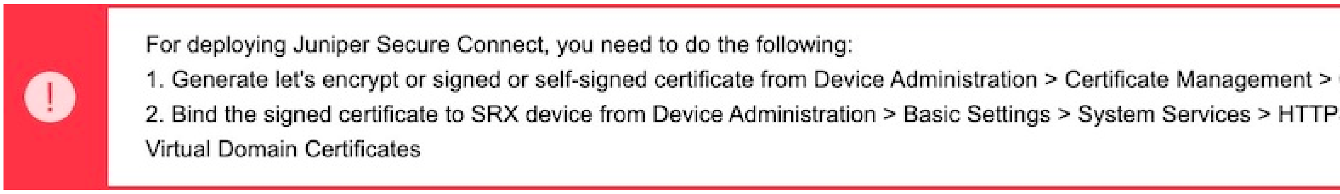
   After logging in successfully, you land on the Basic Settings page.
2. In the J-Web side pane, navigate to **Network** > **VPN** > **IPsec VPN**.

   a. After you click **IPsec VPN**, the IPsec VPN page appears.

   b. 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.

   The following warning message appears:

   Figure 22: Warning Message To Generate And Bind Self-signed Certificate



For deploying Juniper Secure Connect, you need to do the following:
1. Generate let's encrypt or signed or self-signed certificate from Device Administration > Certificate Management >
2. Bind the signed certificate to SRX device from Device Administration > Basic Settings > System Services > HTTP
Virtual Domain Certificates

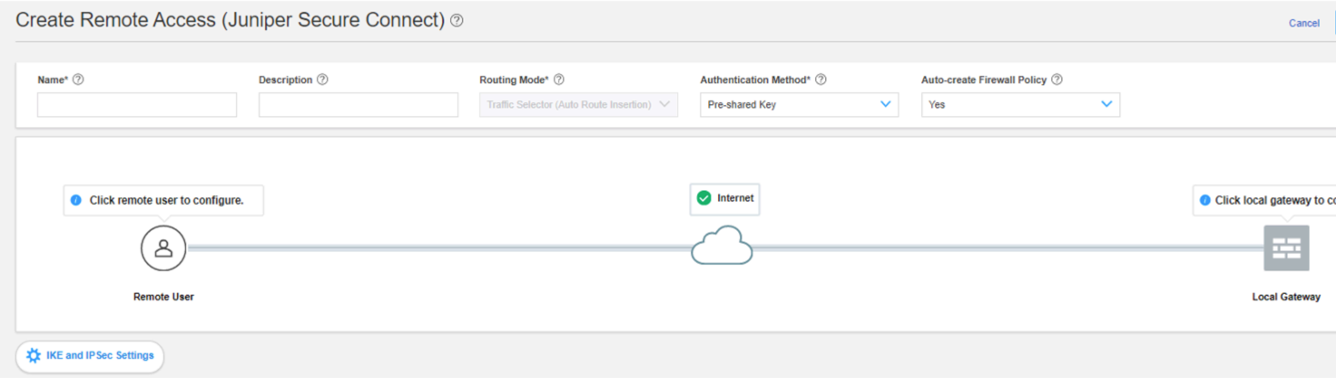
   As mentioned in the warning message, create a self-signed certificate and bind the certificate to the SRX Series Firewall. For more information, see "Deploy Certificates for Juniper Secure Connect" on page 14.

   For detailed information about creating a remote access VPN, see Create a Remote Access VPN—Juniper Secure Connect.

   c. Again navigate to **Network** > **VPN** > **IPsec VPN** and 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. The Create Remote Access (Juniper Secure Connect) page appears.

   Figure 23 on page 166 shows an example of the create remote access page with pre-shared key authentication method.

Figure 23: Create Remote Access Page For Pre-shared Key Authentication Method



Create Remote Access (Juniper Secure Connect)

Name*

Description

Routing Mode*: Traffic Selector (Auto Route Insertion)

Authentication Method*: Pre-shared Key

Auto-create Firewall Policy: Yes

3. On the Create Remote Access (Juniper Secure Connect) page (see Figure 23 on page 166):

   a. 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.

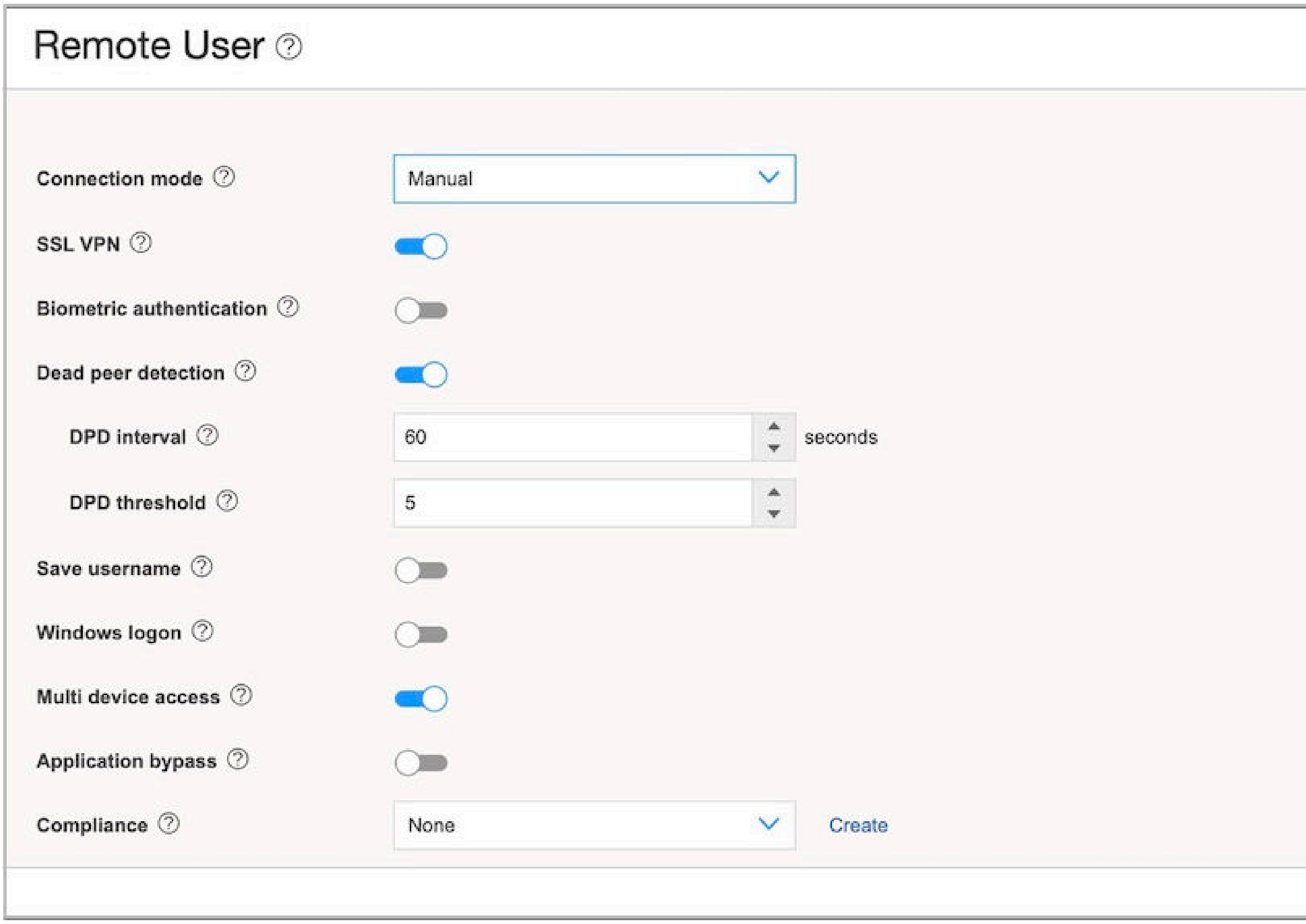
   b. The routing mode is set to **Traffic Selector (Auto Route Insertion)** by default.

   c. Select the authentication method. For this example, let's select **Pre-shared Key** from the drop-down list.

   d. Select **Yes** to create the firewall policy automatically using the **Auto-create Firewall Policy** option.

4. Click **Remote User** icon to configure the Juniper Secure Connect application settings.

Figure 24: Remote User Page



Remote User ?

Connection mode ?	Manual ⌄	
SSL VPN ?	●	
Biometric authentication ?	○	
Dead peer detection ?	●	
DPD interval ?	60	seconds
DPD threshold ?	5	
Save username ?	○	
Windows logon ?	○	
Multi device access ?	●	
Application bypass ?	○	
Compliance ?	None ⌄	Create

Figure 24 on page 167 shows an example of the Remote User page.

Configure the remote user client by selecting the options on the **Remote User** page and then clicking **OK** :

Table 20 on page 168 summarizes the remote user settings options.

Table 20: Remote User Settings Options

Remote User Settings	Description
Default Profile	The **Default Profile** is enabled by default. If you do not want this profile to be the default profile, click the toggle button. If you enable **Default Profile** for the VPN connection profile, Juniper Secure Connect automatically selects default profile as realm name (in this example: **https://192.0.2.12/**). In this case, it is optional to enter the realm name in Juniper Secure Connect. If you disable **Default Profile** for the VPN connection profile, you must enter the realm name along with the gateway address (in this example: **https://192.0.2.12/JUNIPER_SECURE_CONNECT**) in Juniper Secure Connect. **NOTE**: Starting in Junos OS 23.1R1 Release, default profile is deprecated in J-Web. However, in CLI—rather than immediately removing it—we provide backward compatibility and a chance to make your existing configuration conform to the changed configuration. You'll receive a warning message if you continue to use the default-profile option in your configuration. However existing deployments are not affected if you modify the current configuration using CLI. See default-profile (Juniper Secure Connect)
Connection Mode	To establish the client connection manually or automatically, select the appropriate option. • If you select **Manual**, then in the Juniper Secure Connect application, to establish a connection, you must either click the toggle button or select **Connection > Connect** from the menu. • If you select **Always**, then Juniper Secure Connect automatically establishes the connection. *Known Limitation:* **Android device**: If you use or select **Always**, then the configuration is downloaded from the first used SRX device. If the first SRX Series Firewall configuration changes or if you connect to a new SRX device, the configuration does not get downloaded to the Juniper Secure Connect application. This means that once you connect in the Always mode using the Android device, any configuration changes in the SRX Series Firewall do not take effect on Juniper Secure Connect.

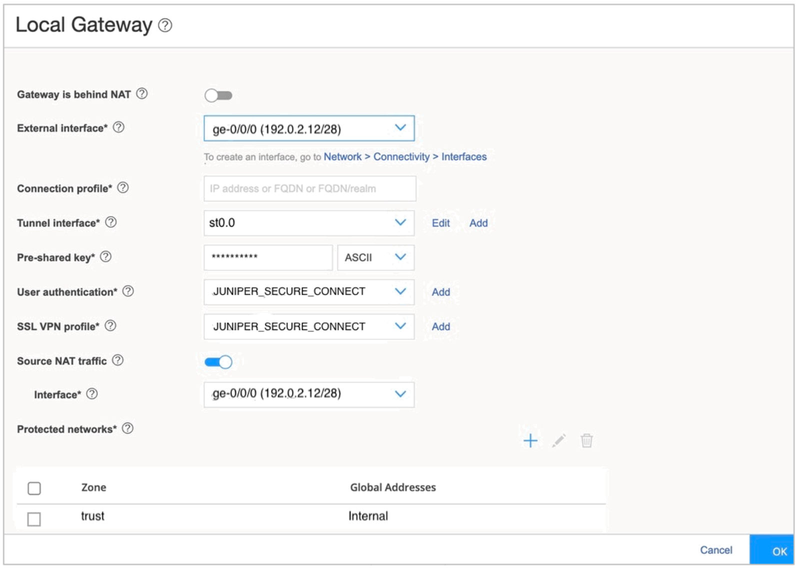
Table 20: Remote User Settings Options *(Continued)*

Remote User Settings	Description
SSL VPN	To enable support for SSL VPN connection from the Juniper Secure Connect application to the SRX Series Firewalls, click the toggle button. Use this option when IPsec ports are not allowed. By enabling **SSL VPN**, the client has the flexibility in connecting the SRX Series Firewalls. By default, **SSL VPN** is enabled.
Biometric authentication	This option is disabled by default. If you enable this option, when you click connect in Juniper Secure Connect, Juniper Secure Connect displays an authentication prompt. This option allows the user to protect their credentials using the operating system's built-in biometric authentication support.
Dead Peer Detection	Dead Peer Detection (DPD) is enabled by default to allow the client to detect if the SRX Series Firewall is reachable and if the device is not reachable, disable the connection till reachability is restored.
Save username	To save credentials on Juniper Secure Connect application, you can enable this option.
Windows Logon	This option allows users to logon to the local Windows system through an already established VPN tunnel (using Windows Pre-Logon), so that it is authenticated to the central Windows domain or Active Directory.
Multi device access	Provide multi access of a user from Juniper Secure Connect client using same credentials and same Gateway URL from different devices
Application bypass	To enables users of the Juniper Secure Connect application to bypass specific applications based on domain names and protocols, eliminating the need for the traffic to pass through the VPN tunnel, you select this option.
Compliance	If you enable this feature on your firewall, the Juniper Secure Connect application can establish the VPN connection based on the admission criteria that you configure. We recommend you enable this feature.

5. Click **Local Gateway** to configure the Local Gateway settings.

   Figure 25 on page 170 shows an example of the local gateway configuration settings.

Figure 25: Local Gateway Configuration



Local Gateway

Gateway is behind NAT: ○

External interface*: ge-0/0/0 (192.0.2.12/28)

To create an interface, go to Network > Connectivity > Interfaces

Connection profile*: IP address or FQDN or FQDN/realm

Tunnel interface*: st0.0 — Edit Add

Pre-shared key*: ********** ASCII

User authentication*: JUNIPER_SECURE_CONNECT — Add

SSL VPN profile*: JUNIPER_SECURE_CONNECT — Add

Source NAT traffic: ●

Interface*: ge-0/0/0 (192.0.2.12/28)

Protected networks*

□	Zone	Global Addresses
□	trust	Internal

a. 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.

b. For older J-Web versions, you need to enter an IKE ID in **user@hostname.com** format. For example, **abc@xyz.com**.

c. In the **External Interface** field, select the IP address for the clients to connect. You must enter this same IP address (in this example: **https://192.0.2.12/**) for the **Gateway Address** field in the Juniper Secure Connect application.

   If you enable **Gateway is behind NAT**, then the NAT IP address becomes the gateway address.

d. 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.

   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**.

e. Enter the preshared key in ASCII format. We do not support hexadecimal format for remote-access VPN.

f. 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.

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.

- 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 and the subnet that you use for the address assignment.
- Enter your DNS server address. Enter WINS server details, if required.
- 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.

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

g. 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.

- 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**.

h. 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.

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

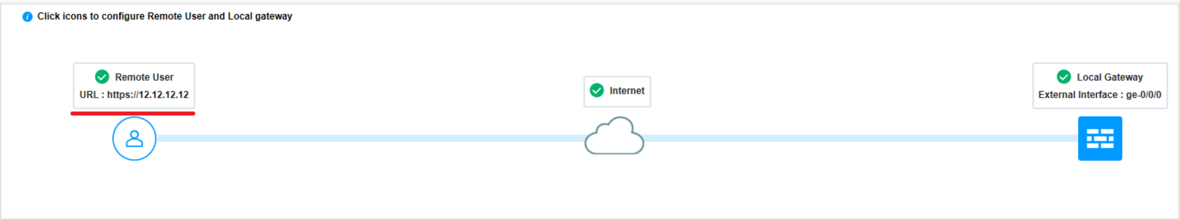
By default, any network 0.0.0.0/0 is allowed. If you configure a specific network, split tunneling for Juniper Secure Connect application is enabled. If you retain the default value, you can restrict access to your defined networks by adjusting the firewall policy from the client network. Click **OK**,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

6. You can now find the URL for the remote users to connect to. Copy and store this URL for sharing with your remote users. You need only the /xxxx information if this configuration is not your default profile.

   Figure 26 on page 172 highlights the URL that remote user must enter in the **Gateway address** field in Juniper Secure Connect application to establish remote access connection.

Figure 26: Commit Remote Access Configuration



Click icons to configure Remote User and Local gateway

Remote User
URL : https://12.12.12.12

Local Gateway
External Interface : ge-0/0/0

a. Click **Save** to complete the Juniper Secure Connect VPN configuration and associated policy if you have selected the auto policy creation option.

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

Download and install Juniper Secure Connect application on the client machine. Launch Juniper Secure Connect and connect to the gateway address of the SRX Series Firewall.

RELATED DOCUMENTATION

Juniper Secure Connect Overview | 1

External User Authentication Using RADIUS | 173

Certificate-Based Validation Using EAP-MSCHAPv2 Authentication | 189

Certificate-Based Validation Using EAP-TLS Authentication | 208

Monitor and Troubleshoot Juniper Secure Connect | 239

External User Authentication Using RADIUS

SUMMARY

This configuration is more secure as it allows you to use the same username and password as your domain login as well as change or recover your credentials without interacting with the firewall administrator. It also adds less workload on the administrator as the password must be changed frequently. We recommend you to use this configuration for authenticating the user.

IN THIS SECTION

We assume that you have completed the basic setup of your SRX Series Firewalls, including interfaces, zones, and security policies as illustrated in the "Juniper Secure Connect Deployment Setup" on page 5.

For information about prerequisites, see "System Requirements for Juniper Secure Connect" on page 11.

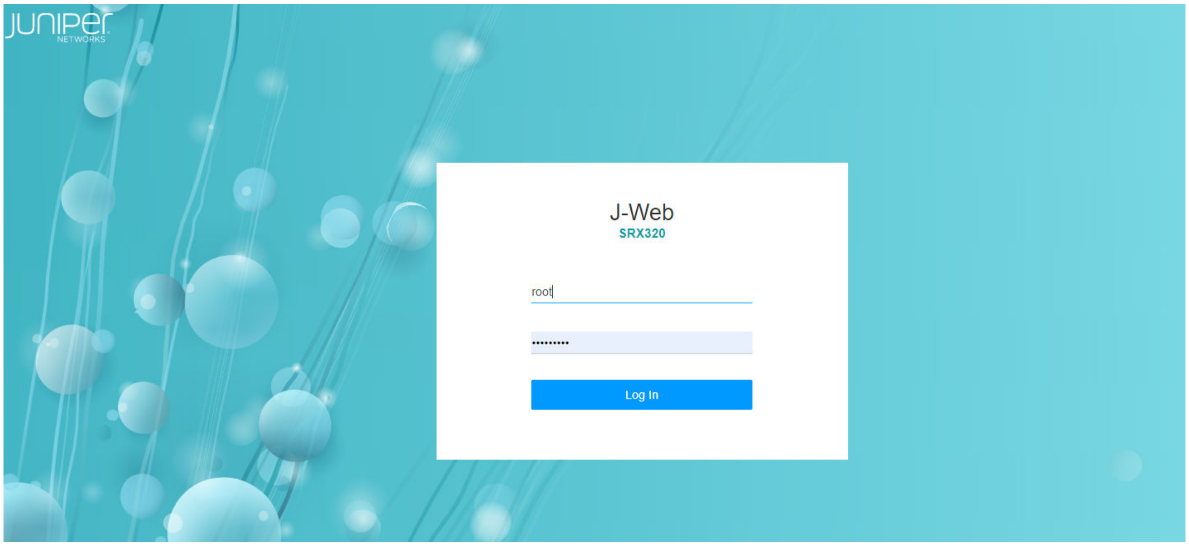
NOTE: You must ensure that the SRX Series Firewall uses either a signed certificate or a self-signed certificate instead of the default system-generated certificate. Before you start configuring Juniper Secure Connect, it is important that you read the instructions in "Get Started with Juniper Secure Connect" on page 10.

Configure Juniper Secure Connect VPN Settings

To configure VPN settings using the J-Web interface:

1. Log in to your SRX Series Firewall using J-Web interface. Figure 27 on page 174 shows J-Web login page.

Figure 27: J-Web Access and Login

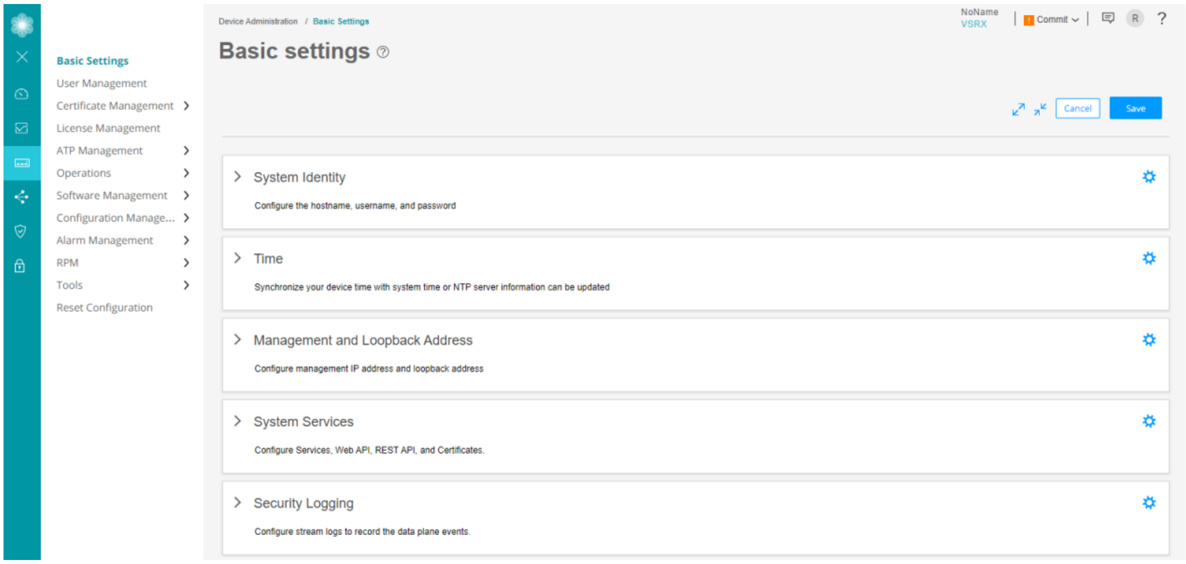


root

•••••••••

After logging in successfully, you land on the Basic Settings page. Figure 28 on page 174 shows an example of the landing page.

Figure 28: J-Web Landing Page



Basic settings

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

Configure Services, Web API, REST API, and Certificates.

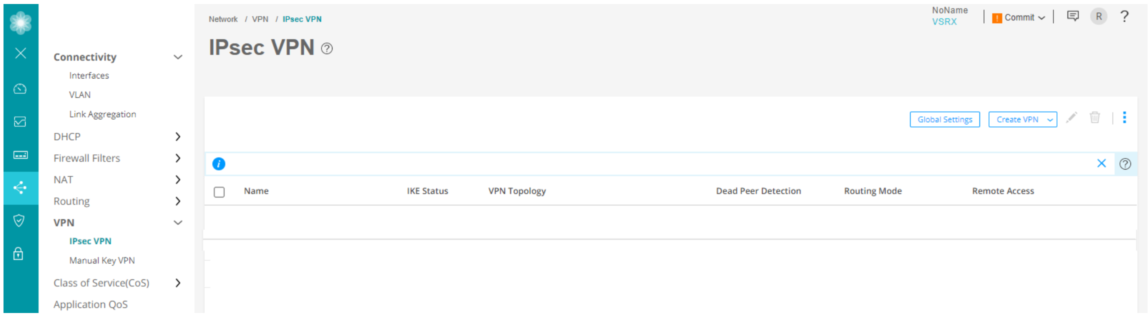
Security Logging

Configure stream logs to record the data plane events.

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

   a. After you click **IPsec VPN**, the IPsec VPN page appears. Figure 29 on page 175 shows an example of the **IPsec VPN** page.

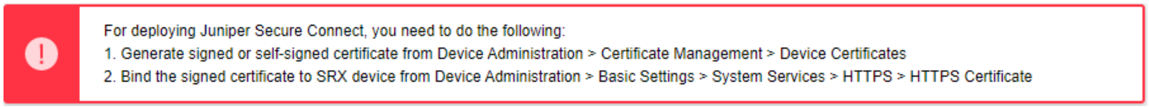
Figure 29: IPsec VPN Page



b. 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.

The following warning message appears:

Figure 30: Warning Message To Generate And Bind Self-signed Certificate



For deploying Juniper Secure Connect, you need to do the following:
1. Generate signed or self-signed certificate from Device Administration > Certificate Management > Device Certificates
2. Bind the signed certificate to SRX device from Device Administration > Basic Settings > System Services > HTTPS > HTTPS Certificate

As mentioned in the warning message, create a self-signed certificate and bind the certificate to the SRX Series Firewall. For more information, see "Deploy Certificates for Juniper Secure Connect" on page 14.

For detailed information about creating a remote access VPN, see Create a Remote Access VPN—Juniper Secure Connect.

c. Again navigate to **Network** > **VPN** > **IPsec VPN** and 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. The Create Remote Access (Juniper Secure Connect) page appears. Figure 31 on page 175 shows an example to create remote access VPN.

Figure 31: Create VPN - Remote Access

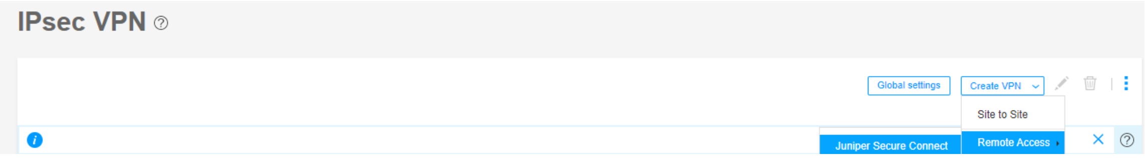
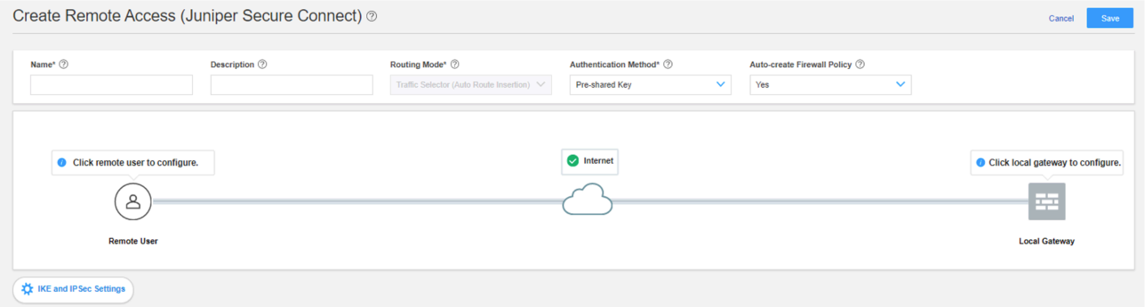


Figure 32 on page 176 shows an example of the create remote access page with pre-shared key authentication method.

Figure 32: Create Remote Access Page For Pre-shared Key Authentication Method



Create Remote Access (Juniper Secure Connect)

Name*:
Description:
Routing Mode*: Traffic Selector (Auto Route Insertion)
Authentication Method*: Pre-shared Key
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

3. On the Create Remote Access (Juniper Secure Connect) page (see Figure 33 on page 176):

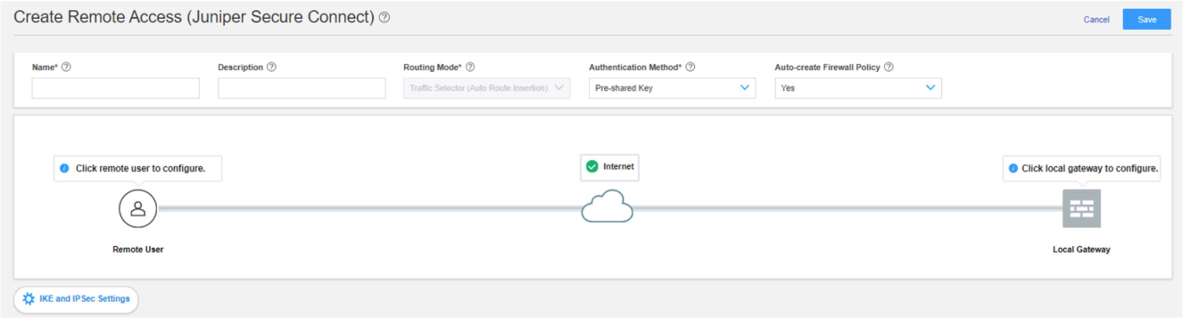
   a. Enter the name for the Remote Access Connection (this is, the name that will be displayed on the End Users Realm Name in Juniper Secure Connect application) and a description.

   b. The routing mode is set to **Traffic Selector (Auto Route Insertion)** by default.

   c. Select the authentication method. For this example, let's select **Pre-shared Key** from the drop-down menu.

   d. Select **Yes** to create the firewall policy automatically using the **Auto-create Firewall Policy** option.

Figure 33: Create Remote Access Page



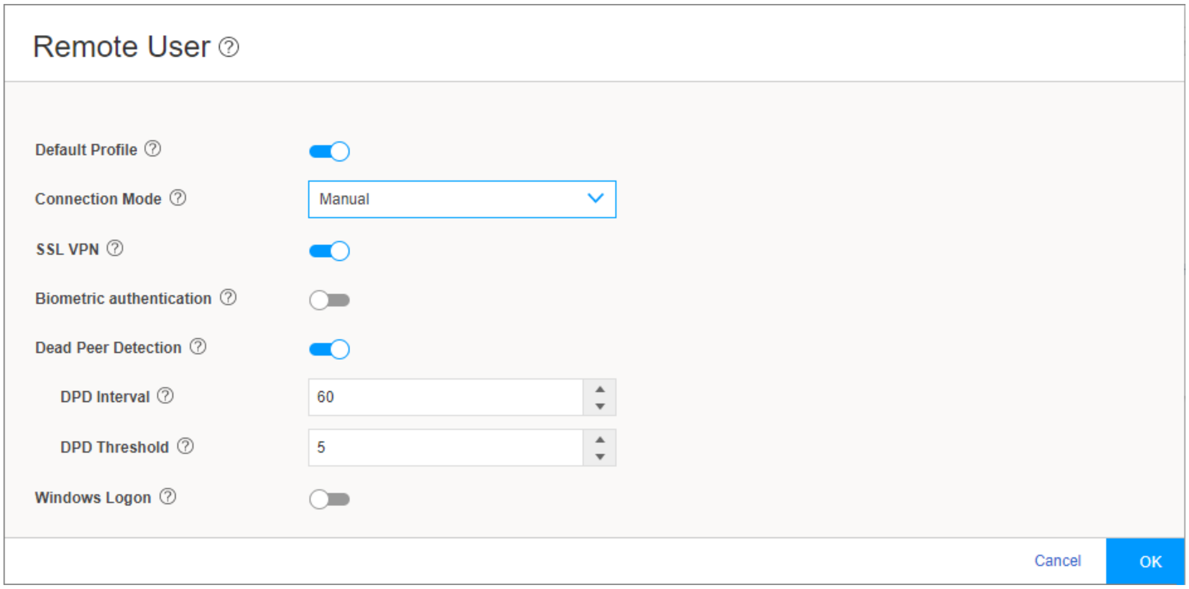
Create Remote Access (Juniper Secure Connect)

Name*:
Description:
Routing Mode*: Traffic Selector (Auto Route Insertion)
Authentication Method*: Pre-shared Key
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

4. Click **Remote User** icon to configure the Juniper Secure Connect application settings.

Figure 34: Remote User Page



Remote User

Default Profile	●
Connection Mode	Manual
SSL VPN	●
Biometric authentication	○
Dead Peer Detection	●
DPD Interval	60
DPD Threshold	5
Windows Logon	○

Figure 34 on page 177 shows an example of the Remote User page.

Configure the remote user client by selecting the options on the **Remote User** page and then clicking **OK** :

Table 21 on page 178 summarizes the remote user settings options.

Table 21: Remote User Client Settings Options

Remote User Client Settings	Description
Default Profile	The **Default Profile** is enabled by default. If you do not want this profile to be the default profile, click the toggle button. If you enable **Default Profile** for the VPN connection profile, Juniper Secure Connect automatically selects default profile as realm name (in this example: **https://12.12.12.12/**). In this case, it is optional to enter the realm name in Juniper Secure Connect. If you disable **Default Profile** for the VPN connection profile, you must enter the realm name along with the gateway address (in this example: **https://12.12.12.12/JUNIPER_SECURE_CONNECT**) in Juniper Secure Connect. **NOTE**: Starting in Junos OS 23.1R1 Release, default profile is deprecated in J-Web. However, in CLI—rather than immediately removing it—we provide backward compatibility and a chance to make your existing configuration conform to the changed configuration. You'll receive a warning message if you continue to use the default-profile option in your configuration. However existing deployments are not affected if you modify the current configuration using CLI. See default-profile (Juniper Secure

Table 21: Remote User Client Settings Options *(Continued)*

Remote User Client Settings	Description
Connection Mode	To establish the client connection manually or automatically, select the appropriate option. • If you select **Manual**, then in the Juniper Secure Connect application, to establish a connection, you must either click the toggle button or select **Connection > Connect** from the menu. • If you select **Always**, then Juniper Secure Connect automatically establishes the connection. *Known Limitation:* **Android device**: If you use or select **Always**, then the configuration is downloaded from the first used SRX device. If the first SRX Series Firewall configuration changes or if you connect to a new SRX device, the configuration does not get downloaded to the Juniper Secure Connect application. This means that once you connect in the Always mode using the Android device, any configuration changes in the SRX Series Firewall do not take effect on Juniper Secure Connect.
SSL VPN	To enable support for SSL VPN connection from the Juniper Secure Connect application to the SRX Series Firewalls, click the toggle button. Use this option when IPsec ports are not allowed. By enabling **SSL VPN**, the client has the flexibility in connecting the SRX Series Firewalls. By default, **SSL VPN** is enabled.
Biometric authentication	This option is disabled by default. If you enable this option, when you click connect in Juniper Secure Connect, Juniper Secure Connect displays an authentication prompt. This option allows the user to protect their credentials using the operating system's built-in biometric authentication support.
Dead Peer Detection	Dead Peer Detection (DPD) is enabled by default to allow the client to detect if the SRX Series Firewall is not reachable, disable the connection till reachability is restored.

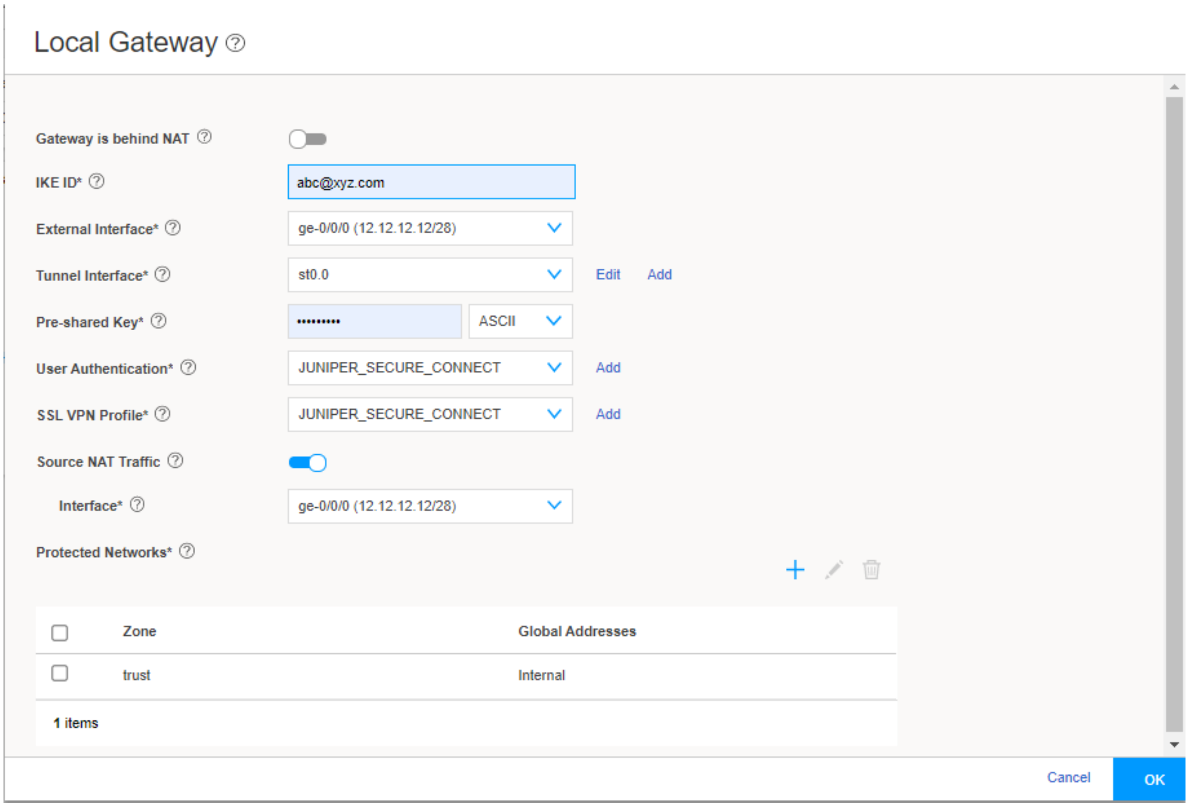
Table 21: Remote User Client Settings Options *(Continued)*

Remote User Client Settings	Description
Windows Logon	This option allows users to logon to the local Windows system through an already established VPN tunnel (using Windows Pre-Logon), so that it is authenticated to the central Windows domain or Active Directory.

5. Click **Local Gateway** to configure the Local Gateway settings.

   Figure 35 on page 180 shows an example of the local gateway configuration settings.

Figure 35: Local Gateway Configuration



Local Gateway ⓘ

Gateway is behind NAT ⓘ ○

IKE ID* ⓘ abc@xyz.com

External Interface* ⓘ ge-0/0/0 (12.12.12.12/28)

Tunnel Interface* ⓘ st0.0 Edit Add

Pre-shared Key* ⓘ ••••••••• ASCII

User Authentication* ⓘ JUNIPER_SECURE_CONNECT Add

SSL VPN Profile* ⓘ JUNIPER_SECURE_CONNECT Add

Source NAT Traffic ⓘ ●

Interface* ⓘ ge-0/0/0 (12.12.12.12/28)

Protected Networks* ⓘ

□	Zone	Global Addresses
□	trust	Internal

1 items

a. 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.

b. Enter a IKE ID in **user@hostname.com** format. For example, **abc@xyz.com**.

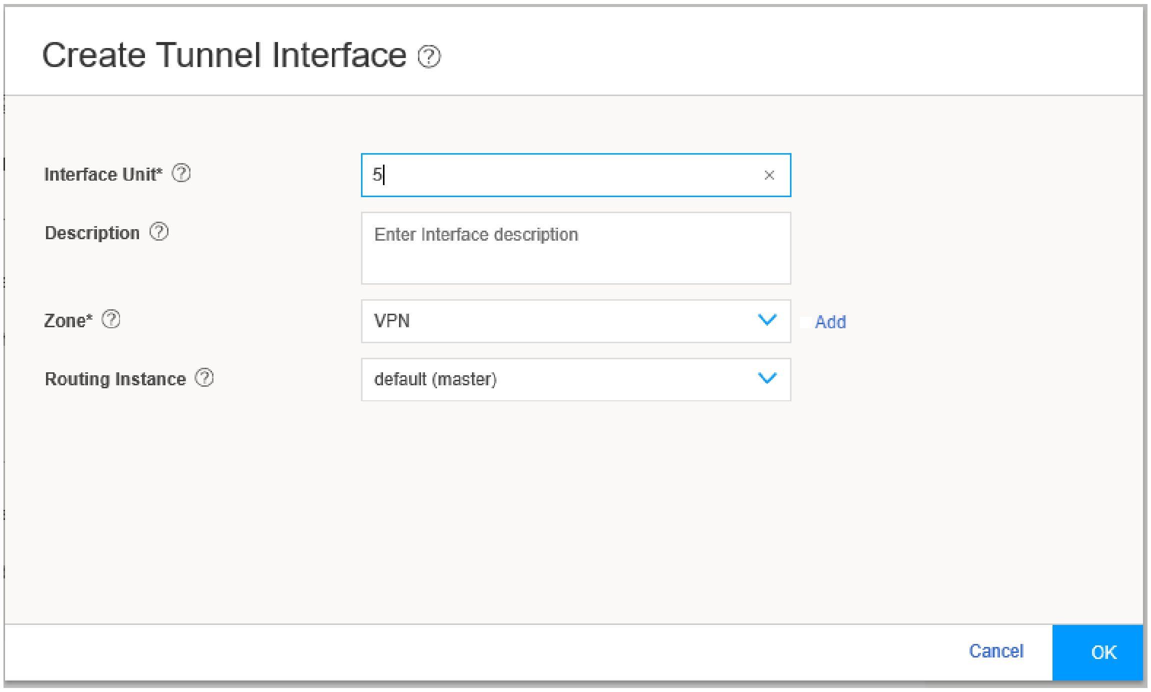
c. In the **External Interface** field, select the IP address for the clients to connect. You must enter this same IP address (in this example: **https://12.12.12.12/**) for the **Gateway Address** field in the Juniper Secure Connect application.

   If you enable **Gateway is behind NAT**, then the NAT IP address becomes the gateway address.

d. 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.

   Figure 36 on page 181 shows an example of the Create Tunnel Interface page.

   Figure 36: Create Tunnel Interface Page



Create Tunnel Interface ?

Interface Unit* ? 5

Description ? Enter Interface description

Zone* ? VPN Add

Routing Instance ? default (master)

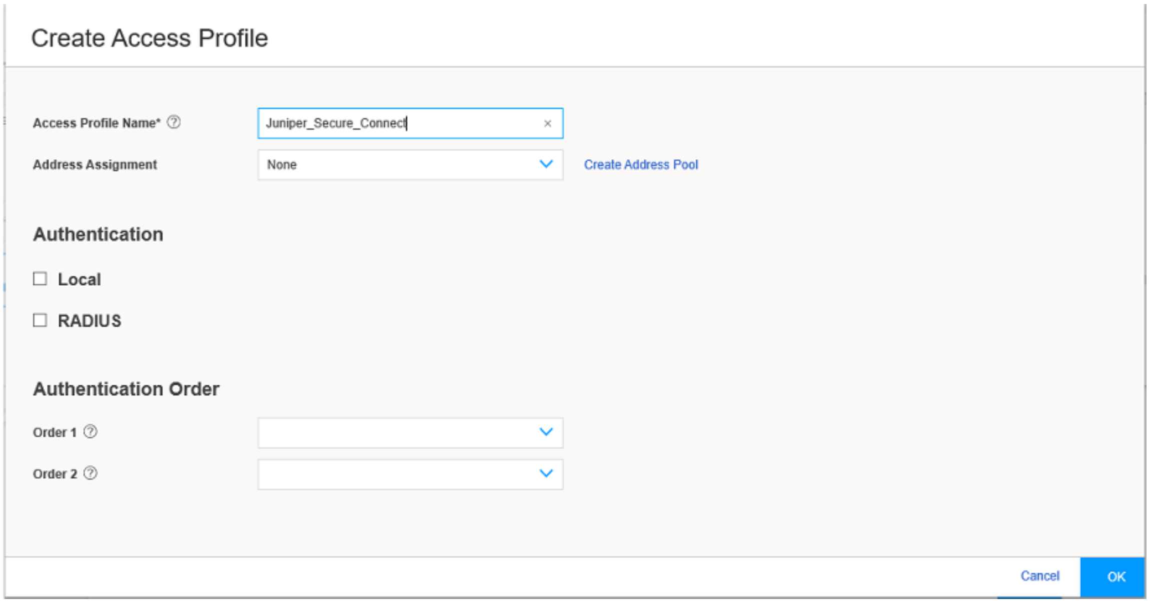
   The next available ST0 logical interface number is displayed in the Interface Unit field and you can enter a description for this interface. Select the zone to add this tunnel interface to. If **Auto-create Firewall Policy** (in Create Remote Access page) is set to **Yes**, the firewall policy uses this zone. Click **OK**.

e. Enter the preshared key in ASCII format. We do not support hexadecimal format for remote-access VPN.

f. 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.

   Figure 37 on page 182 shows an example of the Create Access Profile page.

Figure 37: Create Access Profile Page



Create Access Profile

Access Profile Name* Juniper_Secure_Connect

Address Assignment None

Authentication

□ Local

□ RADIUS

Authentication Order

Order 1

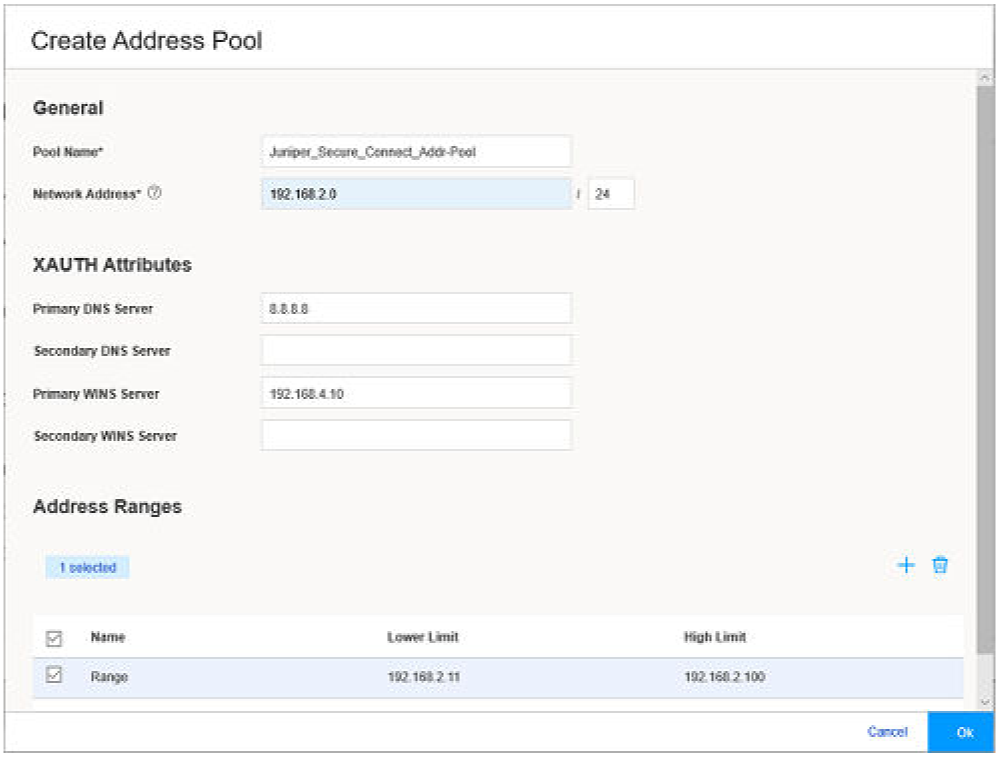
Order 2

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.

The **Create Address Pool** window appears.

Figure 38 on page 183 shows an example of the Create Address Pool page.

Figure 38: Create Address Pool Page



Create Address Pool

General

Pool Name*: Juniper_Secure_Connect_Addr-Pool

Network Address*: 192.168.2.0 / 24

XAUTH Attributes

Primary DNS Server: 8.8.8.8

Secondary DNS Server:

Primary WINS Server: 192.168.4.10

Secondary WINS Server:

Address Ranges

1 selected

☑	Name	Lower Limit	High Limit
☑	Range	192.168.2.11	192.168.2.100

- 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.

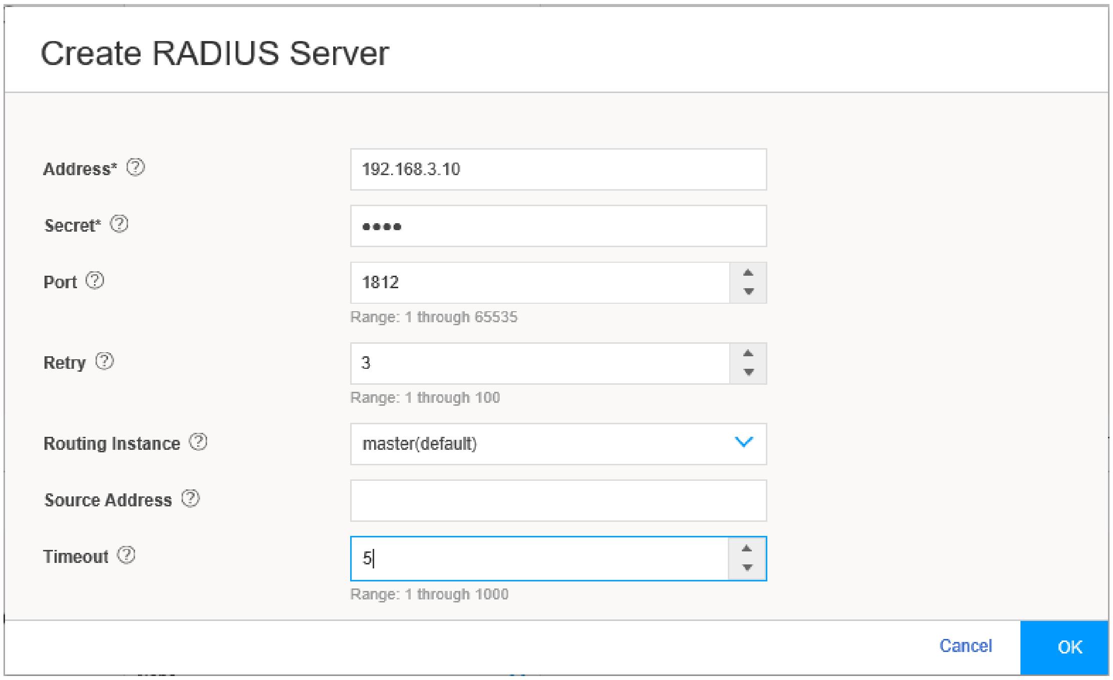
- Enter your DNS server address. Enter WINS server details, if required. Now click the add icon (+) to create the address range to assign IP addresses to the clients.

- Enter the name, and the lower and higher limits. After entering the details, click **OK**.

Select the **RADIUS** check box, where all the authentication details are stored on an external radius server.

- Click the add icon (+) to configure the radius server details. See Figure 39 on page 184.

Figure 39: Create RADIUS Server Page



Create RADIUS Server

Address* ⓘ 192.168.3.10

Secret* ⓘ ●●●●

Port ⓘ 1812

Range: 1 through 65535

Retry ⓘ 3

Range: 1 through 100

Routing Instance ⓘ master(default)

Source Address ⓘ

Timeout ⓘ 5

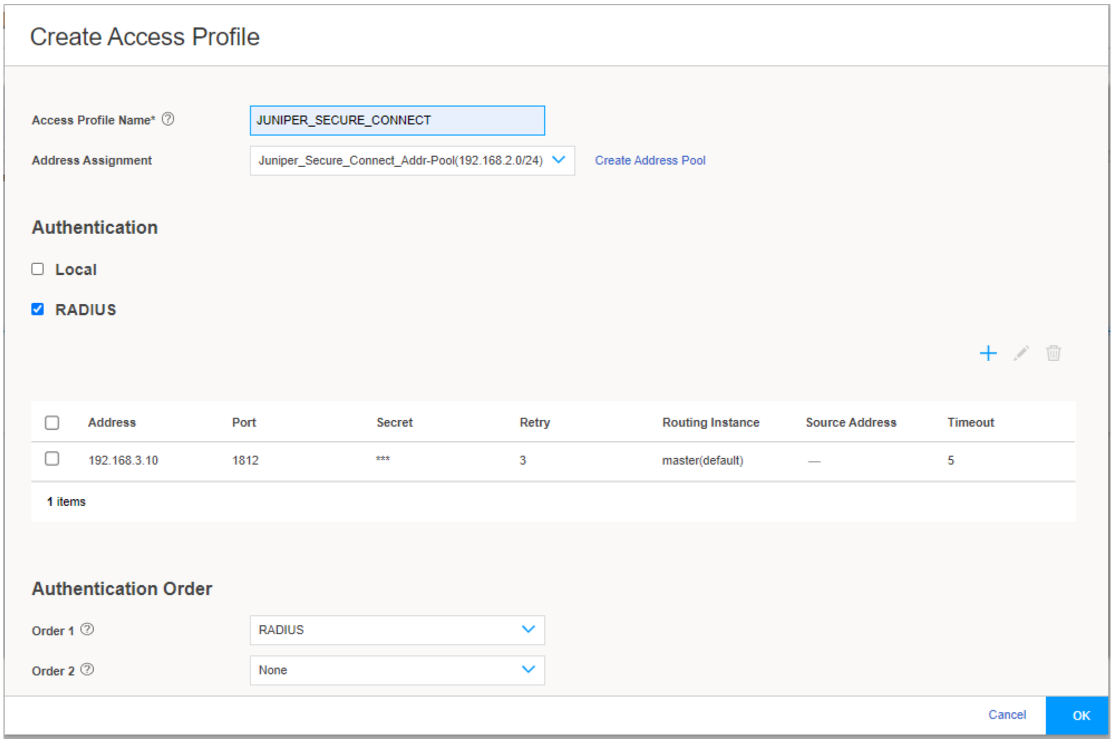
Range: 1 through 1000

- Enter the Radius Server IP Address, the Radius Secret, and Source Address for the radius communications to be sourced from. Click **OK**.

  In the **Authentication Order**, from **Order 1** drop-down list select **RADIUS**. Click **OK** to complete the access profile configuration.

  Figure 40 on page 185 shows an example of Create Access Profile page.

Figure 40: Create Access Profile Page



Create Access Profile

Access Profile Name* JUNIPER_SECURE_CONNECT

Address Assignment Juniper_Secure_Connect_Addr-Pool(192.168.2.0/24)

Authentication

□ Local

☑ RADIUS

□	Address	Port	Secret	Retry	Routing Instance	Source Address	Timeout
□	192.168.3.10	1812	***	3	master(default)	—	5

1 items

Authentication Order

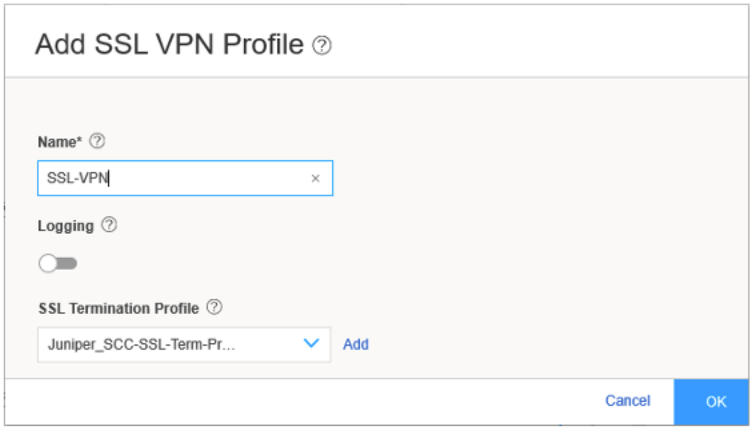
Order 1 RADIUS

Order 2 None

g. 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.

Figure 41 on page 185 shows an example of the Add SSL VPN Profile page.

Figure 41: Add SSL VPN Profile Page



Add SSL VPN Profile

Name* SSL-VPN

Logging ○ (off)

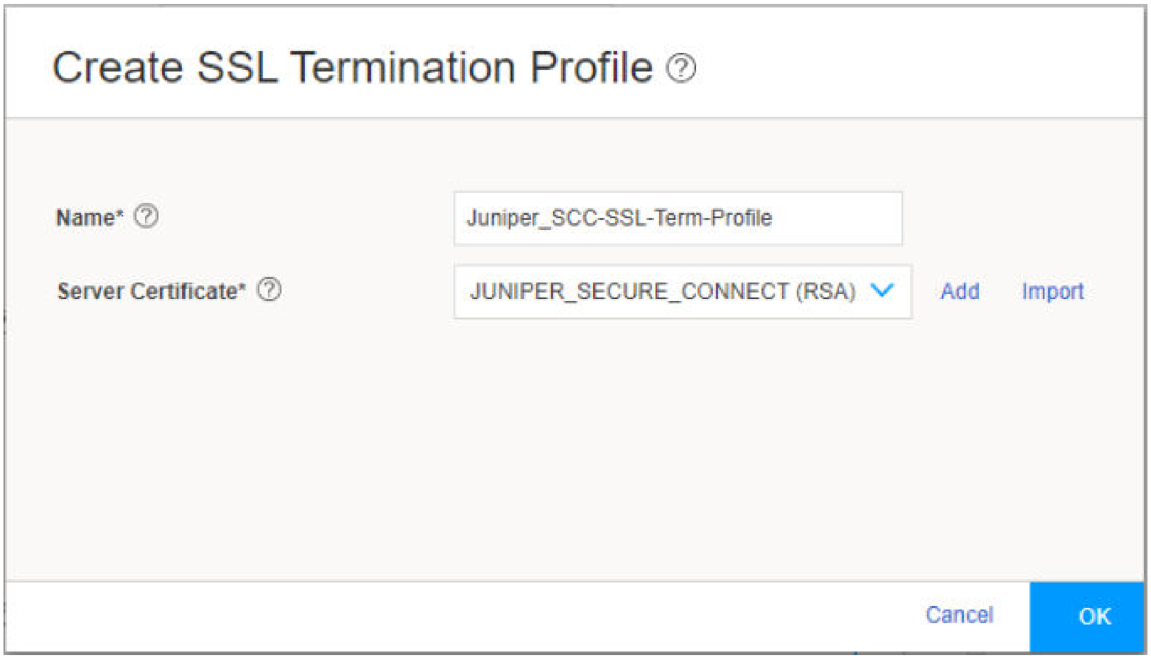
SSL Termination Profile Juniper_SCC-SSL-Term-Pr...

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 dropdown 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.

Figure 42 on page 186 shows an example of the Create SSL Termination Profile page.

Figure 42: Create SSL Termination Profile Page



Create SSL Termination Profile

Name*: Juniper_SCC-SSL-Term-Profile

Server Certificate*: JUNIPER_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.

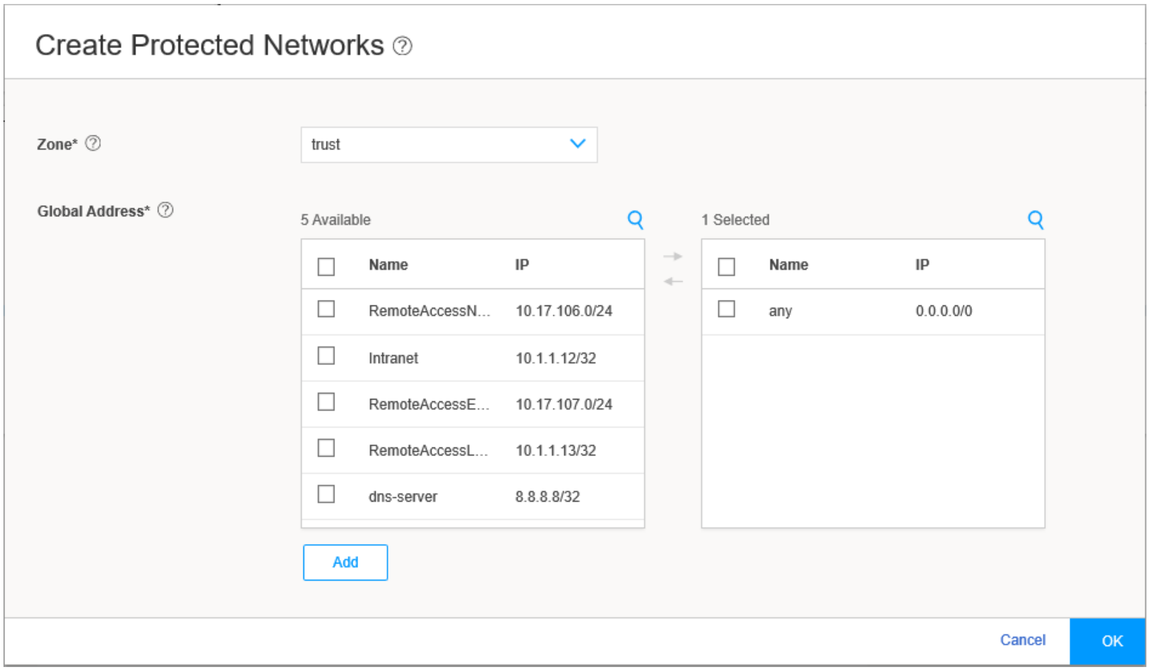
- Click **OK**.

h. 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.

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

Figure 43 on page 187 shows an example of the **Create Protected Networks** page.

Figure 43: Create Protected Networks Page



Create Protected Networks

Zone*: trust

Global Address*

5 Available

□	Name	IP
□	RemoteAccessN...	10.17.106.0/24
□	Intranet	10.1.1.12/32
□	RemoteAccessE...	10.17.107.0/24
□	RemoteAccessL...	10.1.1.13/32
□	dns-server	8.8.8.8/32

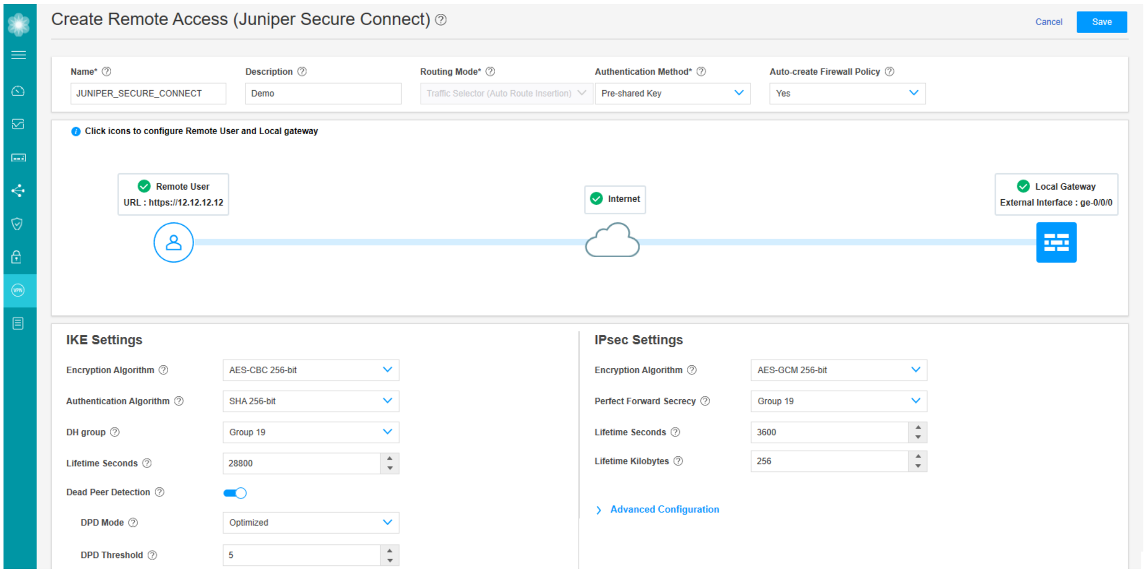
1 Selected

□	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.

Figure 44 on page 188 shows an example of successful completion of remote access configuration with remote user and local gateway.

Figure 44: Complete Remote Access Configuration



Create Remote Access (Juniper Secure Connect)

Name*: JUNIPER_SECURE_CONNECT
Description: Demo
Routing Mode*: Traffic Selector (Auto Route Insertion)
Authentication Method*: Pre-shared Key
Auto-create Firewall Policy: Yes

Click icons to configure Remote User and Local gateway

Remote User
URL : https://12.12.12.12

Internet

Local Gateway
External Interface : ge-0/0/0

IKE Settings

Encryption Algorithm: AES-CBC 256-bit
Authentication Algorithm: SHA 256-bit
DH group: Group 19
Lifetime Seconds: 28800
Dead Peer Detection: ●
DPD Mode: Optimized
DPD Threshold: 5

IPsec Settings

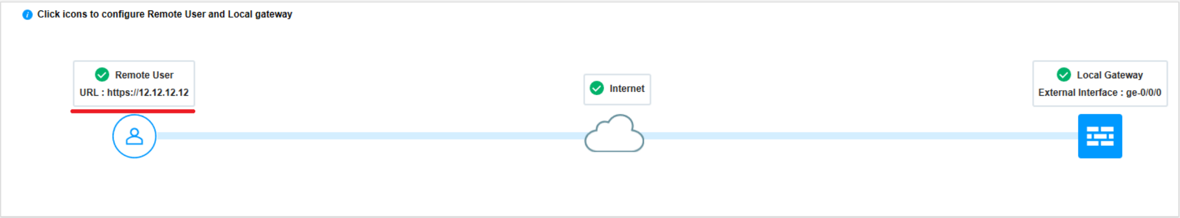
Encryption Algorithm: AES-GCM 256-bit
Perfect Forward Secrecy: Group 19
Lifetime Seconds: 3600
Lifetime Kilobytes: 256

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.

6. You can now find the URL for the remote users to connect to. Copy and store this URL for sharing with your remote users. You need only the /xxxx information if this configuration is not your default profile.

   Figure 45 on page 188 highlights the URL that remote user must enter in the **Gateway address** field in Juniper Secure Connect application to establish remote access connection.

Figure 45: Commit Remote Access Configuration



Click icons to configure Remote User and Local gateway

Remote User
URL : https://12.12.12.12

Internet

Local Gateway
External Interface : ge-0/0/0

a. Click **Save** to complete the Juniper Secure Connect VPN configuration and associated policy if you have selected the auto policy creation option.

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

Download and install Juniper Secure Connect application on the client machine. Launch Juniper Secure Connect and connect to the gateway address of the SRX Series Firewall.

RELATED DOCUMENTATION

Juniper Secure Connect Overview | 1

Local User Authentication Using Pre-shared Key | 164

Certificate-Based Validation Using EAP-MSCHAPv2 Authentication | 189

Certificate-Based Validation Using EAP-TLS Authentication | 208

Monitor and Troubleshoot Juniper Secure Connect | 239

Certificate-Based Validation Using EAP-MSCHAPv2 Authentication

SUMMARY

The EAP-MSCHAPv2 authentication method uses the username and the password for authenticating the user by using the RADIUS server. You use these credentials to download the initial configuration from the SRX Series Firewall. The firewall authenticates the user by using the RADIUS server during remote-access VPN IKE negotiation process.

IN THIS SECTION

We assume that you have completed the basic setup of your SRX Series Firewalls, including interfaces, zones, and security policies as illustrated in the "Juniper Secure Connect Deployment Setup" on page 5.

For information about prerequisites, see "System Requirements for Juniper Secure Connect" on page 11.

Ensure that you have a Public Key Infrastructure (PKI) configured as the back-end authentication. In this case, you only need to install the root certificate of the CA on each client. Note that we do not support local authentication in this scenario.

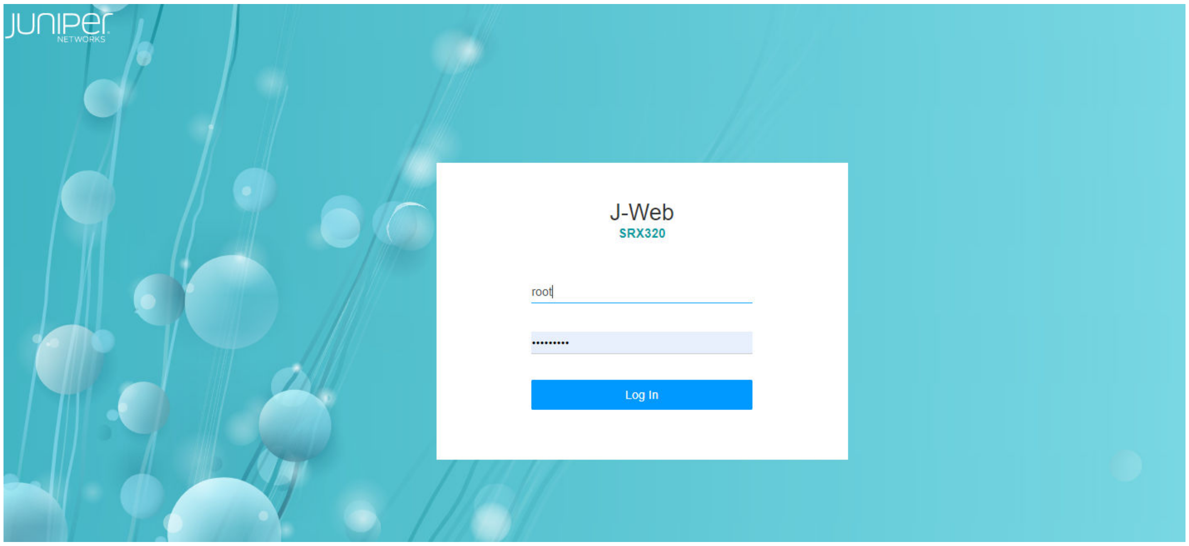
NOTE: You must ensure that the SRX Series Firewall uses either a signed certificate or a self-signed certificate instead of the default system-generated certificate. Before you start configuring Juniper Secure Connect, it is important that you read the instructions in "Get Started with Juniper Secure Connect" on page 10.

Configure Juniper Secure Connect VPN Settings

To configure VPN settings using the J-Web interface:

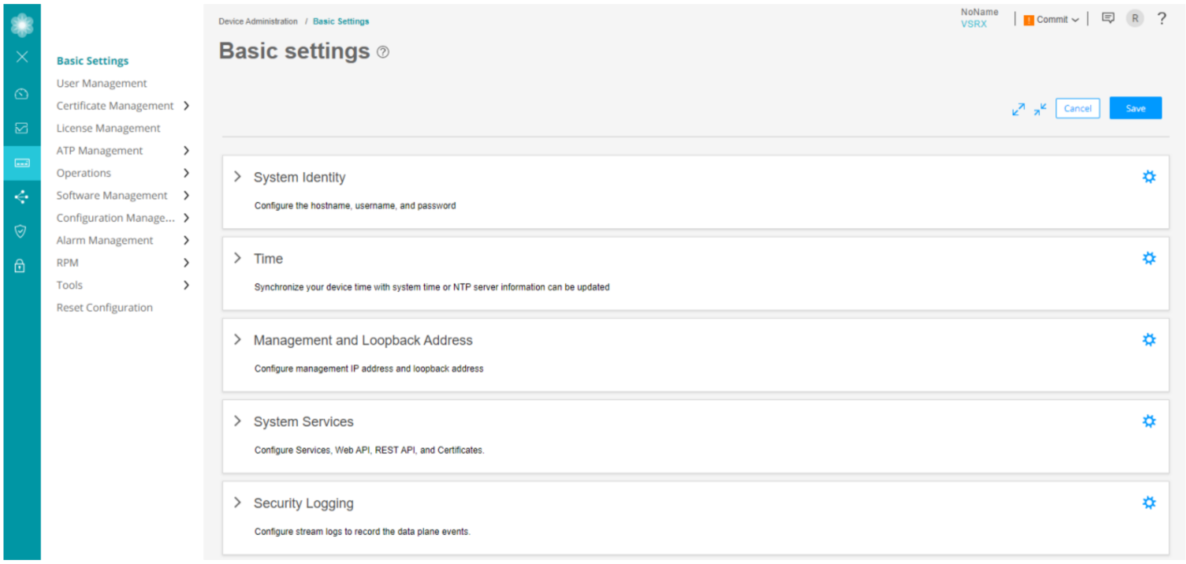
1. Log in to your SRX Series Firewall using J-Web interface. Figure 46 on page 190 shows J-Web login page.

   Figure 46: J-Web Access and Login



   After logging in successfully, you land on the Basic Settings page. Figure 47 on page 191 shows an example of the landing page.

Figure 47: J-Web Landing Page



Basic settings

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

Configure Services, Web API, REST API, and Certificates.

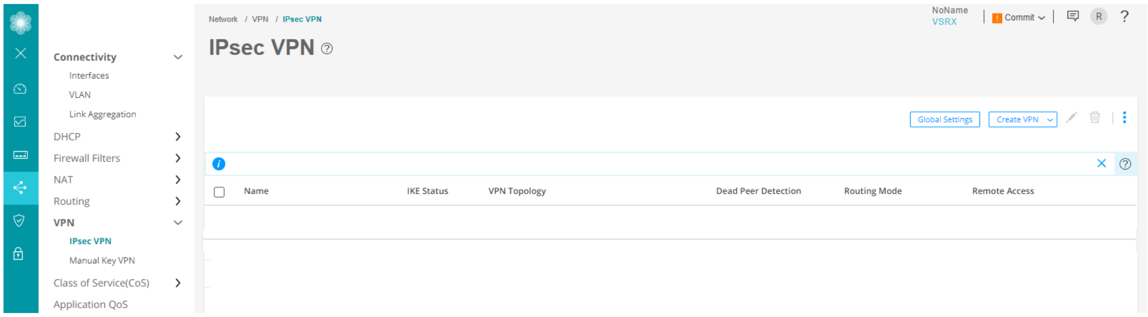
Security Logging

Configure stream logs to record the data plane events.

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

   a. After you click **IPsec VPN**, the IPsec VPN page appears. Figure 48 on page 191 shows an example of the **IPsec VPN** page.

Figure 48: IPsec VPN Page



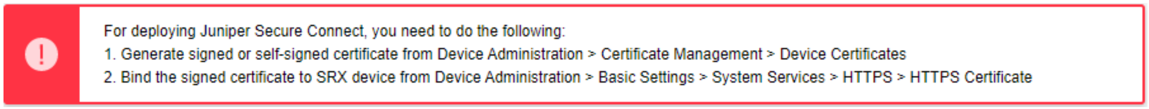
IPsec VPN

☐	Name	IKE Status	VPN Topology	Dead Peer Detection	Routing Mode	Remote Access

   b. 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.

   The following warning message appears:

Figure 49: Warning Message To Generate And Bind Self-signed Certificate



For deploying Juniper Secure Connect, you need to do the following:
1. Generate signed or self-signed certificate from Device Administration > Certificate Management > Device Certificates
2. Bind the signed certificate to SRX device from Device Administration > Basic Settings > System Services > HTTPS > HTTPS Certificate

As mentioned in the warning message, create a self-signed certificate and bind the certificate to the SRX Series Firewall. For more information, see "Deploy Certificates for Juniper Secure Connect" on page 14.

For detailed information about creating a remote access VPN, see Create a Remote Access VPN—Juniper Secure Connect.

c. Again navigate to **Network** > **VPN** > **IPsec VPN** and 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. The Create Remote Access (Juniper Secure Connect) page appears. Figure 50 on page 192 shows an example to create remote access VPN.

Figure 50: Create VPN - Remote Access

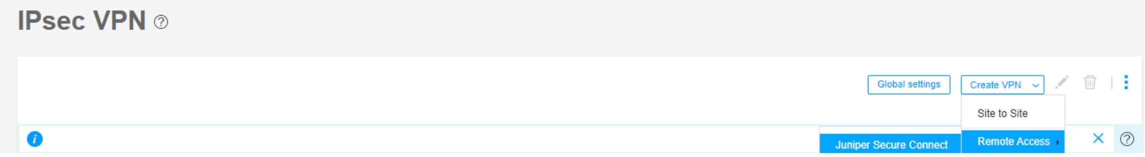
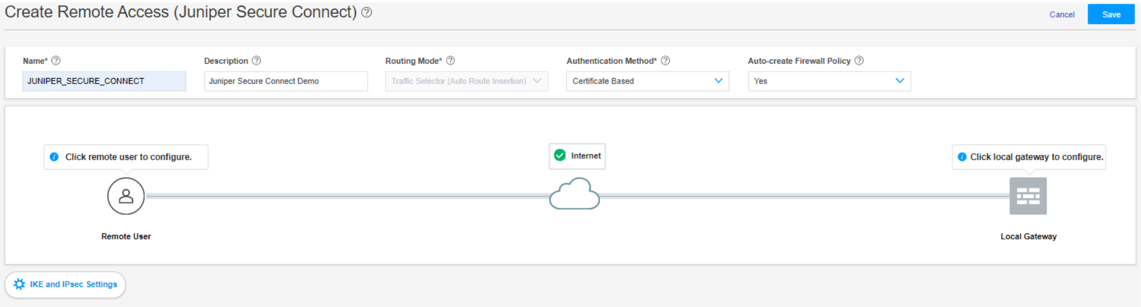


Figure 51 on page 192 shows an example of the create remote access page with **Certificate Based** authentication method.

Figure 51: Create Remote Access Page For Certificate-Based Authentication Method



Create Remote Access (Juniper Secure Connect)

Name*: JUNIPER_SECURE_CONNECT
Description: Juniper Secure Connect Demo
Routing Mode*: Traffic Selector (Auto Route Insertion)
Authentication Method*: Certificate Based
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

3. On the Create Remote Access (Juniper Secure Connect) page (see Figure 52 on page 193):

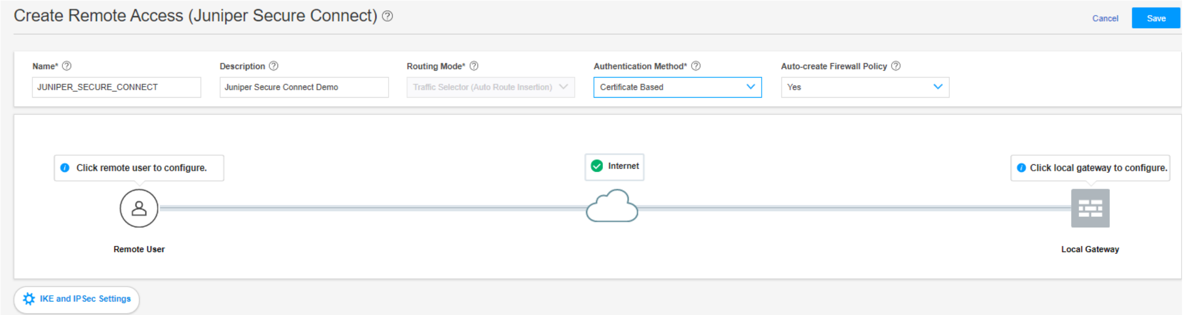
a. Enter the name for the Remote Access Connection (this is, the name that will be displayed on the End Users Realm Name in Juniper Secure Connect application) and a description.

b. The routing mode is set to **Traffic Selector (Auto Route Insertion)** by default.

c. Select the authentication method. For this example, let's select **Certificate Based** from the drop-down list.

d. Select **Yes** to create the firewall policy automatically using **Auto-create Firewall Policy** option.

Figure 52: Certificate-Based Authentication Method



Create Remote Access (Juniper Secure Connect)

Name*: JUNIPER_SECURE_CONNECT

Description: Juniper Secure Connect Demo

Routing Mode*: Traffic Selector (Auto Route Insertion)

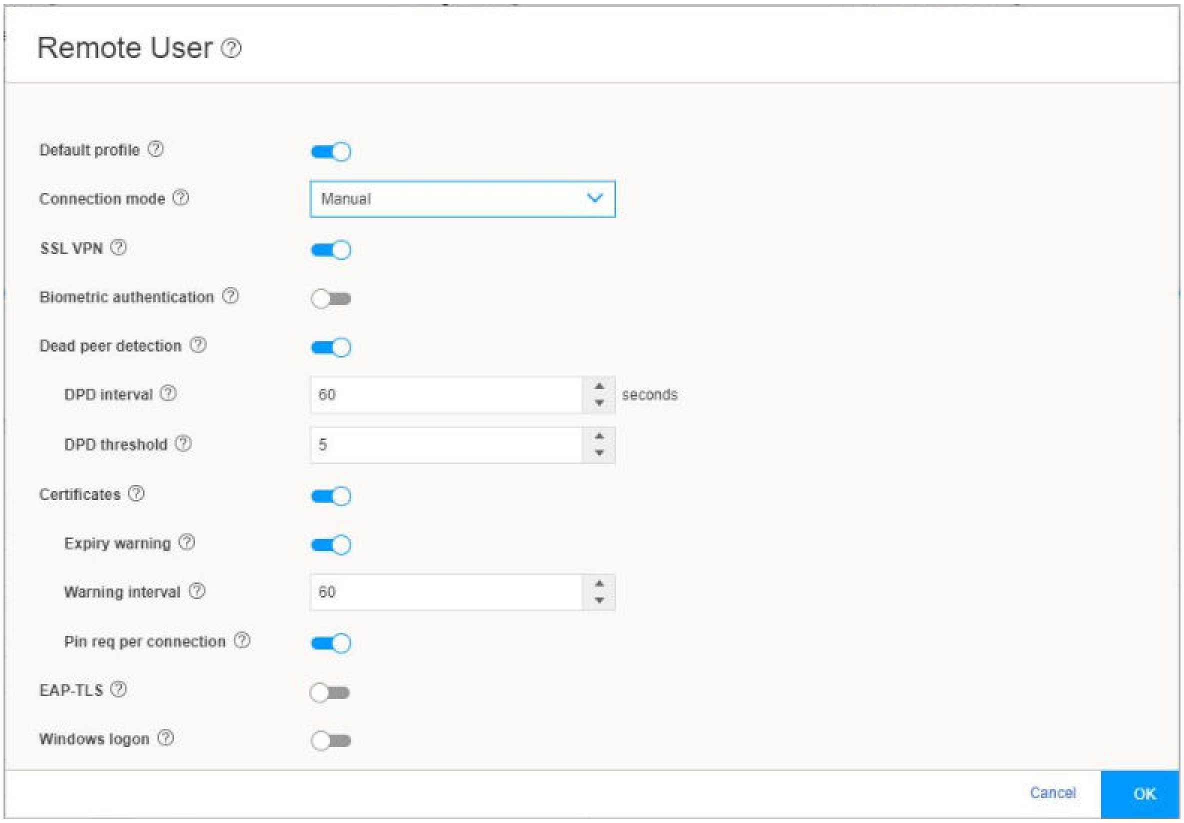
Authentication Method*: Certificate Based

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

4. Click **Remote User** icon to configure the Juniper Secure Connect application settings.

Figure 53: Remote User Page



Remote User ⓘ

Default profile ⓘ	●
Connection mode ⓘ	Manual
SSL VPN ⓘ	●
Biometric authentication ⓘ	○
Dead peer detection ⓘ	●
DPD interval ⓘ	60 seconds
DPD threshold ⓘ	5
Certificates ⓘ	●
Expiry warning ⓘ	●
Warning interval ⓘ	60
Pin req per connection ⓘ	●
EAP-TLS ⓘ	○
Windows logon ⓘ	○

Figure 53 on page 194 shows an example of the Remote User page.

Configure the remote user client by selecting the options on the **Remote User** page and then clicking **OK** :

Table 22 on page 195 summarizes the remote user settings options.

Table 22: Remote User Client Settings Options

Remote User Client Settings	Description
Default Profile	The **Default Profile** is enabled by default. If you do not want this profile to be the default profile, click the toggle button. If you enable **Default Profile** for the VPN connection profile, Juniper Secure Connect automatically selects default profile as realm name (in this example: **https://12.12.12.12/**). In this case, it is optional to enter the realm name in Juniper Secure Connect. If you disable **Default Profile** for the VPN connection profile, you must enter the realm name along with the gateway address (in this example: **https://12.12.12.12/JUNIPER_SECURE_CONNECT**) in Juniper Secure Connect. **NOTE**: Starting in Junos OS 23.1R1 Release, default profile is deprecated in J-Web. However, in CLI—rather than immediately removing it—we provide backward compatibility and a chance to make your existing configuration conform to the changed configuration. You'll receive a warning message if you continue to use the default-profile option in your configuration. However existing deployments are not affected if you modify the current configuration using CLI. See default-profile (Juniper Secure
Connection Mode	To establish the client connection manually or automatically, select the appropriate option. • If you select **Manual**, then in the Juniper Secure Connect application, to establish a connection, you must either click the toggle button or select **Connection > Connect** from the menu. • If you select **Always**, then Juniper Secure Connect automatically establishes the connection. *Known Limitation:* **Android device**: If you use or select **Always**, then the configuration is downloaded from the first used SRX device. If the first SRX Series Firewall configuration changes or if you connect to a new SRX device, the configuration does not get downloaded to the Juniper Secure Connect application. This means that once you connect in the Always mode using the Android device, any configuration changes in the SRX Series Firewall do not take effect on Juniper Secure Connect.

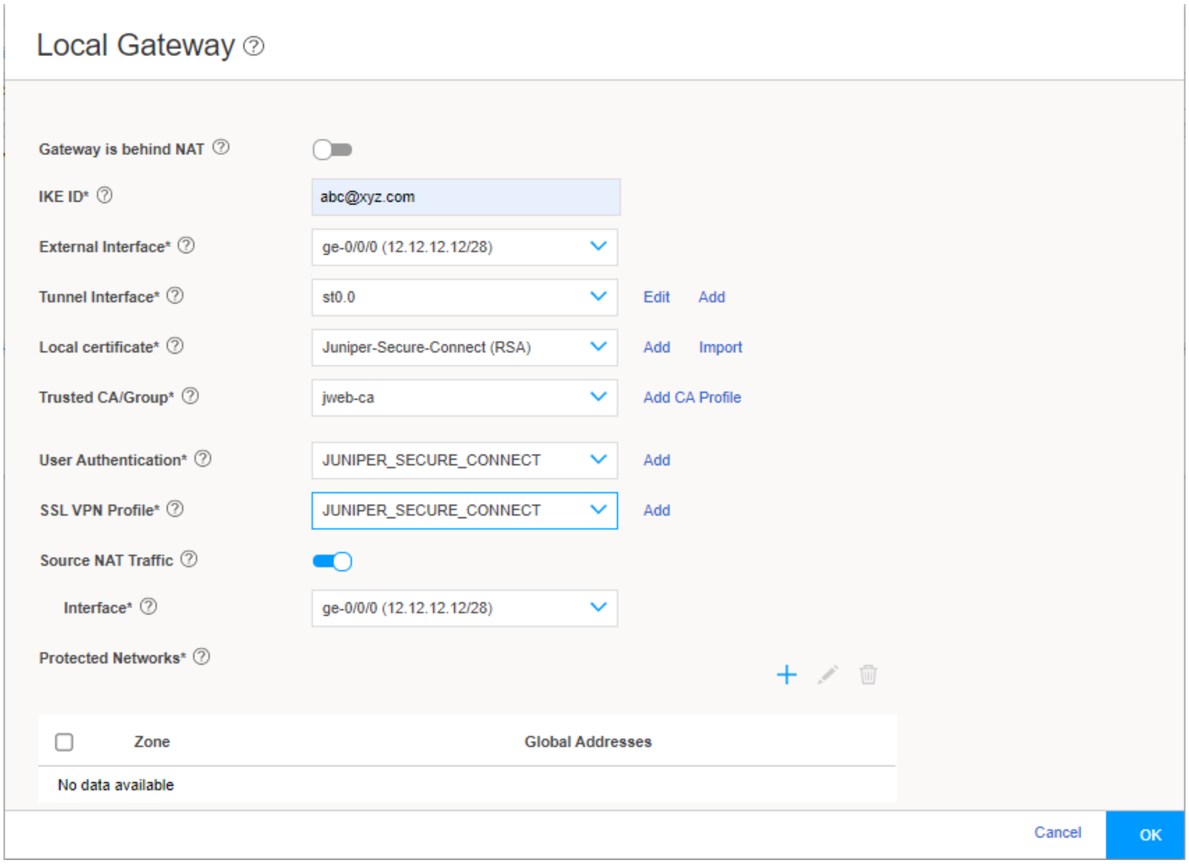
Table 22: Remote User Client Settings Options *(Continued)*

Remote User Client Settings	Description
SSL VPN	To enable support for SSL VPN connection from the Juniper Secure Connect application to the SRX Series Firewalls, click the toggle button. By enabling **SSL VPN**, the client has the flexibility in connecting the SRX Series Firewalls. By default, **SSL VPN** is enabled.
Biometric authentication	This option is disabled by default. If you enable this option, when you click connect in Juniper Secure Connect, Juniper Secure Connect displays an authentication prompt. This option allows the user to protect their credentials using the operating system's built-in biometric authentication support.
Dead Peer Detection	Dead Peer Detection (DPD) is enabled by default to allow the client to detect if the SRX Series Firewall is not reachable, disable the connection till reachability is restored.
Certificates	This option is enabled by default to configure certificate options. • **Expiry Warning**—This option is enabled by default. When enabled, you receive certificate expiration warning on the Secure Connect client, when the certificate is about to expire. • **Warning Interval**—Enter the Interval at which the warning is displayed in days • **Pin Req Per Connection**—This option is enabled by default. When enabled, you must enter the certificate pin for every connection.
EAP-TLS	**EAP-TLS** is enabled by default. As, in this example we are using EAP-MSCHAPv2, toggle the EAP-TLS switch to disabled state.
Windows Logon	This option allows users to logon to the local Windows system through an already established VPN tunnel (using Windows Pre-Logon), so that it is authenticated to the central Windows domain or Active Directory.

5. Click **Local Gateway** to configure the Local Gateway settings.

   Figure 54 on page 197 shows an example of the local gateway configuration settings.

Figure 54: Local Gateway Configuration



Local Gateway

Gateway is behind NAT: off

IKE ID*: abc@xyz.com

External Interface*: ge-0/0/0 (12.12.12.12/28)

Tunnel Interface*: st0.0

Local certificate*: Juniper-Secure-Connect (RSA)

Trusted CA/Group*: jweb-ca

User Authentication*: JUNIPER_SECURE_CONNECT

SSL VPN Profile*: JUNIPER_SECURE_CONNECT

Source NAT Traffic: on

Interface*: ge-0/0/0 (12.12.12.12/28)

Protected Networks*

☐	Zone	Global Addresses
No data available		

a. 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.

b. Enter a IKE ID in **user@hostname.com** format. For example, **abc@xyz.com**.

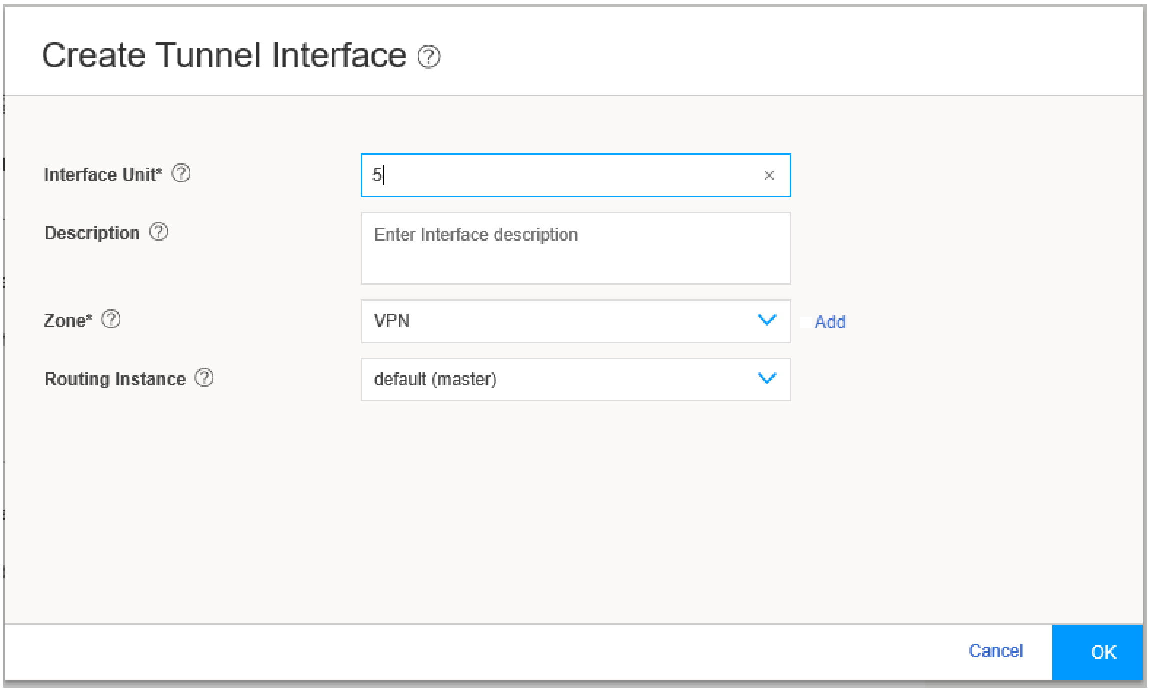
c. In the **External Interface** field, select the IP address for the clients to connect. You must enter this same IP address (in this example: **https://12.12.12.12/**) for the **Gateway Address** field in the Juniper Secure Connect application.

   If you enable **Gateway is behind NAT**, then the NAT IP address becomes the gateway address.

d. 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.

   Figure 55 on page 198 shows an example of the Create Tunnel Interface page.

Figure 55: Create Tunnel Interface Page



Create Tunnel Interface

Interface Unit* 5

Description Enter Interface description

Zone* VPN

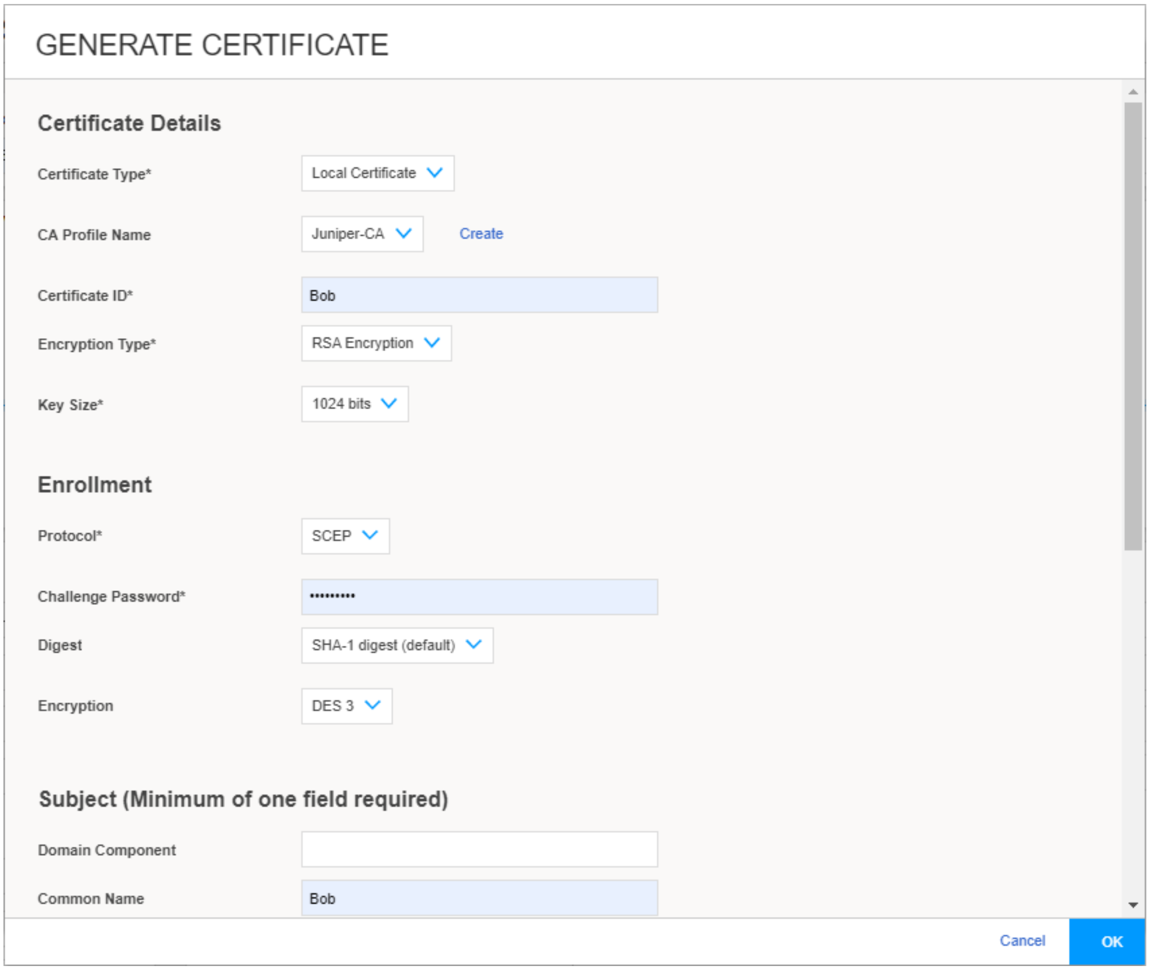
Routing Instance default (master)

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**.

e. From the **Local certificate** field, select one of your already externally signed local certificates. Click **Add** to add a new local certificate or click **Import** to import the local certificate.

Figure 56 on page 199 shows a configuration example only.

Figure 56: Generate Certificate Page For Local certificate



GENERATE CERTIFICATE

Certificate Details

Certificate Type* Local Certificate

CA Profile Name Juniper-CA Create

Certificate ID* Bob

Encryption Type* RSA Encryption

Key Size* 1024 bits

Enrollment

Protocol* SCEP

Challenge Password* •••••••••

Digest SHA-1 digest (default)

Encryption DES 3

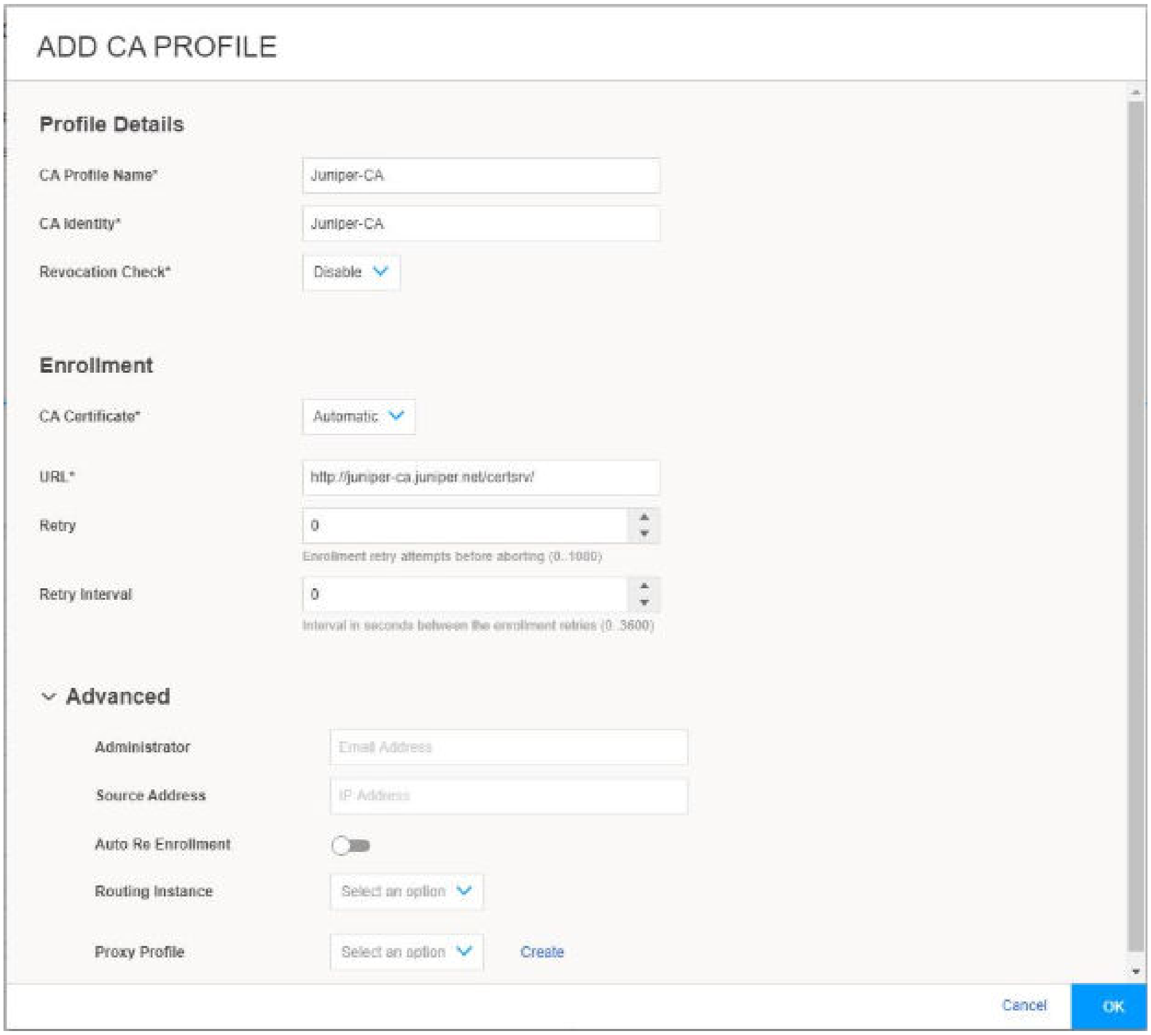
Subject (Minimum of one field required)

Domain Component

Common Name Bob

f. For CA certificate, from the **Trusted CA/Group** field, select one of your already externally signed CA certificates, including the matching Trusted CA/Group. If you do not have any of these, click **Add CA Profile** and fill in the values that match your environment. Figure 57 on page 200 shows an example of Add CA PROFILE page.

Figure 57: ADD CA PROFILE page



ADD CA PROFILE

Profile Details

CA Profile Name* Juniper-CA

CA Identity* Juniper-CA

Revocation Check* Disable

Enrollment

CA Certificate* Automatic

URL* http://juniper-ca.juniper.net/certsrv/

Retry 0

Enrollment retry attempts before aborting (0..1000)

Retry Interval 0

Interval in seconds between the enrollment retries (0..3600)

Advanced

Administrator Email Address

Source Address IP Address

Auto Re Enrollment

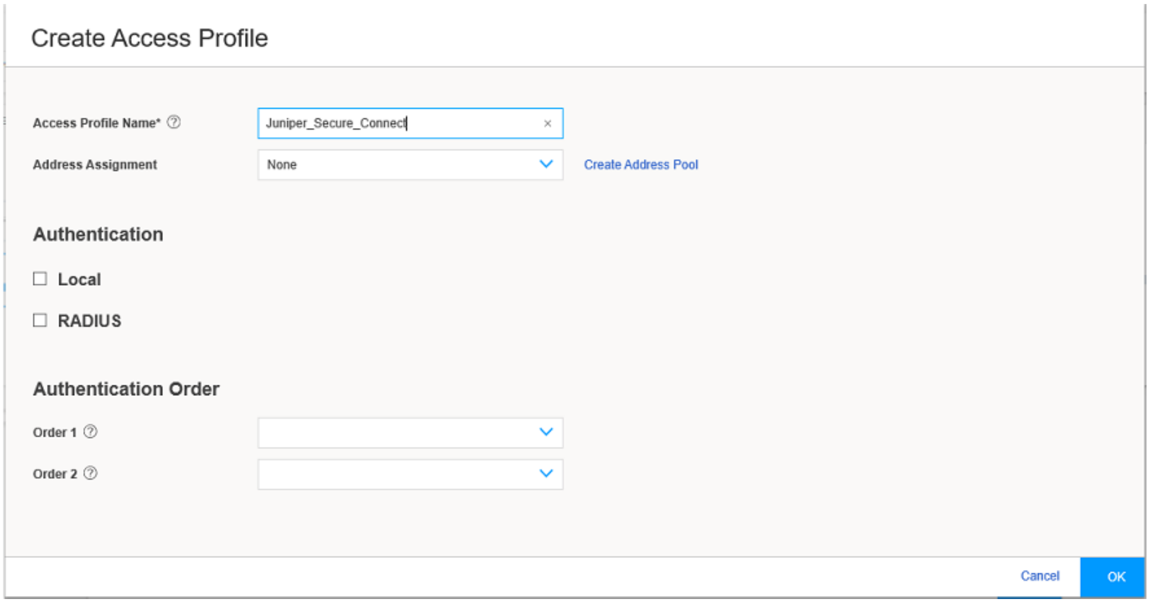
Routing Instance Select an option

Proxy Profile Select an option Create

g. 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.

Figure 58 on page 201 shows an example of the Create Access Profile page.

Figure 58: Create Access Profile Page



Create Access Profile

Access Profile Name*: Juniper_Secure_Connect

Address Assignment: None

Authentication

☐ Local

☐ RADIUS

Authentication Order

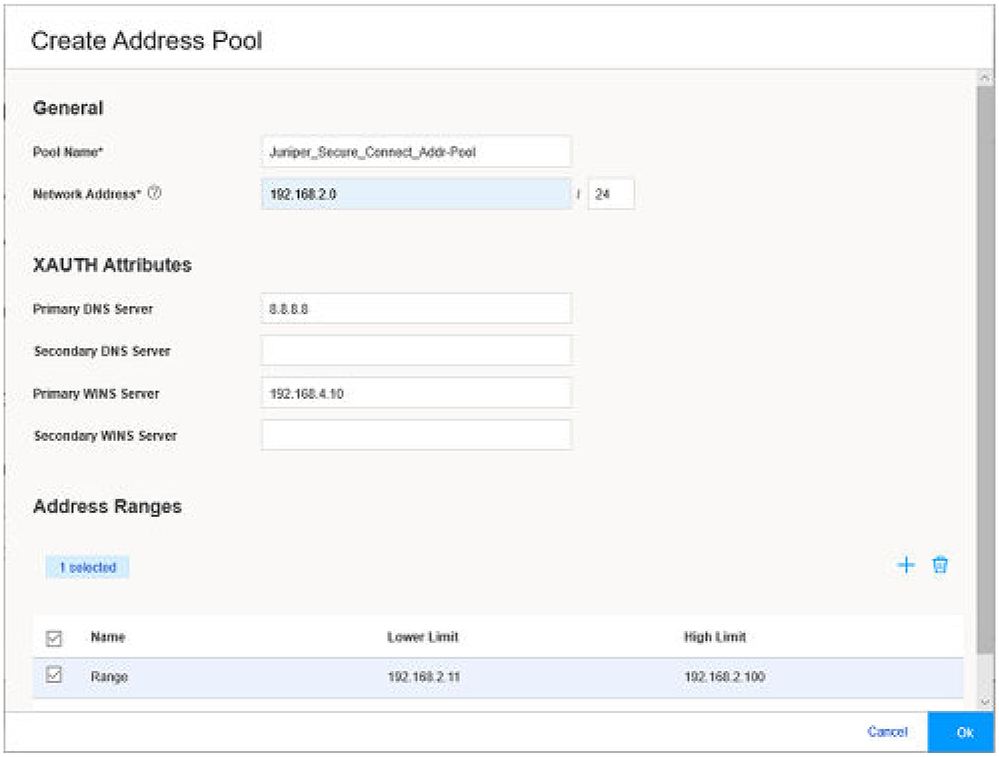
Order 1:

Order 2:

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.

Figure 59 on page 202 shows an example of the Create Address Pool page.

Figure 59: Create Address Pool Page



Create Address Pool

General

Pool Name*	Juniper_Secure_Connect_Addr-Pool
Network Address*	192.168.2.0 / 24

XAUTH Attributes

Primary DNS Server	8.8.8.8
Secondary DNS Server	
Primary WINS Server	192.168.4.10
Secondary WINS Server	

Address Ranges

1 selected

☑	Name	Lower Limit	High Limit
☑	Range	192.168.2.11	192.168.2.100

- 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.

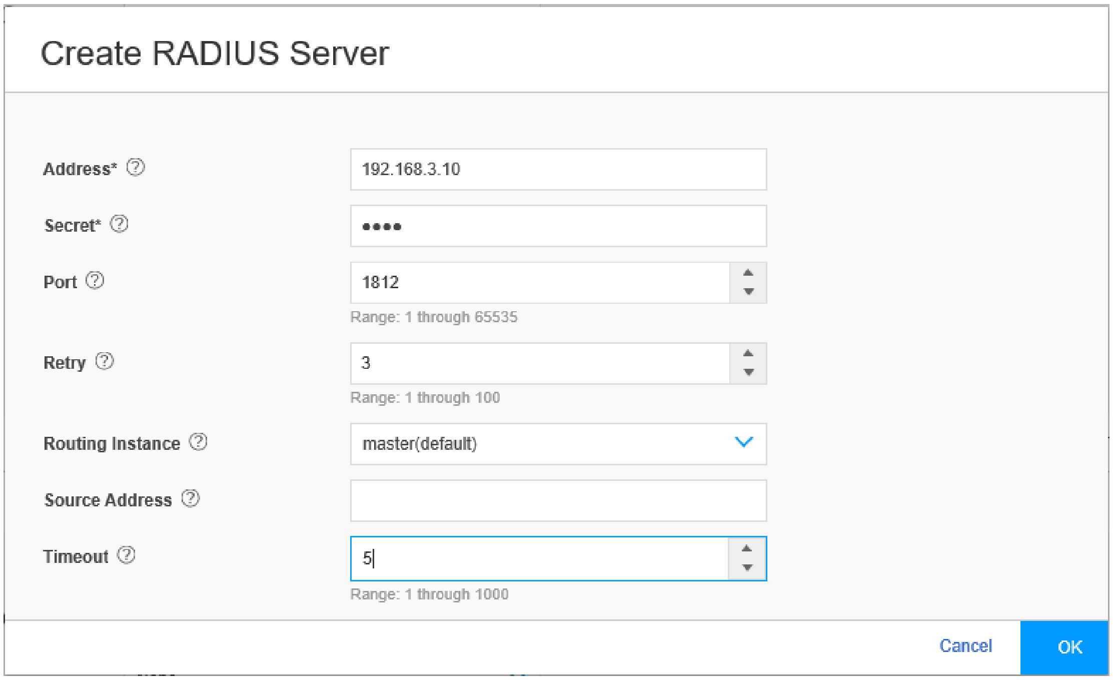
- Enter your DNS server address. Enter WINS server details, if required. Now click the add icon (+) to create the address range to assign IP addresses to the clients.

- Enter the name, and the lower and higher limits. After entering the details, click **OK**.

Select the **RADIUS** check box, where all the authentication details are stored on an external radius server.

- Click the add icon (+) to configure the Radius Server details. See Figure 60 on page 203.

Figure 60: Create RADIUS Server Page



Create RADIUS Server

Address* 192.168.3.10

Secret* ●●●●

Port 1812
Range: 1 through 65535

Retry 3
Range: 1 through 100

Routing Instance master(default)

Source Address

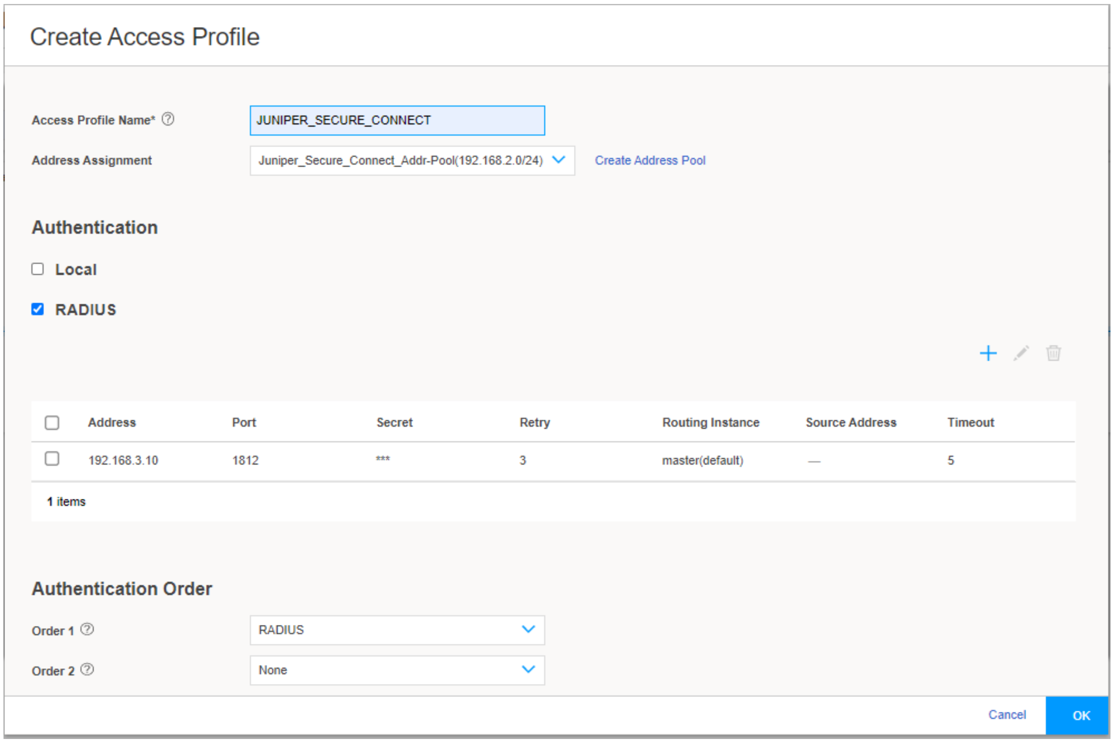
Timeout 5
Range: 1 through 1000

- Enter the Radius Server IP Address, the Radius Secret, and Source Address for the radius communications to be sourced from. Click **OK**.

  In the **Authentication Order**, from **Order 1** drop-down list select **RADIUS**. Click **OK** to complete the access profile configuration.

  Figure 61 on page 204 shows an example of Create Access Profile page.

Figure 61: Create Access Profile Page



Create Access Profile

Access Profile Name* ⓘ JUNIPER_SECURE_CONNECT

Address Assignment Juniper_Secure_Connect_Addr-Pool(192.168.2.0/24)

Authentication

□ Local

☑ RADIUS

□	Address	Port	Secret	Retry	Routing Instance	Source Address	Timeout
□	192.168.3.10	1812	***	3	master(default)	—	5

1 items

Authentication Order

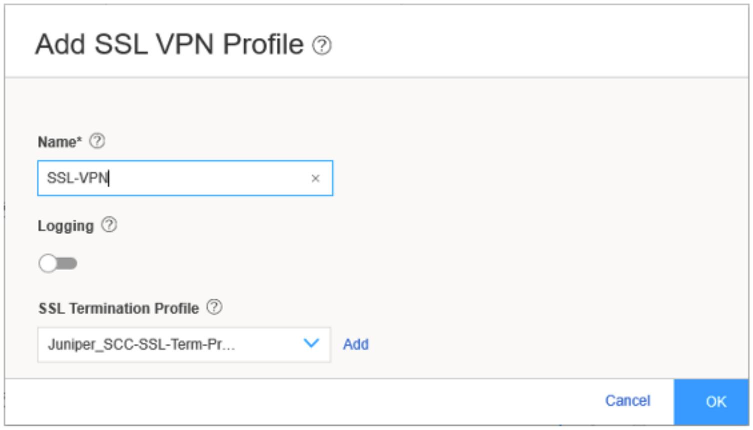
Order 1 ⓘ RADIUS

Order 2 ⓘ None

h. 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.

Figure 62 on page 204 shows an example of the Add SSL VPN Profile page.

Figure 62: Add SSL VPN Profile Page



Add SSL VPN Profile ⓘ

Name* ⓘ SSL-VPN

Logging ⓘ

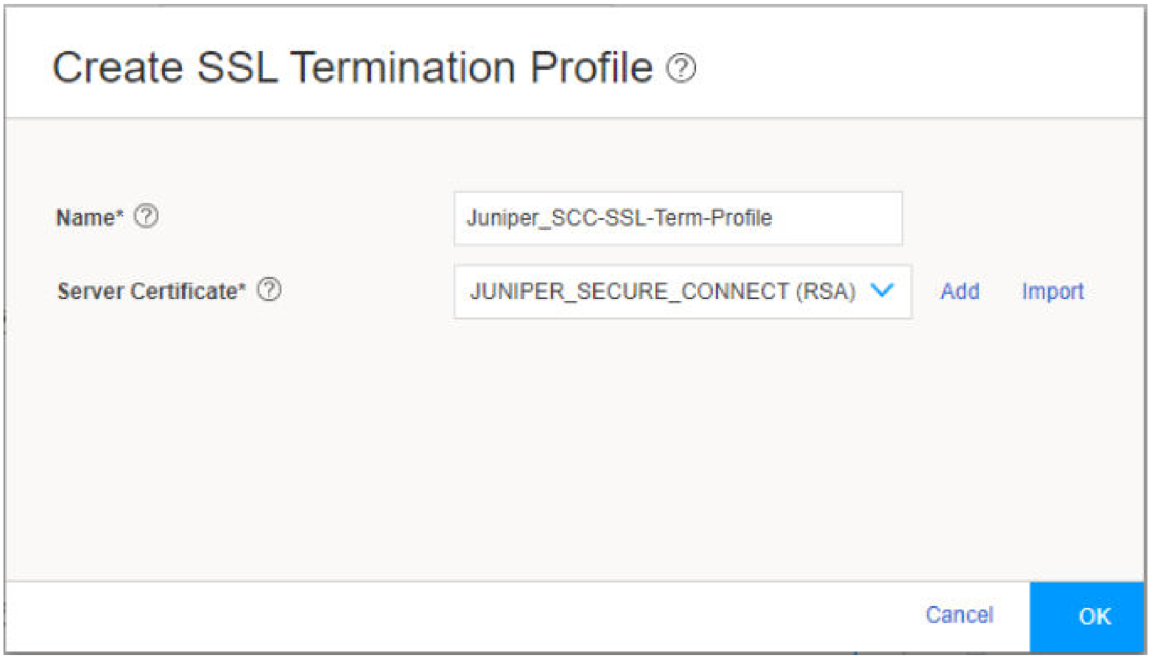
SSL Termination Profile ⓘ Juniper_SCC-SSL-Term-Pr...

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.

Figure 63 on page 205 shows an example of the Create SSL Termination Profile page.

Figure 63: Create SSL Termination Profile Page



Create SSL Termination Profile

Name*: Juniper_SCC-SSL-Term-Profile

Server Certificate*: JUNIPER_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.

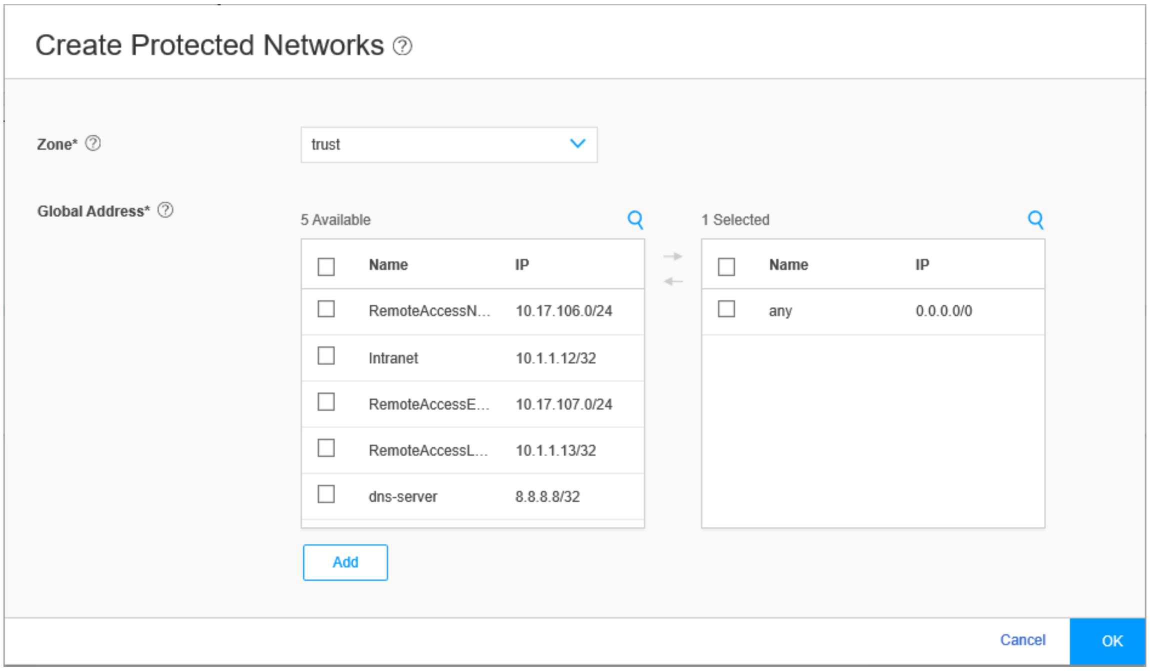
- Click **OK**.

i. 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.

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

Figure 64 on page 206 shows an example of the Create Protected Networks page.

Figure 64: Create Protected Networks Page



Create Protected Networks ⓘ

Zone* ⓘ: trust

Global Address* ⓘ

5 Available

□	Name	IP
□	RemoteAccessN...	10.17.106.0/24
□	Intranet	10.1.1.12/32
□	RemoteAccessE...	10.17.107.0/24
□	RemoteAccessL...	10.1.1.13/32
□	dns-server	8.8.8.8/32

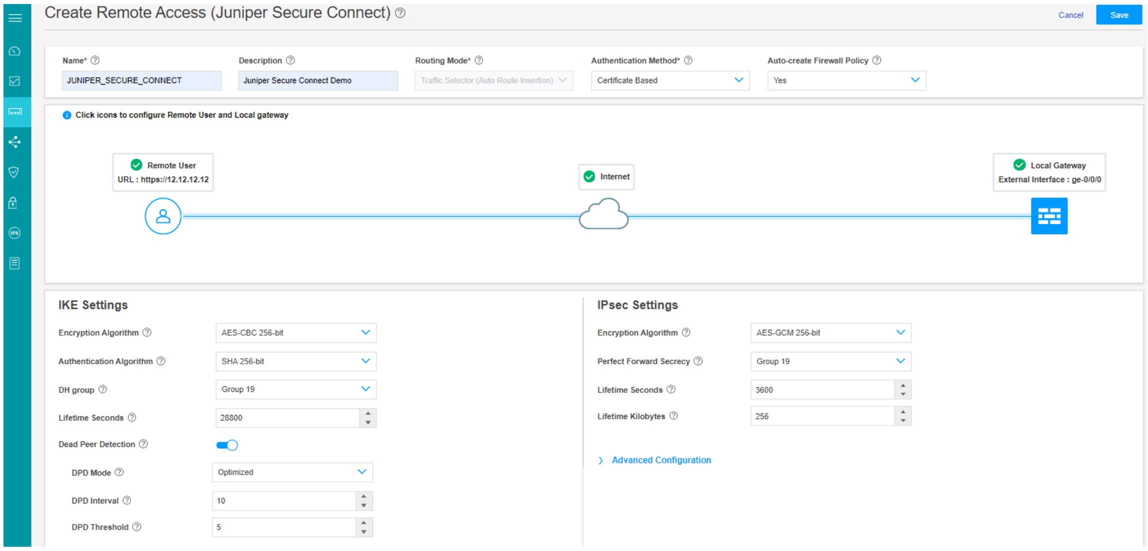
1 Selected

□	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.

Figure 65 on page 207 shows an example of successful completion of remote access configuration with remote user and local gateway.

Figure 65: Complete Remote Access Configuration



Create Remote Access (Juniper Secure Connect)

Name*: JUNIPER_SECURE_CONNECT

Description: Juniper Secure Connect Demo

Routing Mode*: Traffic Selector (Auto Route Insertion)

Authentication Method*: Certificate Based

Auto-create Firewall Policy: Yes

Click icons to configure Remote User and Local gateway

Remote User
URL : https://12.12.12.12

Internet

Local Gateway
External Interface : ge-0/0/0

IKE Settings

Encryption Algorithm: AES-CBC 256-bit

Authentication Algorithm: SHA 256-bit

DH group: Group 19

Lifetime Seconds: 28800

Dead Peer Detection

DPD Mode: Optimized

DPD Interval: 10

DPD Threshold: 5

IPsec Settings

Encryption Algorithm: AES-GCM 256-bit

Perfect Forward Secrecy: Group 19

Lifetime Seconds: 3600

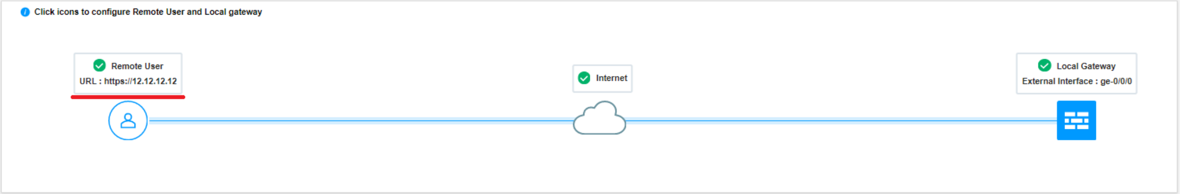
Lifetime Kilobytes: 256

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.

6. You can now find the URL for the remote users to connect to. Copy and store this URL for sharing with your remote users. You need only the /xxxx information if this configuration is not your default profile.

   Figure 66 on page 207 highlights the URL that remote user must enter in the **Gateway address** field in Juniper Secure Connect application to establish remote access connection.

Figure 66: Commit Remote Access Configuration



Click icons to configure Remote User and Local gateway

Remote User
URL : https://12.12.12.12

Internet

Local Gateway
External Interface : ge-0/0/0

   a. Click **Save** to complete the Juniper Secure Connect VPN configuration and associated policy if you have selected the auto policy creation option.

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

Download and install Juniper Secure Connect application on the client machine. Launch Juniper Secure Connect and connect to the gateway address of the SRX Series Firewall. You must also place the root CA certificate at the appropriate directory location for your respective platform where you've installed Juniper Secure Connect application.

RELATED DOCUMENTATION

Certificate-Based Validation Using EAP-TLS Authentication

SUMMARY

In this configuration, you use the EAP-TLS authentication method to validate the user certificates. You continue to use the username and password for external user authentication using the RADIUS server to download the initial configuration from the SRX Series Firewall.

IN THIS SECTION

We assume that you have completed the basic setup of your SRX Series Firewalls, including interfaces, zones, and security policies as illustrated in the "Juniper Secure Connect Deployment Setup" on page 5.

For information about prerequisites, see "System Requirements for Juniper Secure Connect" on page 11.

Ensure that you have a Public Key Infrastructure (PKI) configured as the backend authentication. In this case, you need to install the root certificate of the CA on each client as well as a user specific certificate on each client device. Note that local authentication is not supported in this scenario.

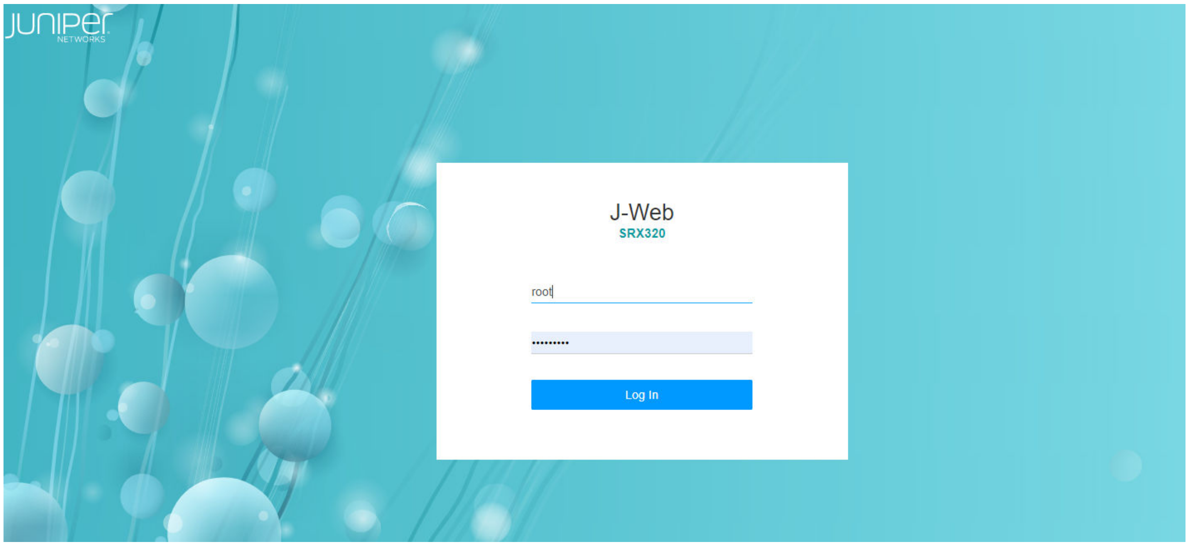
NOTE: You must ensure that the SRX Series Firewall uses either a signed certificate or a self-signed certificate instead of the default system-generated certificate. Before you start configuring Juniper Secure Connect, it is important that you read the instructions in "Get Started with Juniper Secure Connect" on page 10.

Configure Juniper Secure Connect VPN Settings

To configure VPN settings using the J-Web interface:

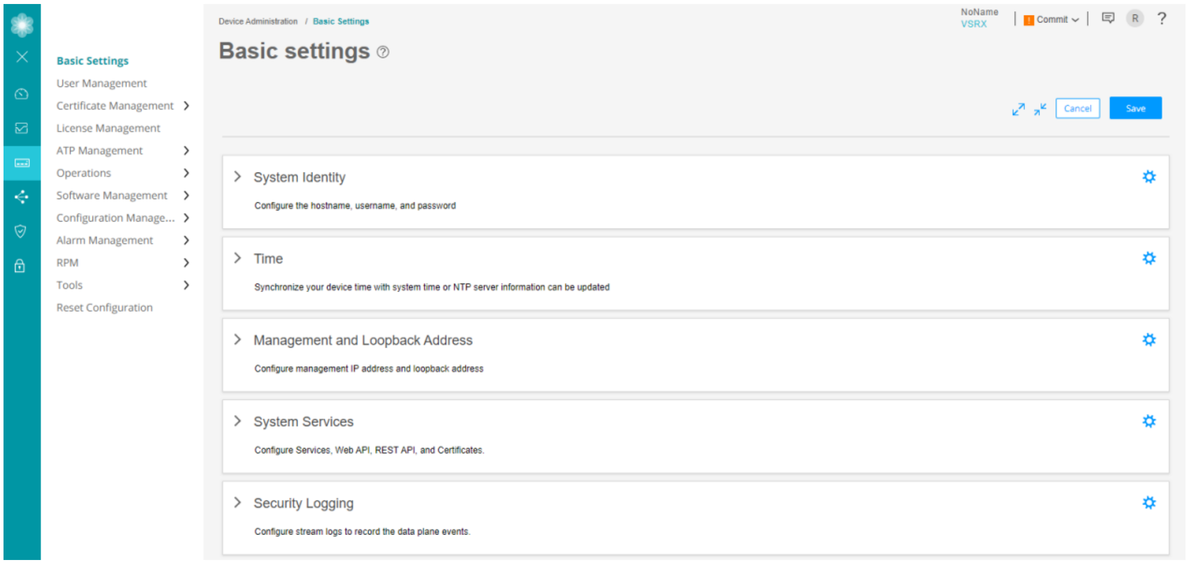
1. Log in to your SRX Series Firewall using J-Web interface. Figure 67 on page 209 shows J-Web login page.

   Figure 67: J-Web Access and Login

   After logging in successfully, you land on the Basic Settings page. Figure 68 on page 210 shows an example of the landing page.

Figure 68: J-Web Landing Page



Basic settings

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

Configure Services, Web API, REST API, and Certificates.

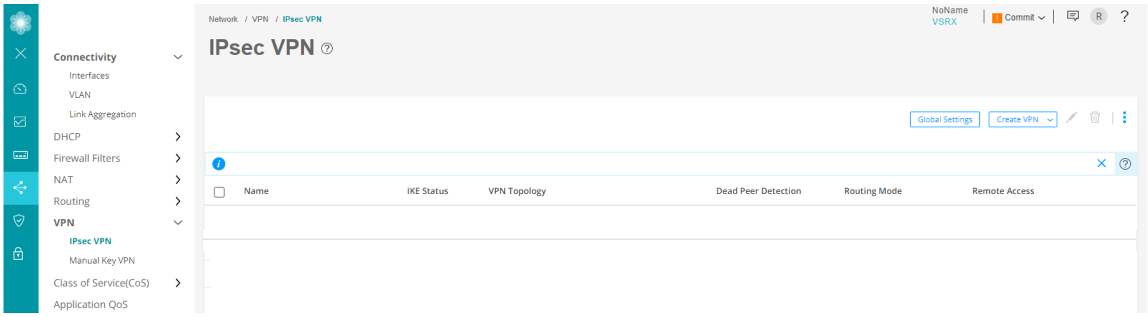
Security Logging

Configure stream logs to record the data plane events.

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

   a. After you click **IPsec VPN**, the IPsec VPN page appears. Figure 69 on page 210 shows an example of the IPsec VPN page.

Figure 69: IPsec VPN Page



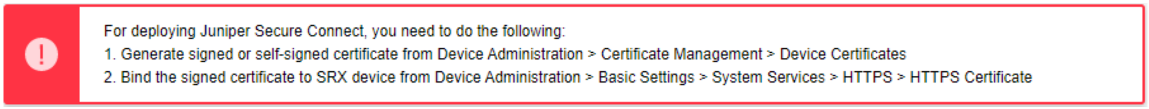
IPsec VPN

□	Name	IKE Status	VPN Topology	Dead Peer Detection	Routing Mode	Remote Access

   b. 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.

   The following warning message appears:

Figure 70: Warning Message To Generate And Bind Self-signed Certificate



For deploying Juniper Secure Connect, you need to do the following:
1. Generate signed or self-signed certificate from Device Administration > Certificate Management > Device Certificates
2. Bind the signed certificate to SRX device from Device Administration > Basic Settings > System Services > HTTPS > HTTPS Certificate

As mentioned in the warning message, create a self-signed certificate and bind the certificate to the SRX Series Firewall. For more information, see "Deploy Certificates for Juniper Secure Connect" on page 14.

For detailed information about creating a remote access VPN, see Create a Remote Access VPN—Juniper Secure Connect.

c. Again navigate to **Network** > **VPN** > **IPsec VPN** and 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. The Create Remote Access (Juniper Secure Connect) page appears. Figure 71 on page 211 shows an example to create remote access VPN.

Figure 71: Create VPN - Remote Access

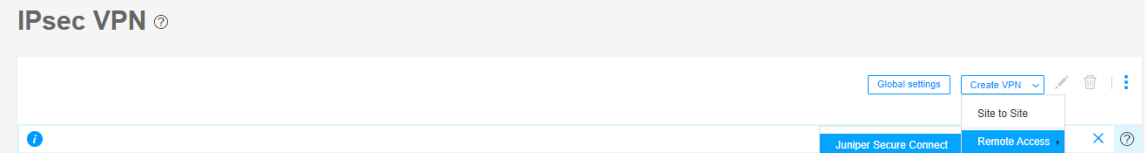
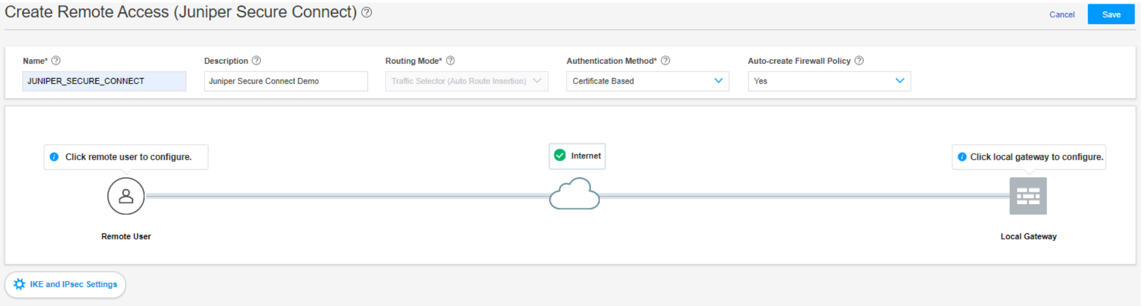


Figure 72 on page 211 shows an example of the Create Remote Access page with Certificate-based authentication method.

Figure 72: Create Remote Access Page For Certificate-Based Authentication Method



Create Remote Access (Juniper Secure Connect)

Name*: JUNIPER_SECURE_CONNECT
Description: Juniper Secure Connect Demo
Routing Mode*: Traffic Selector (Auto Route Insertion)
Authentication Method*: Certificate Based
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

3. On the Create Remote Access (Juniper Secure Connect) page (see Figure 73 on page 212):

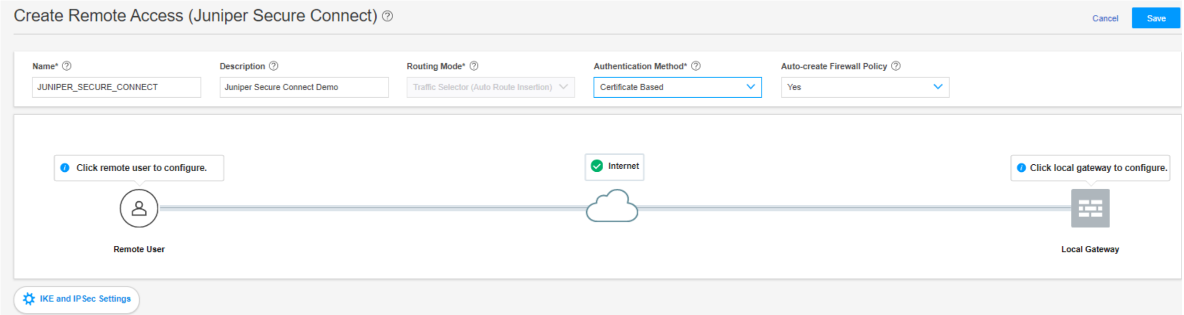
   a. Enter the name for the Remote Access Connection (this is, the name that will be displayed on the End Users Realm Name in Juniper Secure Connect application) and a description.

b. The routing mode is set to **Traffic Selector (Auto Route Insertion)** by default.

c. Select the authentication method. For this example, let's select **Certificate Based** from the drop-down list.

d. Select **Yes** to create the firewall policy automatically using **Auto-create Firewall Policy** option.

Figure 73: Certificate-Based Authentication Method



Create Remote Access (Juniper Secure Connect)

Name*: JUNIPER_SECURE_CONNECT

Description: Juniper Secure Connect Demo

Routing Mode*: Traffic Selector (Auto Route Insertion)

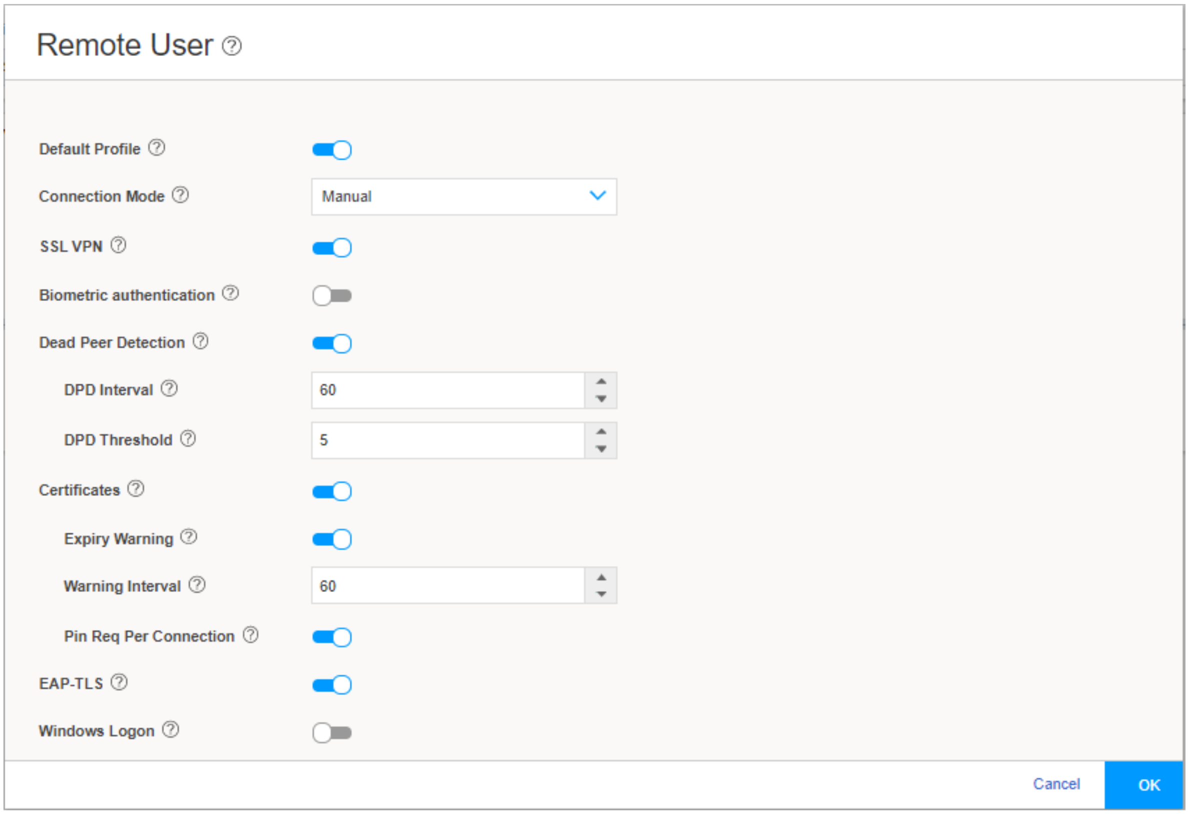
Authentication Method*: Certificate Based

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

4. Click **Remote User** icon to configure the Juniper Secure Connect application settings.

Figure 74: Remote User Page



Remote User

Default Profile	●
Connection Mode	Manual
SSL VPN	●
Biometric authentication	○
Dead Peer Detection	●
DPD Interval	60
DPD Threshold	5
Certificates	●
Expiry Warning	●
Warning Interval	60
Pin Req Per Connection	●
EAP-TLS	●
Windows Logon	○

Figure 74 on page 213 shows an example of the Remote User page.

Configure the remote user client by selecting the options on the **Remote User** page and then clicking **OK** :

Table 23 on page 214 summarizes the remote user settings options.

Table 23: Remote User Client Settings Options

Remote User Client Settings	Description
Default Profile	The **Default Profile** is enabled by default. If you do not want this profile to be the default profile, click the toggle button. If you enable **Default Profile** for the VPN connection profile, Juniper Secure Connect automatically selects default profile as realm name (in this example: **https://12.12.12.12/**). In this case, it is optional to enter the realm name in Juniper Secure Connect. If you disable **Default Profile** for the VPN connection profile, you must enter the realm name along with the gateway address (in this example: **https://12.12.12.12/JUNIPER_SECURE_CONNECT**) in Juniper Secure Connect. **NOTE**: Starting in Junos OS 23.1R1 Release, default profile is deprecated in J-Web. However, in CLI—rather than immediately removing it—we provide backward compatibility and a chance to make your existing configuration conform to the changed configuration. You'll receive a warning message if you continue to use the default-profile option in your configuration. However existing deployments are not affected if you modify the current configuration using CLI. See default-profile (Juniper Secure
Connection Mode	To establish the client connection manually or automatically, select the appropriate option. • If you select **Manual**, then in the Juniper Secure Connect application, to establish a connection, you must either click the toggle button or select **Connection > Connect** from the menu. • If you select **Always**, then Juniper Secure Connect automatically establishes the connection. *Known Limitation:* **Android device**: If you use or select **Always**, then the configuration is downloaded from the first used SRX device. If the first SRX Series Firewall configuration changes or if you connect to a new SRX device, the configuration does not get downloaded to the Juniper Secure Connect application. This means that once you connect in the Always mode using the Android device, any configuration changes in the SRX Series Firewall do not take effect on Juniper Secure Connect.

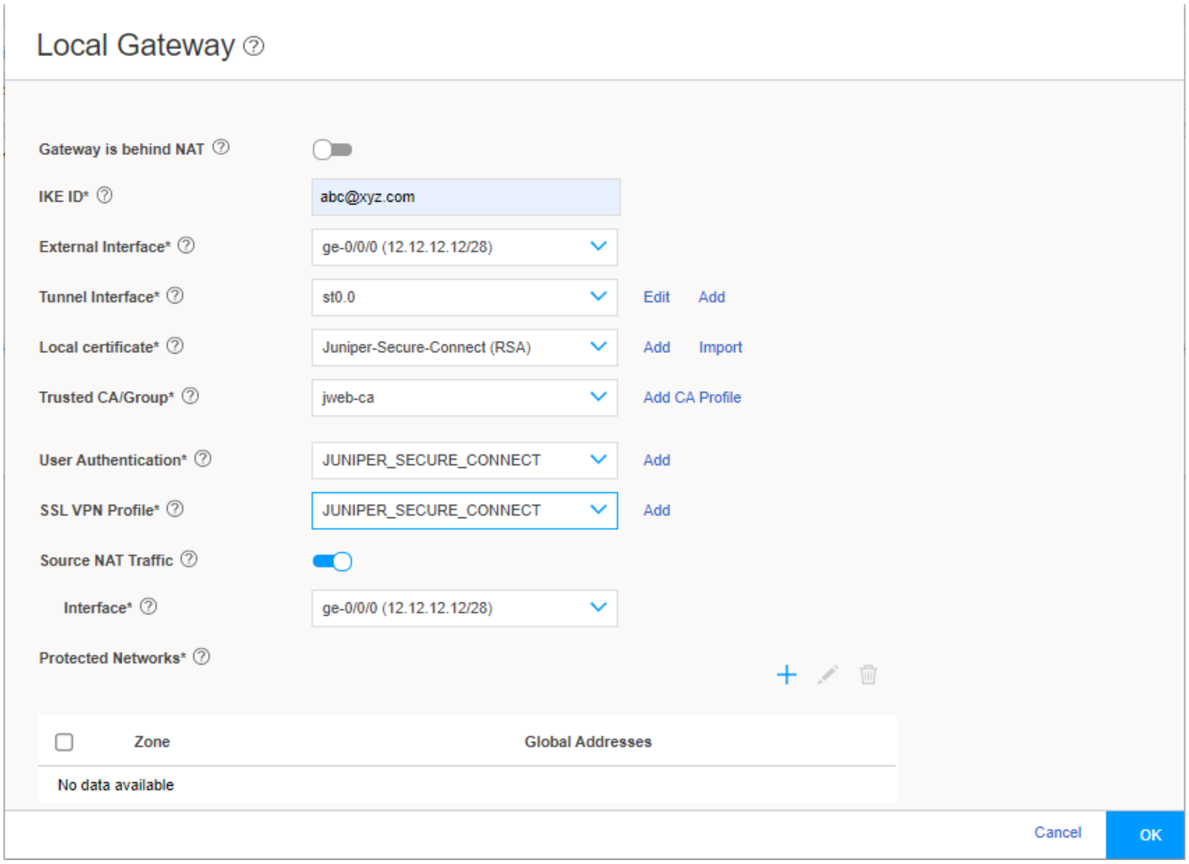
Table 23: Remote User Client Settings Options *(Continued)*

Remote User Client Settings	Description
SSL VPN	To enable support for SSL VPN connection from the Juniper Secure Connect application to the SRX Series Firewalls, click the toggle button. By enabling **SSL VPN**, the client has the flexibility in connecting the SRX Series Firewalls. By default, **SSL VPN** is enabled.
Biometric authentication	This option is disabled by default. If you enable this option, when you click connect in Juniper Secure Connect, Juniper Secure Connect displays an authentication prompt. This option allows the user to protect their credentials using the operating system's built-in biometric authentication support.
Dead Peer Detection	Dead Peer Detection (DPD) is enabled by default to allow the client to detect if the SRX Series Firewall is not reachable, disable the connection till reachability is restored.
Certificates	This option is enabled by default to configure certificate options. • **Expiry Warning**—This option is enabled by default. When enabled, you receive certificate expiration warning on the Secure Connect client, when the certificate is about to expire. • **Warning Interval**—Enter the Interval at which the warning is displayed in days • **Pin Req Per Connection**—This option is enabled by default. When enabled, you must enter the certificate pin for every connection.
EAP-TLS	**EAP-TLS** is enabled by default.
Windows Logon	This option allows users to logon to the local Windows system through an already established VPN tunnel (using Windows Pre-Logon), so that it is authenticated to the central Windows domain or Active Directory.

5. Click **Local Gateway** to configure the Local Gateway settings.

   Figure 75 on page 216 shows an example of the local gateway configuration settings.

Figure 75: Local Gateway Configuration



Local Gateway ⓘ

Gateway is behind NAT ⓘ	○	
IKE ID* ⓘ	abc@xyz.com	
External Interface* ⓘ	ge-0/0/0 (12.12.12.12/28)	
Tunnel Interface* ⓘ	st0.0	Edit Add
Local certificate* ⓘ	Juniper-Secure-Connect (RSA)	Add Import
Trusted CA/Group* ⓘ	jweb-ca	Add CA Profile
User Authentication* ⓘ	JUNIPER_SECURE_CONNECT	Add
SSL VPN Profile* ⓘ	JUNIPER_SECURE_CONNECT	Add
Source NAT Traffic ⓘ	●	
Interface* ⓘ	ge-0/0/0 (12.12.12.12/28)	
Protected Networks* ⓘ		

□	Zone	Global Addresses
No data available		

a. 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.

b. Enter a IKE ID in **user@hostname.com** format. For example, **abc@xyz.com**.

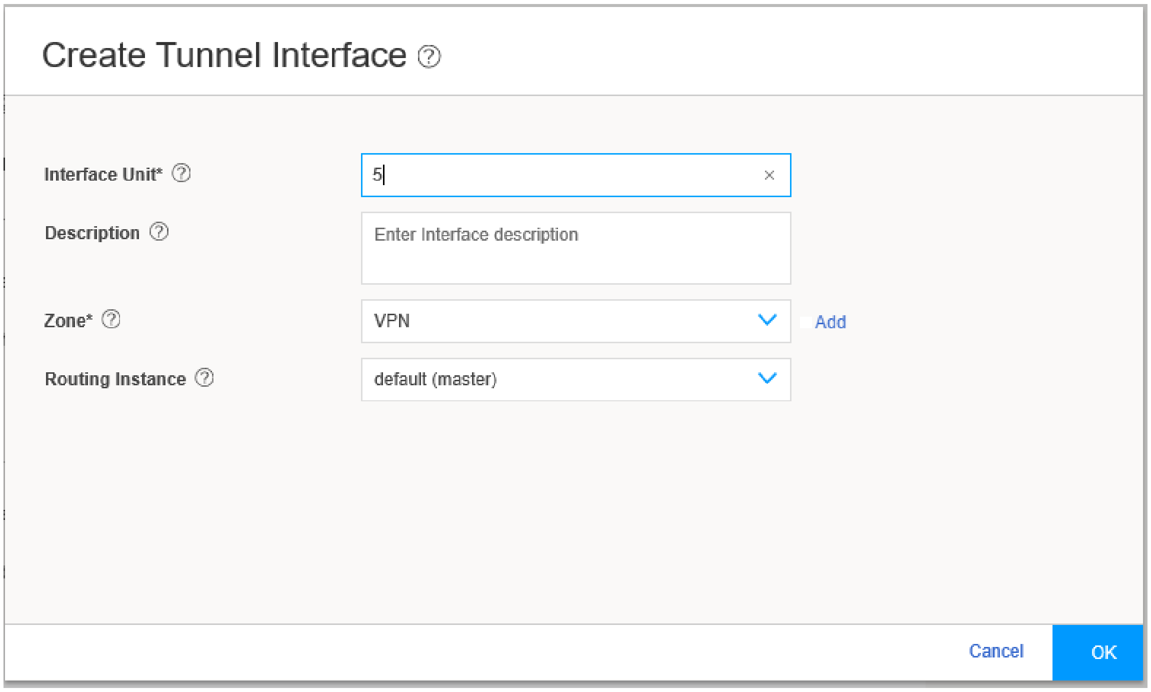
c. In the **External Interface** field, select the IP address for the clients to connect. You must enter this same IP address (in this example: **https://12.12.12.12/**) for the **Gateway Address** field in the Juniper Secure Connect application.

   If you enable **Gateway is behind NAT**, then the NAT IP address becomes the gateway address.

d. 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.

   Figure 76 on page 217 shows an example of the Create Tunnel Interface page.

Figure 76: Create Tunnel Interface Page



Create Tunnel Interface

Interface Unit* 5

Description: Enter Interface description

Zone* VPN

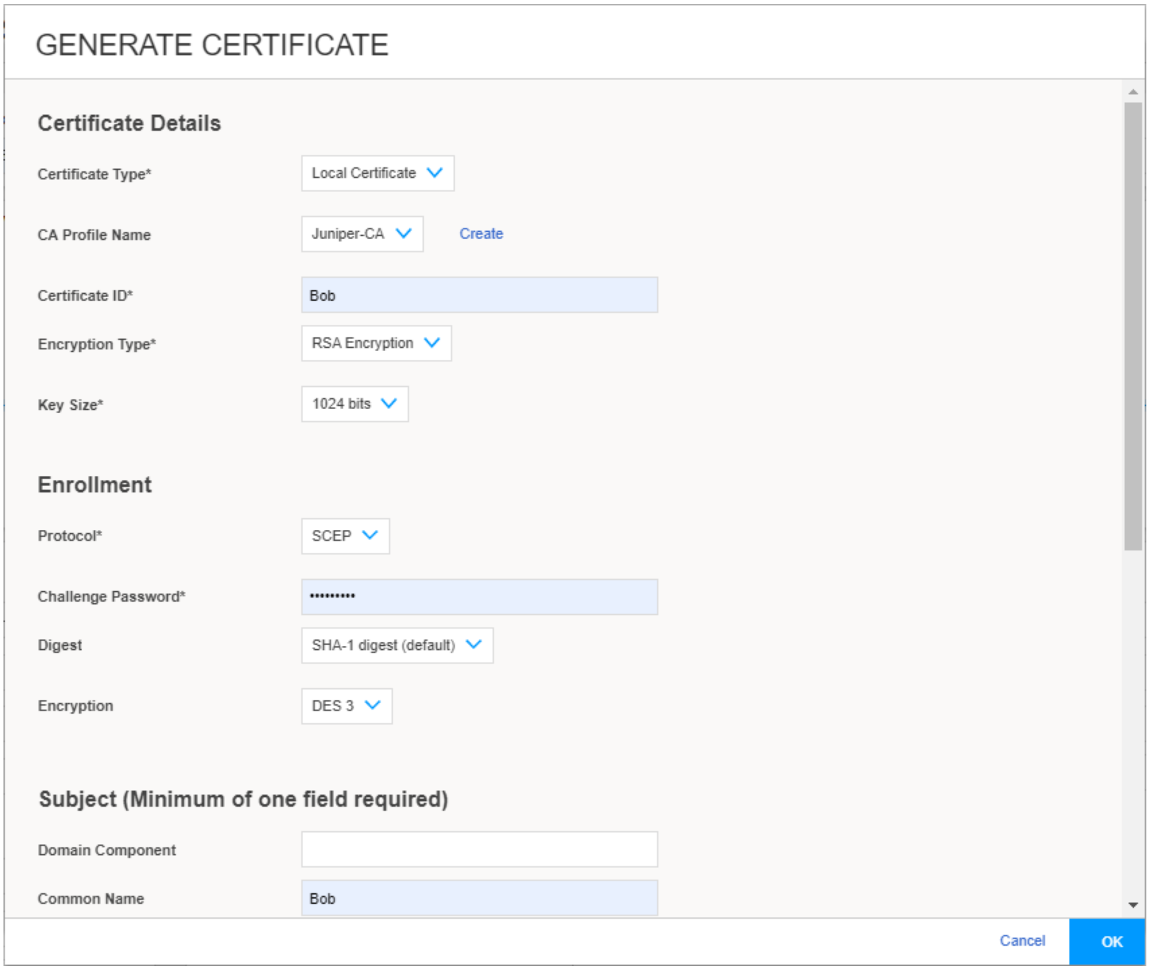
Routing Instance: default (master)

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**.

e. From the **Local certificate** field, select one of your already externally signed local certificates. Click **Add** to add a new local certificate or click **Import** to import the local certificate.

Figure 77 on page 218 shows a configuration example only.

Figure 77: Generate Certificate Page For Local certificate



GENERATE CERTIFICATE

Certificate Details

Certificate Type*	Local Certificate
CA Profile Name	Juniper-CA
Certificate ID*	Bob
Encryption Type*	RSA Encryption
Key Size*	1024 bits

Enrollment

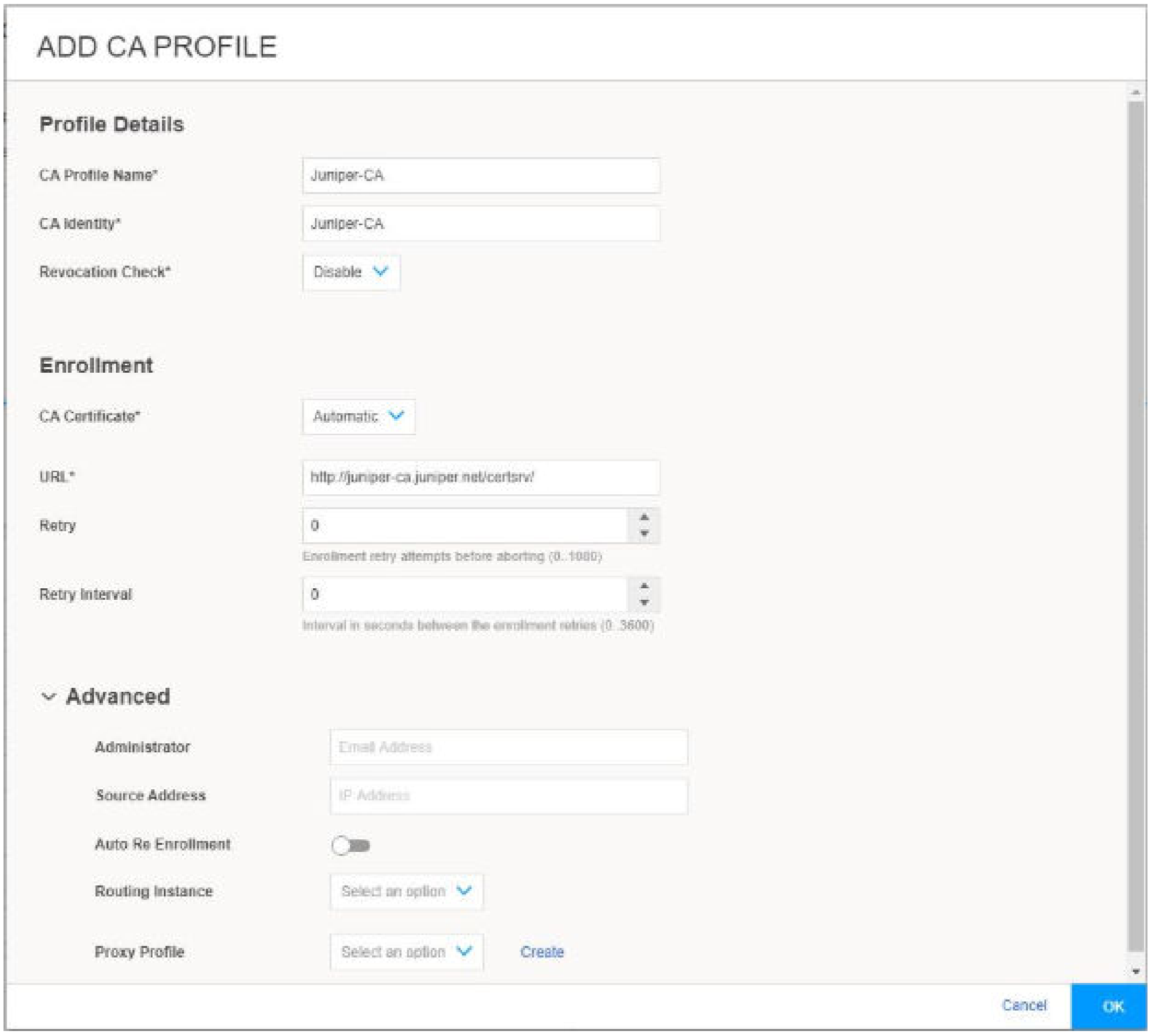
Protocol*	SCEP
Challenge Password*	•••••••••
Digest	SHA-1 digest (default)
Encryption	DES 3

Subject (Minimum of one field required)

Domain Component	
Common Name	Bob

f. For CA certificate, from the **Trusted CA/Group** field, select one of your already externally signed CA certificates, including the matching Trusted CA/Group. If you do not have any of these, click **Add CA Profile** and fill in the values that match your environment. Figure 78 on page 219 shows an example of Add CA PROFILE page.

Figure 78: ADD CA PROFILE page



ADD CA PROFILE

Profile Details

CA Profile Name*: Juniper-CA

CA Identity*: Juniper-CA

Revocation Check*: Disable

Enrollment

CA Certificate*: Automatic

URL*: http://juniper-ca.juniper.net/certsrv/

Retry: 0

Enrollment retry attempts before aborting (0..1000)

Retry Interval: 0

Interval in seconds between the enrollment retries (0..3600)

Advanced

Administrator: Email Address

Source Address: IP Address

Auto Re Enrollment

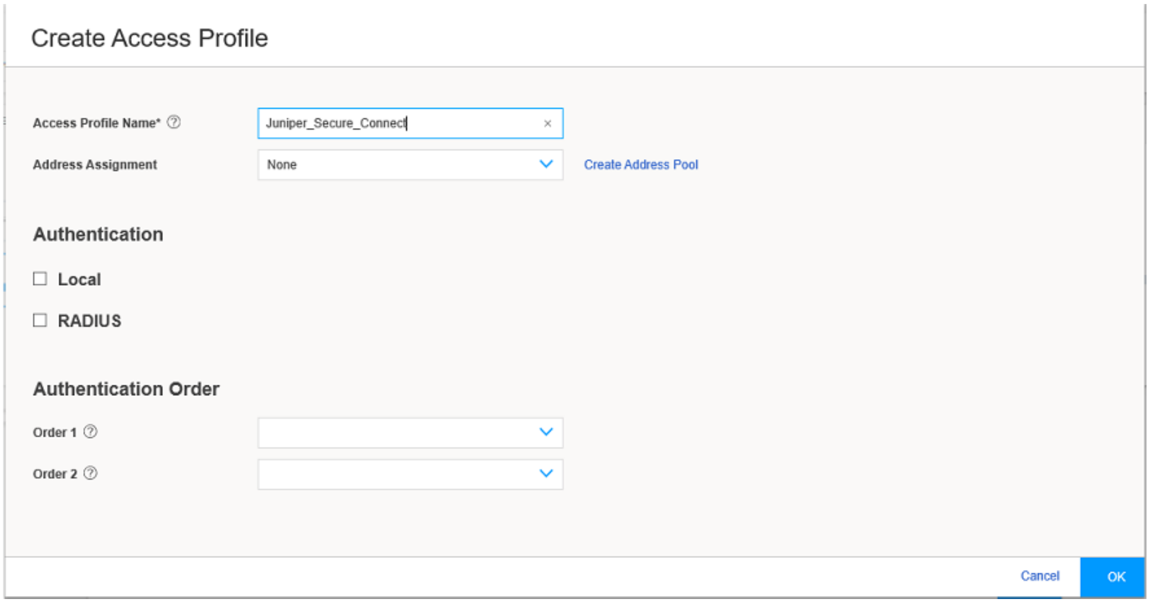
Routing Instance: Select an option

Proxy Profile: Select an option

g. In the **User Authentication** dropdown menu, you can select existing access profile or click **Add** to create a new Access Profile. If you click **Add**, the **Create Access Profile** window appears.

Figure 79 on page 220 shows an example of the Create Access Profile page.

Figure 79: Create Access Profile Page



Create Access Profile

Access Profile Name* Juniper_Secure_Connect

Address Assignment None

Create Address Pool

Authentication

□ Local

□ RADIUS

Authentication Order

Order 1

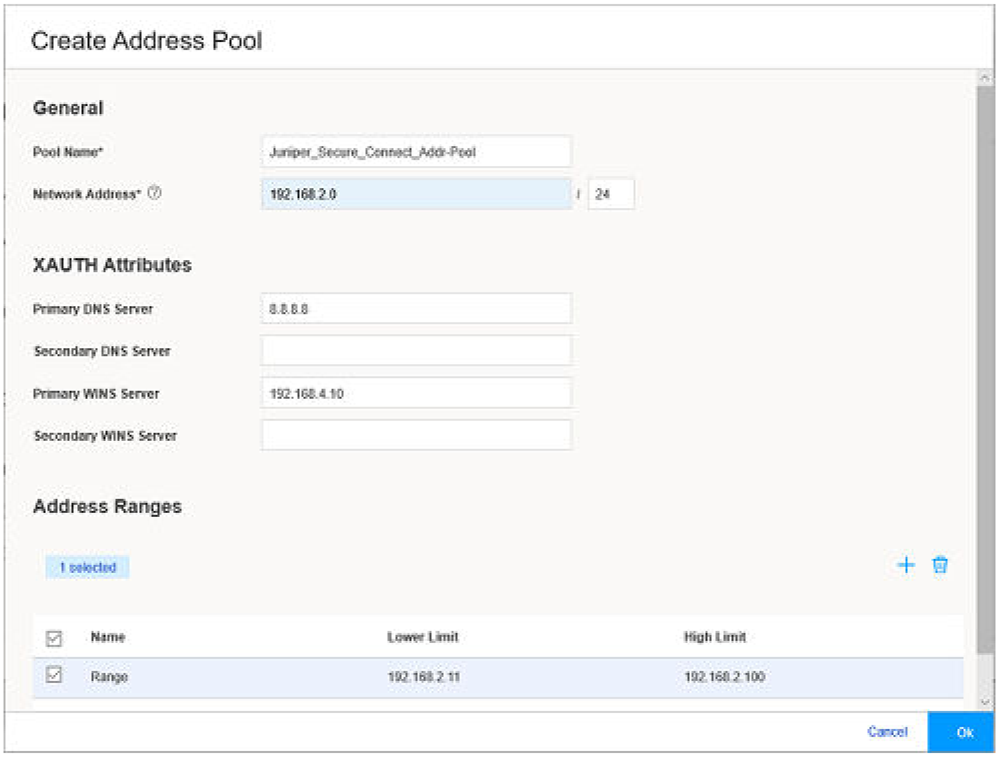
Order 2

Cancel OK

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.

Figure 80 on page 221 shows an example of the Create Address Pool page.

Figure 80: Create Address Pool Page



Create Address Pool

General

Pool Name*: Juniper_Secure_Connect_Addr-Pool

Network Address*: 192.168.2.0 / 24

XAUTH Attributes

Primary DNS Server: 8.8.8.8

Secondary DNS Server:

Primary WINS Server: 192.168.4.10

Secondary WINS Server:

Address Ranges

1 selected

☑	Name	Lower Limit	High Limit
☑	Range	192.168.2.11	192.168.2.100

- 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.

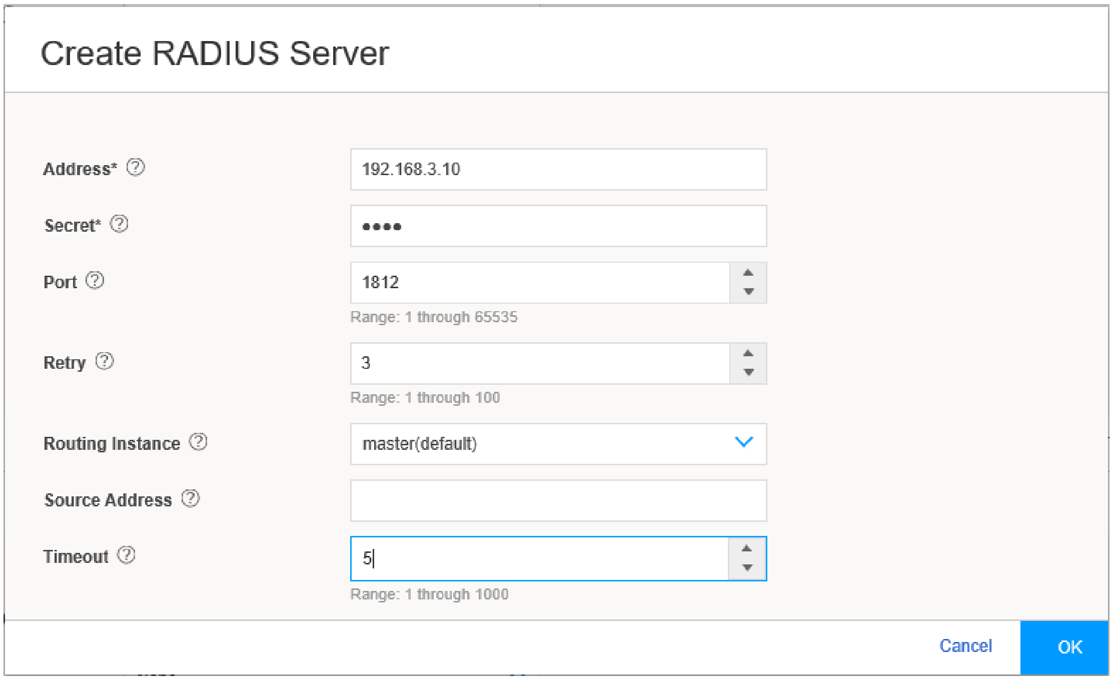
- Enter your DNS server address. Enter WINS server details, if required. Now click the add icon (+) to create the address range to assign IP addresses to the clients.

- Enter the name, and the lower and higher limits. After entering the details, click **OK**.

Select the **RADIUS** check box, where all the authentication details are stored on an external radius server.

- Click on the add icon (+) to configure the radius server details. See Figure 81 on page 222.

Figure 81: Create RADIUS Server Page



Create RADIUS Server

Address* 192.168.3.10

Secret* ••••

Port 1812

Range: 1 through 65535

Retry 3

Range: 1 through 100

Routing Instance master(default)

Source Address

Timeout 5

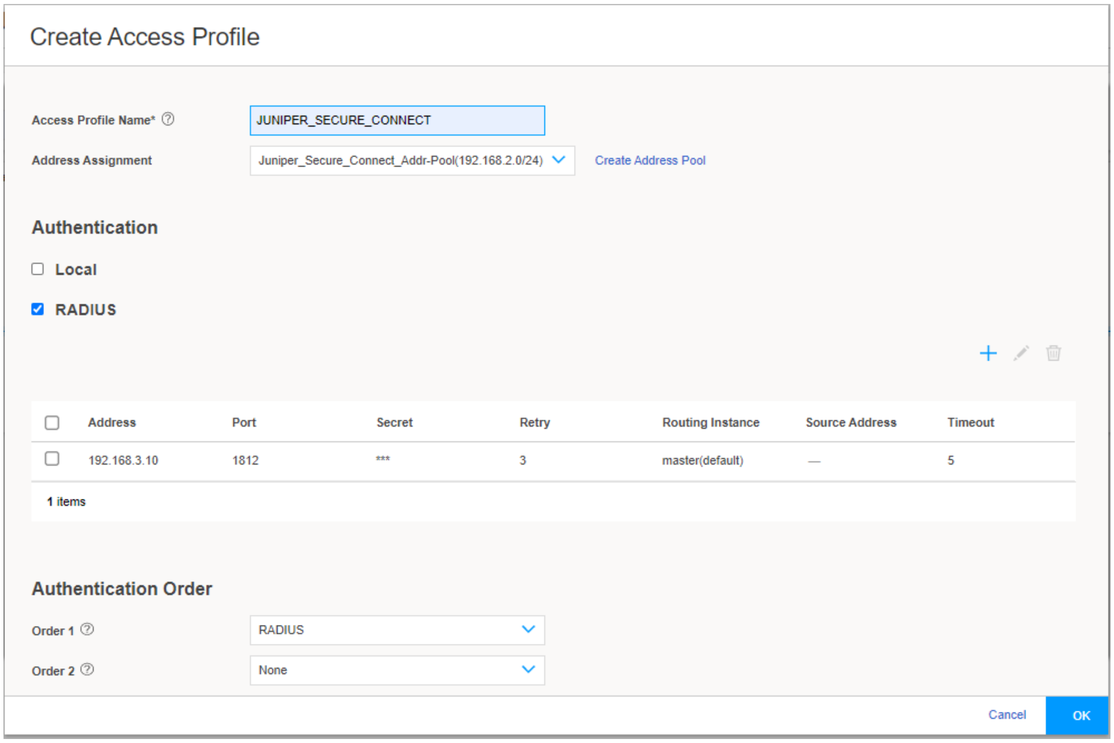
Range: 1 through 1000

- Enter the Radius Server IP Address, the Radius Secret, and Source Address for the radius communications to be sourced from. Click **OK**.

  In the **Authentication Order**, from **Order 1** drop-down list select **RADIUS**. Click **OK** to complete the access profile configuration.

  Figure 82 on page 223 shows an example of Create Access Profile page.

Figure 82: Create Access Profile Page



Create Access Profile

Access Profile Name* JUNIPER_SECURE_CONNECT

Address Assignment Juniper_Secure_Connect_Addr-Pool(192.168.2.0/24) Create Address Pool

Authentication

□ Local

☑ RADIUS

□	Address	Port	Secret	Retry	Routing Instance	Source Address	Timeout
□	192.168.3.10	1812	***	3	master(default)	—	5

1 items

Authentication Order

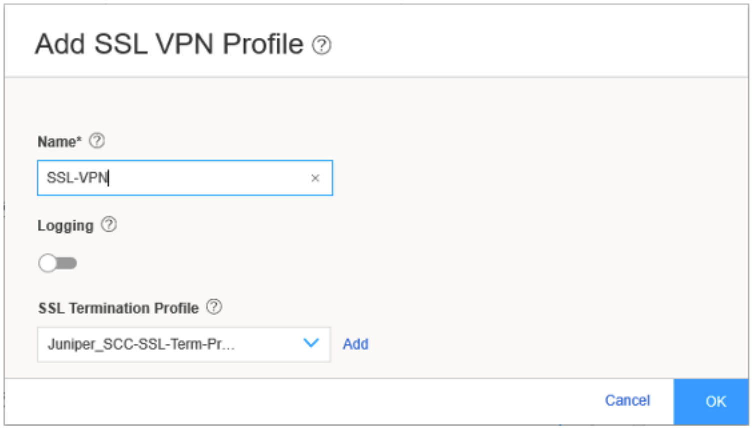
Order 1 RADIUS

Order 2 None

h. 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.

Figure 83 on page 223 shows an example of the Add SSL VPN Profile page.

Figure 83: Add SSL VPN Profile Page



Add SSL VPN Profile

Name* SSL-VPN

Logging

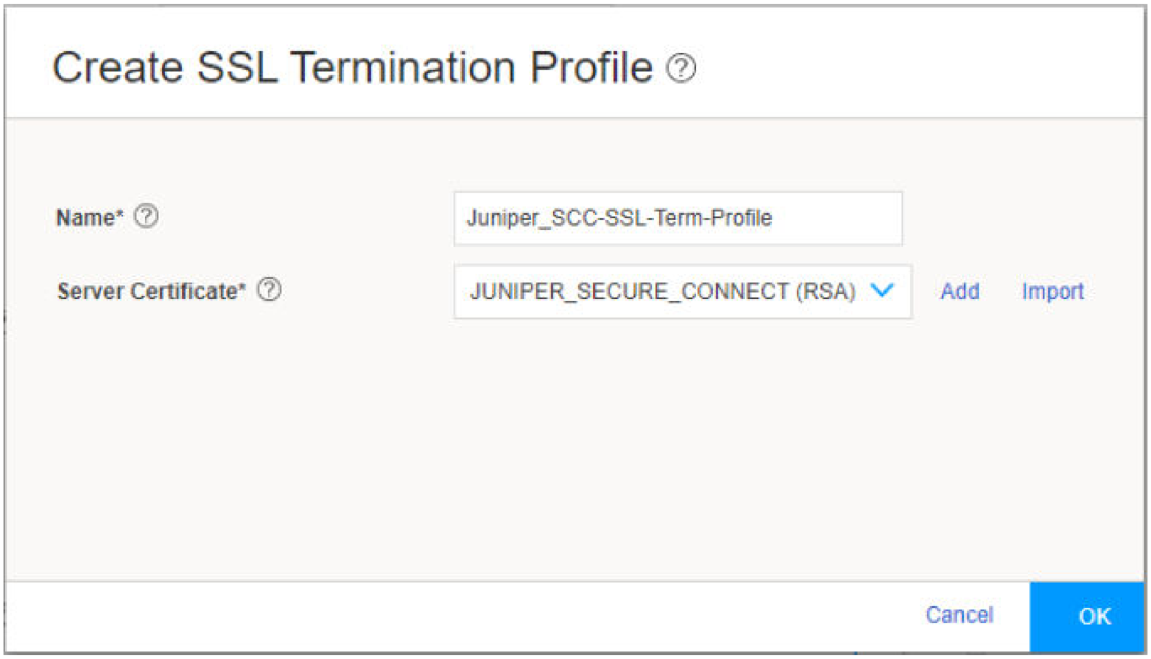
SSL Termination Profile Juniper_SCC-SSL-Term-Pr...

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 act 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.

Figure 84 on page 224 shows an example of the Create SSL Termination Profile page.

Figure 84: Create SSL Termination Profile Page



Create SSL Termination Profile

Name*: Juniper_SCC-SSL-Term-Profile

Server Certificate*: JUNIPER_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.

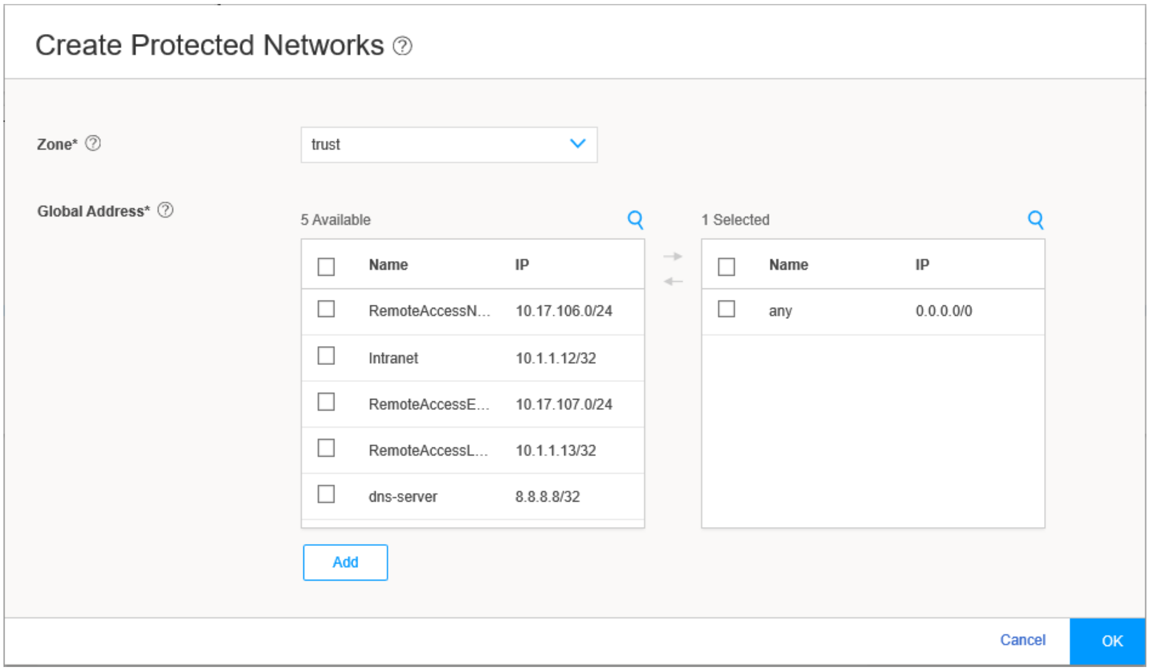
- Click **OK**.

i. 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.

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

Figure 85 on page 225 shows an example of the Create Protected Networks page.

Figure 85: Create Protected Networks Page



Create Protected Networks

Zone*: trust

Global Address*

5 Available

□	Name	IP
□	RemoteAccessN...	10.17.106.0/24
□	Intranet	10.1.1.12/32
□	RemoteAccessE...	10.17.107.0/24
□	RemoteAccessL...	10.1.1.13/32
□	dns-server	8.8.8.8/32

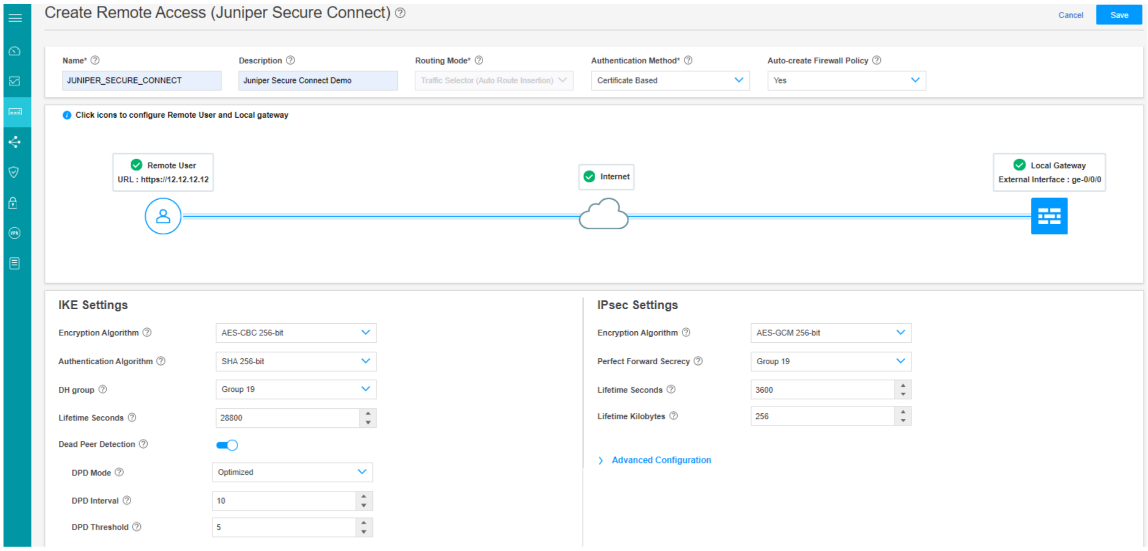
1 Selected

□	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.

Figure 86 on page 226 shows an example of successful completion of remote access configuration with remote user and local gateway.

Figure 86: Complete Remote Access Configuration



Create Remote Access (Juniper Secure Connect)

Name*: JUNIPER_SECURE_CONNECT

Description: Juniper Secure Connect Demo

Routing Mode*: Traffic Selector (Auto Route Insertion)

Authentication Method*: Certificate Based

Auto-create Firewall Policy: Yes

Click icons to configure Remote User and Local gateway

Remote User URL : https://12.12.12.12

Internet

Local Gateway External Interface : ge-0/0/0

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

DPD Threshold: 5

IPsec Settings

Encryption Algorithm: AES-GCM 256-bit

Perfect Forward Secrecy: Group 19

Lifetime Seconds: 3600

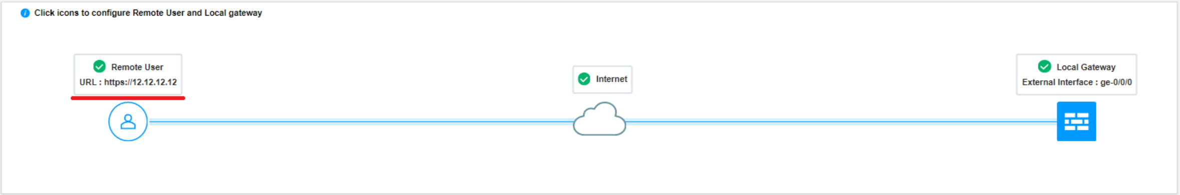
Lifetime Kilobytes: 256

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.

6. You can now find the URL for the remote users to connect to. Copy and store this URL for sharing with your remote users. You need only the /xxxx information if this configuration is not your default profile.

   Figure 87 on page 226 highlights the URL that remote user must enter in the **Gateway address** field in Juniper Secure Connect application to establish remote access connection.

Figure 87: Commit Remote Access Configuration



Click icons to configure Remote User and Local gateway

Remote User URL : https://12.12.12.12

Internet

Local Gateway External Interface : ge-0/0/0

a. Click **Save** to complete the Juniper Secure Connect VPN Configuration and associated policy if you have selected the auto policy creation option.

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

Download and install Juniper Secure Connect application on the client machine. Launch Juniper Secure Connect and connect to the gateway address of the SRX Series Firewall. You must also place the root CA certificate and user certificate at the appropriate directory location for the respective platform where you've installed Juniper Secure Connect application.

RELATED DOCUMENTATION

- Juniper Secure Connect Overview | **1**
- Local User Authentication Using Pre-shared Key | **164**
- External User Authentication Using RADIUS | **173**
- Certificate-Based Validation Using EAP-MSCHAPv2 Authentication | **189**
- Monitor and Troubleshoot Juniper Secure Connect | **239**

4

CHAPTER

Configure Juniper Secure Connect

SUMMARY

In this topic, you'll learn about configuring Juniper Secure Connect.

IN THIS CHAPTER

Juniper Secure Connect provides various features to suite your requirement. To learn about configuring these features in Juniper Secure connect, see the following topics:

- "Configure Prelogon Compliance (CLI Procedure)" on page 233
- "Configure Application Bypass (CLI Procedure)" on page 229

RELATED DOCUMENTATION

Get Started with Juniper Secure Connect | **10**

Configure Application Bypass (CLI Procedure)

SUMMARY

Read this topic to understand and configure application bypass feature in Juniper Secure Connect.

IN THIS SECTION

What is Application Bypass

Application bypass feature enables the users of the Juniper Secure Connect application to bypass specific applications based on domain names and protocols, eliminating the need for the traffic to pass through the VPN tunnel. This is different from split tunnel where you leverage VPN to encrypt confidential data while still have direct access to the internet. With application bypass, you still use VPN to encrypt confidential data, however, you can bypass VPN for certain applications defined by the administrator based on domain names and protocols.

We support Application Bypass on full tunnel configuration. Administrators configure this feature in the SRX Series Firewall in remote access client configuration parameters. These parameters define how Juniper Secure Connect client establishes VPN tunnel with your security device.

Using this task configuration, you can configure application bypass feature for remote access VPN solution in the SRX Series Firewall. As an administrator, if you want the users of your organization to access certain websites without going through the remote access VPN tunnel, follow the below procedure -

1. Identify the applications with their domain names and protocols. For example, if you want the users to be able to access enterprise applications like Zoom, Sharepoint, Salesforce, etc., without going through the VPN, then you need to specify them in the configuration as follows -

   - For Oracle cloud application suite, specify *cloud.oracle.com* as the domain name match criteria.

   - For Salesforce CRM application and all its sub-domain names, specify the application match criteria as *.salesforce.com* using the keyword `wildcard`. When you specify using `wildcard` keyword, if your main domain is salesforce.com, then the wildcard sub-domain names of the Salesforce application can be login.salesforce.com, help.salesforce.com, and developer.salesforce.com etc. So, with this, you can bypass VPN for login.salesforce.com, help.salesforce.com, and developer.salesforce.com. Any left most label part of the domain name will be used with the specified matched criteria.

   - To match any domain name containing a specific value, use `contains` keyword. For example, for domain-name with value sharepoint.com, specify *sharepoint.com* with `contains` keyword. So any domain-name that contains sharepoint.com will also bypass the VPN. This is different from wildcard match because with contains keyword, the domain name string can be anywhere in the FQDN. For example, if you use example.gov with contains keyword, it matches all conditions like example.gov.in, edu.example.gov.

   - For bypassing applications based on protocol, specify either `tcp`, `udp` or `all`.

2. Categorize these applications based on your use case to group them with a `term` *name*. In your SRX Series Firewall, you can create multiple terms to configure multiple application bypass entries and associate them to a particular remote client's configuration parameters at the `[edit security remote-access client-config]` hierarchy level.

3. Identify the remote client to which you can associate the application bypass rules.

How to Configure Application Bypass

To configure application bypass feature using the command line interface:

1. Log in to your SRX Series Firewall using the command line interface (CLI).

2. Configure remote-access VPN in full tunnel configuration mode. See one of the following procedures based on the authentication method used -

   - "Local User Authentication Using Pre-shared Key (CLI Procedure)" on page 74

   - "External User Authentication (CLI Procedure)" on page 91

- "Certificate-Based Validation Using EAP-MSCHAPv2 Authentication (CLI Procedure)" on page 127
- "Certificate-Based Validation Using EAP-TLS Authentication (CLI Procedure)" on page 145

3. To bypass the VPN, configure the identified applications as shown in Table 24 on page 231

Table 24: Application Bypass Configuration Parameters

Options	Domain Name/Protocol	Description
fqdn	cloud.example.com	Specify a cloud application.
wildcard	.example.in	Covers enterprise applications like - • payroll.example.in • sales.example.in • marketing.example.in • hr.example.in
contains	example.edu	Specify content that contains the specific domain name.
protocol	• tcp • udp	Specify TCP and UDP based applications.

4. - Using `domain-name` as *FQDN* -

```
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT application-
bypass term term1 description Cloud Applications
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT application-
bypass term term1 domain-name fqdn cloud.example.com
```

- Using `domain-name` with `wildcard` keyword -

```
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT application-
bypass term term2 description Enterprise Applications
```

```
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT application-bypass term term2 domain-name wildcard .example.com
```

- Using domain-name containing a value, say, *sharepoint.com* -

```
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT application-bypass term term3 description Education Services
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT application-bypass term term3 domain-name contains example.edu
```

- Based on tcp -

```
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT application-bypass term term4 description All TCP based applications
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT application-bypass term term4 protocol tcp
```

- Based on udp -

```
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT application-bypass term term4 description All UDP based applications
user@host# set security remote-access client-config JUNIPER_SECURE_CONNECT application-bypass term term4 protocol udp
```

5. When you are done configuring the feature on your device, enter commit from configuration mode.

Once Juniper Secure Connect VPN connection is established, your end users can now bypass remote-access VPN when they access these applications, thus simplifying their experience.

RELATED DOCUMENTATION

application-bypass (Juniper Secure Connect)

Configure Prelogon Compliance (CLI Procedure)

SUMMARY

Read this topic to know about prelogon compliance checks and how to configure them in Juniper Secure Connect.

IN THIS SECTION

What is Prelogon Compliance

Juniper Secure Connect application exchanges details with the SRX Series Firewall to perform prelogon compliance checks. The administrator configures the prelogon compliance rules on the SRX Series Firewall to validate the status of a connecting client device. These prelogon compliance checks refers to validations that are performed prior to authentication. Based on the different match criteria, action is taken to admit or reject a connecting client device.

This feature ensures that the Juniper Secure Connect application fulfills the connection criteria with the SRX Series Firewall, thereby providing enhanced security measures set by the administrator.

The purpose of prelogon compliance policies is to validate the endpoint's current context based on the compliance criteria set by your organization. You authorize the access based on these compliance policies. The device performs the prelogon compliance check using prelogon compliance policies prior to the user authentication.

As an administrator you configure a set of rules on your SRX Series Firewall to allow or reject an endpoint before establishing a remote access VPN connection. Here endpoint refers to the client or the host on which Secure Connect application is installed. You create rules based on the supported client platforms like Windows, macOS, Android and iOS. You can use multiple other match criteria like Device ID, hostname, ms-domain name and ms-workgroup name for the match criteria.

The SRX Series Firewall processes these rules based on certain evaluation criteria. See compliance (Juniper Secure Connect) evaluation criteria for further details on evaluation criteria. For more details on the compliance rule name, term rule name, match criteria and action, see compliance (Juniper Secure Connect).

How to Configure Prelogon Compliance Rules

Let us consider the following rules mentioned in Table 25 on page 234 for this configuration task -

Table 25: Prelogon Compliance Rules

Compliance Rule Name	Term Name	Match Criteria (Values)	Action
Compliant	SecureConnect	platform • windows • app-version<23.4.13.14.29669 • macos • os-version<12.5.1	reject
	Decommissioned	deviceid • c8163be5d7077d35989e0b0e6b9271bfa53003e4251a24e588c10302c4972123	reject
	BYOD	deviceid • c8163be5d7077d35989e0b0e6b9271bfa5312fa2251a24e588c10302c4903kd2	accept

Table 25: Prelogon Compliance Rules *(Continued)*

Compliance Rule Name	Term Name	Match Criteria (Values)	Action
	CorpDevices	• hostname • device1 • device2 • ms-domain • example.net • deviceid • c8163be5d7077d35989e0b0e6b9271bfa5300fa2251a24e578c10302c4972aff • c8163be5d7077d35989e0b0e6b9271bfa5300fa2251a24e588c10302c4972124	accept

To configure prelogon compliance rules using the command line interface:

1. Log in to your SRX Series Firewall using the command line interface (CLI).

2. Configure remote-access VPN in full tunnel configuration mode. See one of the following procedures based on the authentication method used -

   - "Local User Authentication Using Pre-shared Key (CLI Procedure)" on page 74

   - "External User Authentication (CLI Procedure)" on page 91

   - "Certificate-Based Validation Using EAP-MSCHAPv2 Authentication (CLI Procedure)" on page 127

   - "Certificate-Based Validation Using EAP-TLS Authentication (CLI Procedure)" on page 145

3. Refer to the prelogon compliance rules as shown in Table 25 on page 234 to configure the rules on your SRX Series Firewall.

4. Configure prelogon compliance policy *Compliant* at `[edit security remote-access]` hierarchy level -

- With term rule *SecureConnect* and its match criteria and action -

```
[edit security remote-access]
user@host# set compliance pre-logon Compliant term SecureConnect match platform windows
app-version less-than 23.4.13.14.29669
user@host# set compliance pre-logon Compliant term SecureConnect match platform macos app-
version less-than 23.3.4.70.29996
user@host# set compliance pre-logon Compliant term SecureConnect action reject
```

  In this term rule, for the specified Juniper Secure Connect app-version for Windows and macOS endpoints, the connection will be rejected. To know your app-version, see Juniper Secure Connect User Guide for the specific endpoint based on the supported Operating System.

- With term rule *OS* and its match criteria and action -

```
[edit security remote-access]
user@host# set compliance pre-logon Compliant term OS match platform windows os-version
less-than 10.21H2.19044.2604
user@host# set compliance pre-logon Compliant term OS match platform macos os-version less-
than 12.5.1
user@host# set compliance pre-logon Compliant term OS action reject
```

  In this term rule, for the specified os-versions for Windows and macOS endpoints, the connection will be rejected.

- With term rule *Decommissioned* and its match criteria and action -

```
[edit security remote-access]
user@host# set compliance pre-logon Compliant term Decommissioned match deviceid
c8163be5d7077d35989e0b0e6b9271bfa53003e4251a24e588c10302c4972123
user@host# set compliance pre-logon Compliant term Decommissioned action reject
```

  In this term rule, for the specified Device ID, the connection will be rejected. To get the Device ID, see Juniper Secure Connect User Guide

- With term rule *BYOD* and its match criteria and action -

```
[edit security remote-access]
user@host# set compliance pre-logon Compliant term BYOD match deviceid
```

```
c8163be5d7077d35989e0b0e6b9271bfa5312fa2251a24e588c10302c4903kd2
user@host# set compliance pre-logon Compliant term BYOD action accept
```

In this term rule, for the specified Device ID, the connection will be accepted. To know the Device ID, see Juniper Secure Connect User Guide

- With term rule *CorpDevices* and its match criteria and action -

```
[edit security remote-access]
user@host# set compliance pre-logon Compliant term CorpDevices match hostname device1
user@host# set compliance pre-logon Compliant term CorpDevices match hostname device2
user@host# set compliance pre-logon Compliant term CorpDevices match ms-domain example.net
user@host# set compliance pre-logon Compliant term CorpDevices match deviceid
c8163be5d7077d35989e0b0e6b9271bfa5300fa2251a24e578c10302c4972aff
user@host# set compliance pre-logon Compliant term CorpDevices match deviceid
c8163be5d7077d35989e0b0e6b9271bfa5300fa2251a24e588c10302c4972124
user@host# set compliance pre-logon Compliant term CorpDevices action accept
```

  In this term rule, for the specified hostnames, ms-domain name and Device ID the connection will be accepted. To know the Device ID, see Juniper Secure Connect User Guide

5. For any other criteria that is not defined in this compliance rule *Compliant*, i.e. when no further term rule is specified for an unmatched rule, the default action is `reject`.

6. Once the compliance rules are defined for a compliance policy, attach the compliance policy to the remote-access profile, *ra.example.com* created in step 2 -

```
[edit security remote-access profile ra.example.com]
user@host# set compliance pre-logon SecureConnect
```

7. When you are done configuring the feature on your device, enter commit from configuration mode.

8. Based on the use case, you can create multiple compliance policies like *SecureConnect* and attach each of them to the remote-access profiles that you create. Ensure one compliance policy is associated to a remote-access profile.

This features ensures that the Juniper Secure Connect application fulfills the connection criteria with the SRX Series Firewall, thereby providing enhanced security measures set by the administrator.

RELATED DOCUMENTATION

compliance (Juniper Secure Connect)

5

CHAPTER

Monitor Juniper Secure Connect

SUMMARY

In this topic, you'll learn about monitoring Juniper Secure Connect.

IN THIS CHAPTER

You can monitor Juniper Secure Connect VPN connections, Junos OS logs and Juniper Secure Connect application logs. To learn about monitoring Juniper Secure connect, see the following topics:

- "Monitor and Troubleshoot Juniper Secure Connect" on page 239
- "Juniper Secure Connect Integration with JIMS" on page 255

RELATED DOCUMENTATION

Get Started with Juniper Secure Connect | 10

Monitor and Troubleshoot Juniper Secure Connect

SUMMARY

This topic contains information about VPN monitoring and troubleshooting issues with Juniper Secure Connect.

IN THIS SECTION

For monitoring the VPN connection, use the J-Web interface, as described in "Monitor Your VPN Connection" on page 239.

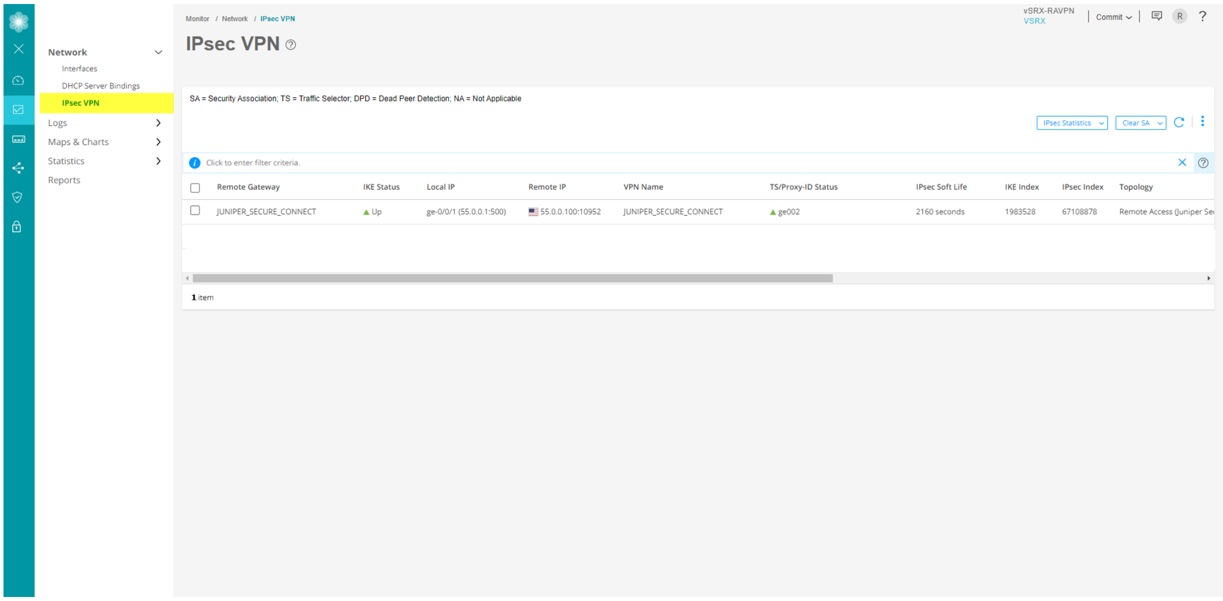
If you encounter any issues while using Juniper Secure Connect application, we recommend that you follow these steps to check the log messages and locate the issue:

- "Check the logs in Junos OS" on page 241
- "Check the logs in the Juniper Secure Connect application" on page 242

Monitor Your VPN Connection

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 88 on page 240 shows the sample IPsec VPN page under monitoring menu option.

Figure 88: Monitor IPsec VPN Page



Monitor / Network / IPsec VPN

IPsec VPN

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

Click to enter filter criteria.

□	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

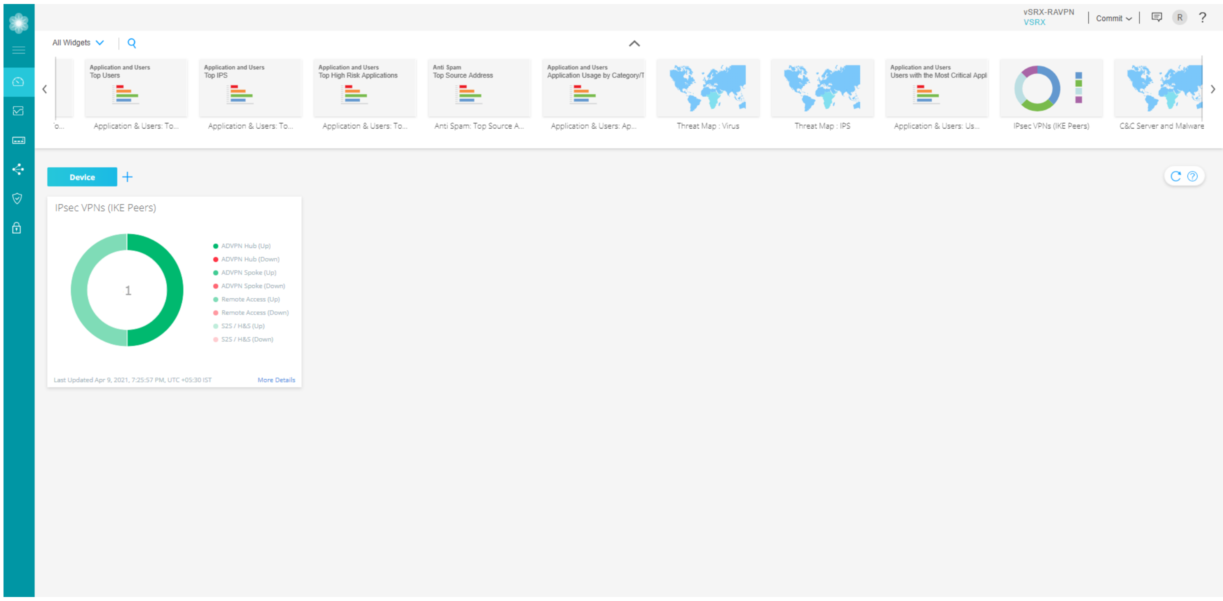
1 item

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 89 on page 241. Hover over the sections in the widget, to view the IKE peers count with VPN topology type. See Dashboard Overview .

Figure 89: Sample IPsec VPNs (IKE Peers) Dashboard

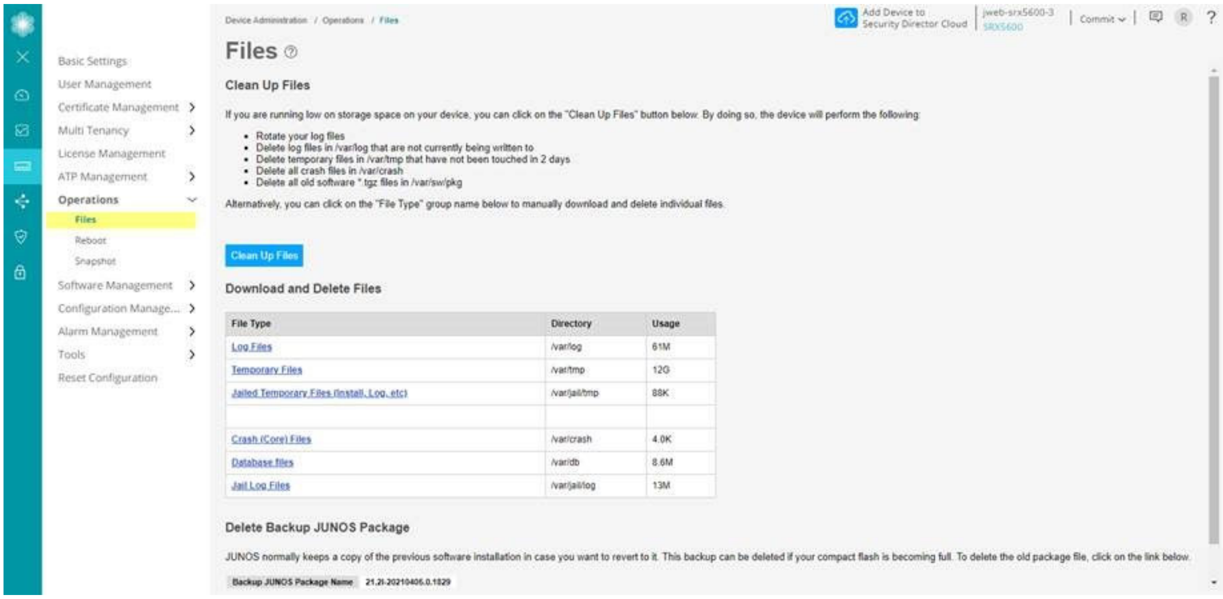


Check Junos OS Logs

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 90: Files Page



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

IN THIS SECTION

Windows

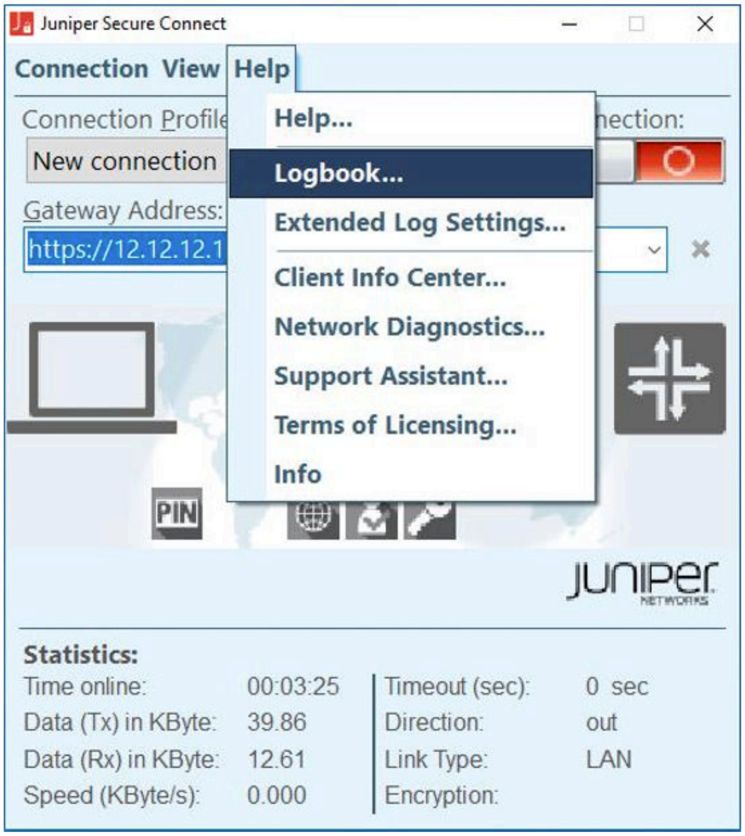
Following are the steps to check the Juniper Secure Connect application logs on a Windows device:

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 91: Logbook Menu Option



Connection Profile: New connection

Gateway Address: https://12.12.12.1

Connection:

Statistics:

Time online: 00:03:25

Data (Tx) in KByte: 39.86

Data (Rx) in KByte: 12.61

Speed (KByte/s): 0.000

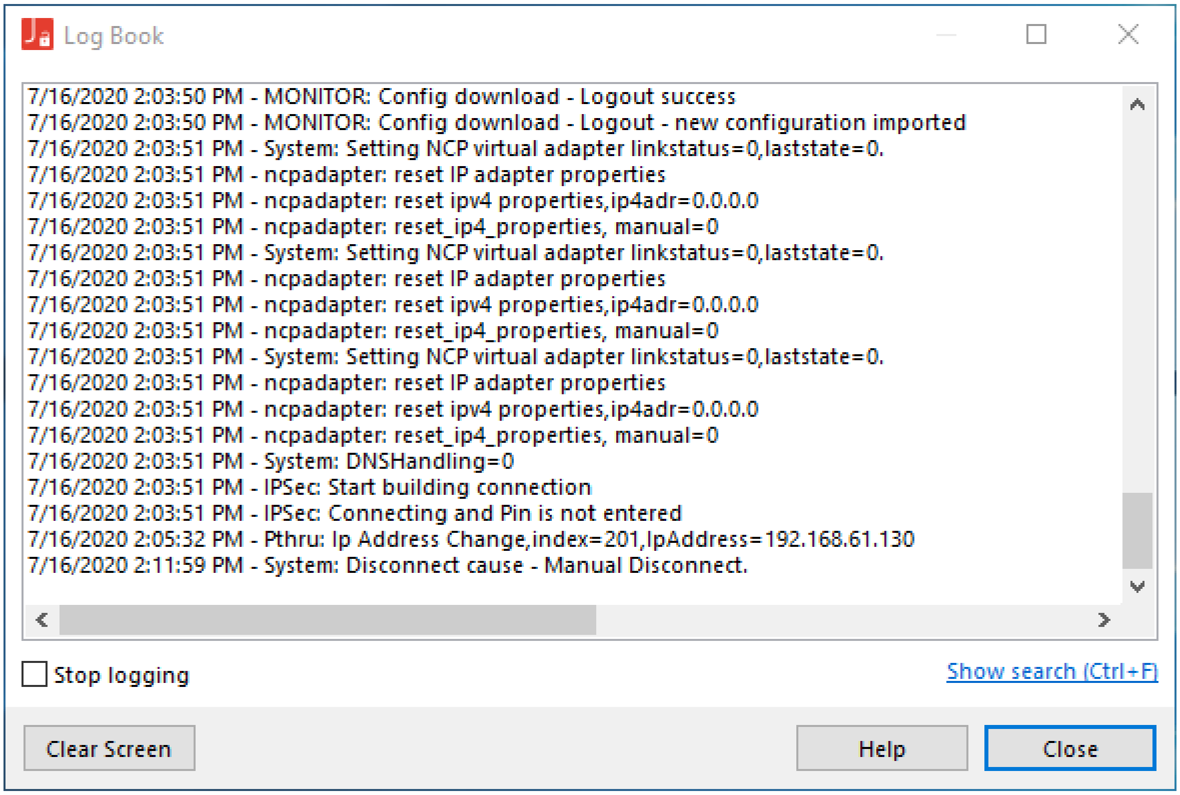
Timeout (sec): 0 sec

Direction: out

Link Type: LAN

Encryption:

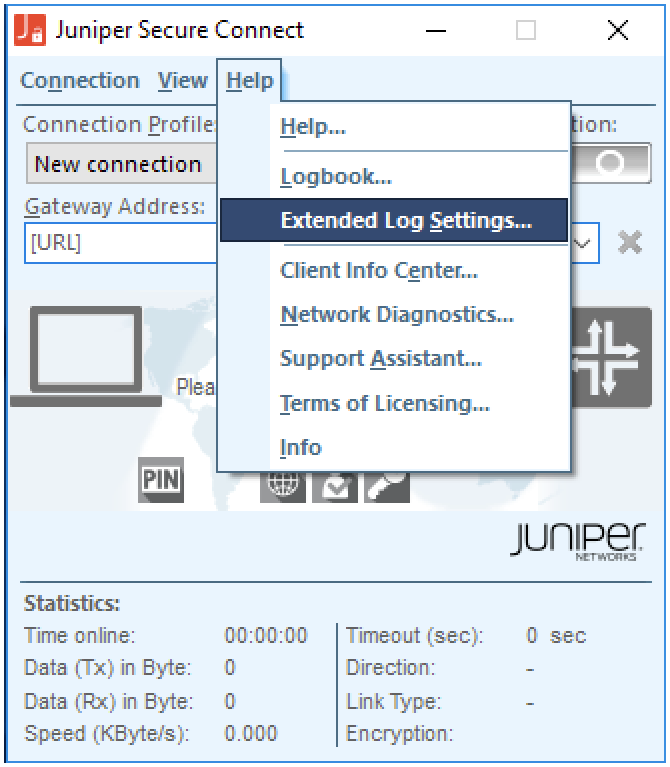
Figure 92: Log Message Display



```
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 93: Extended Log Settings Menu Option

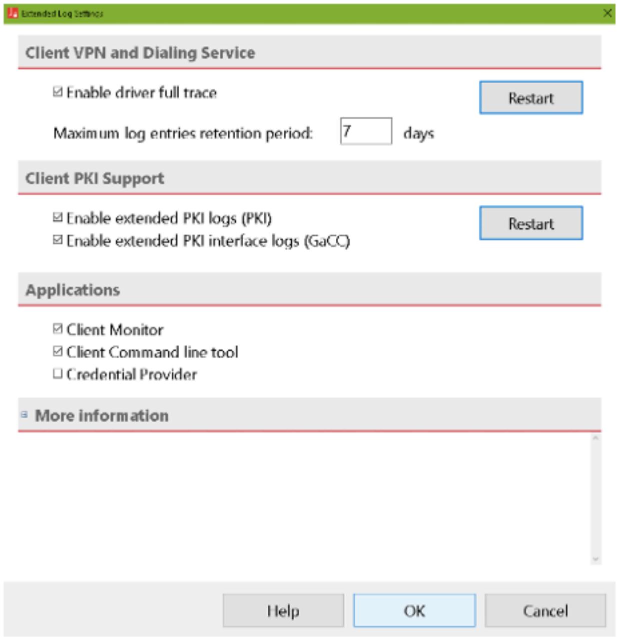


Statistics:

```
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 94: 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)

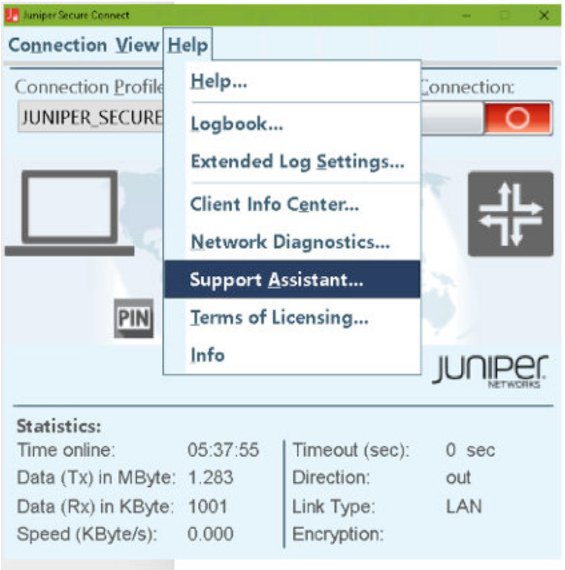
Applications

☑ 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 95: Support Assistant Menu Option

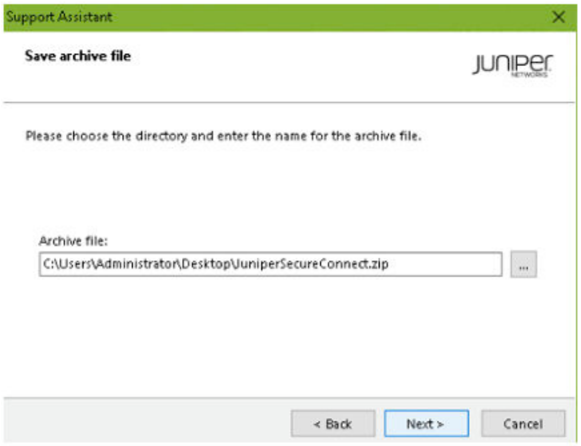


Statistics:

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.

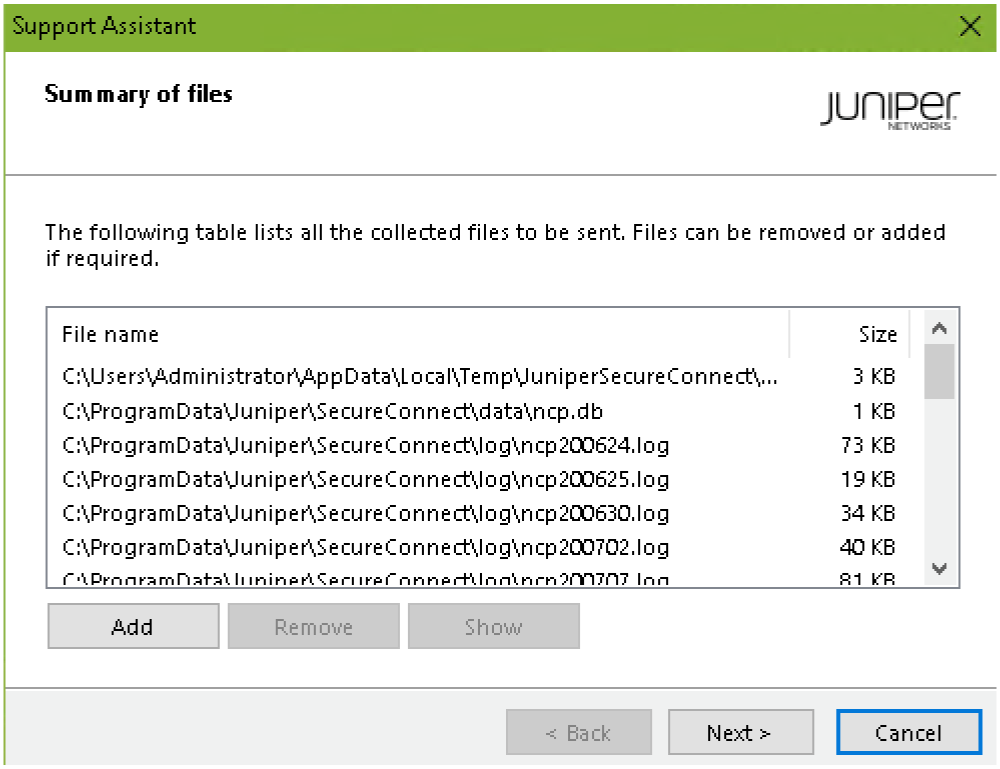
Figure 96: Save Archive File



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

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

Figure 97: Log Files List

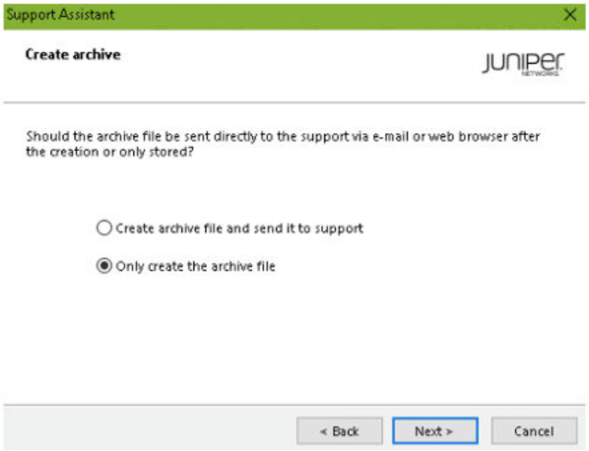


The following table lists all the collected files to be sent. Files can be removed or added if required.

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 98: Create Only Archive File



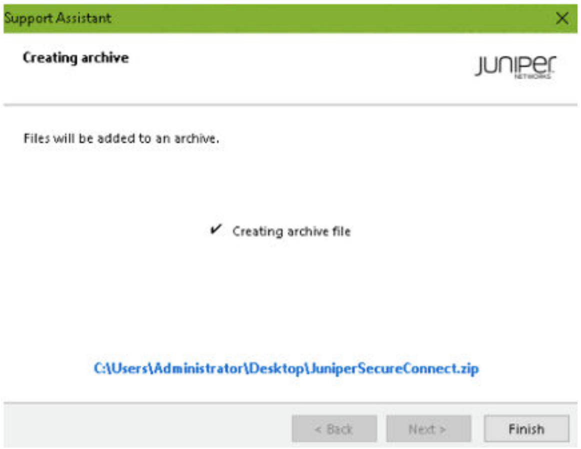
Should the archive file be sent directly to the support via e-mail or web browser after the creation or only stored?

○ 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 99: Successful Creation of Log Files Archival



Files will be added to an archive.

✓ Creating archive file

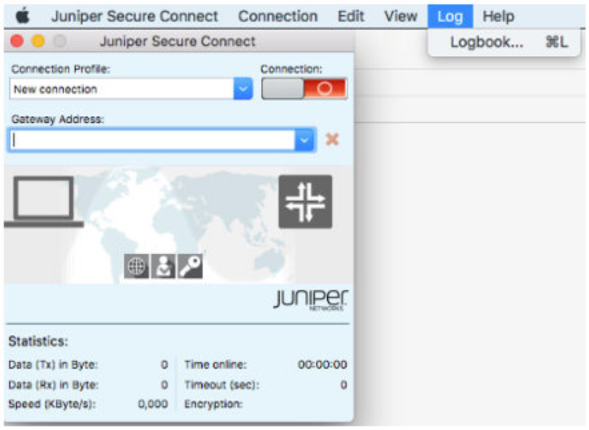
C:\Users\Administrator\Desktop\JuniperSecureConnect.zip

7. Click **Finish**.

macOS

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

Figure 100: Logbook Menu Option



Connection Profile: New connection

Connection:

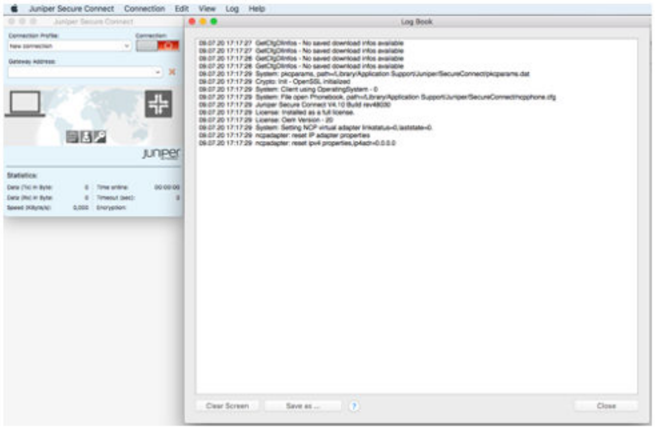
Gateway Address:

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 101: Displaying Log Information

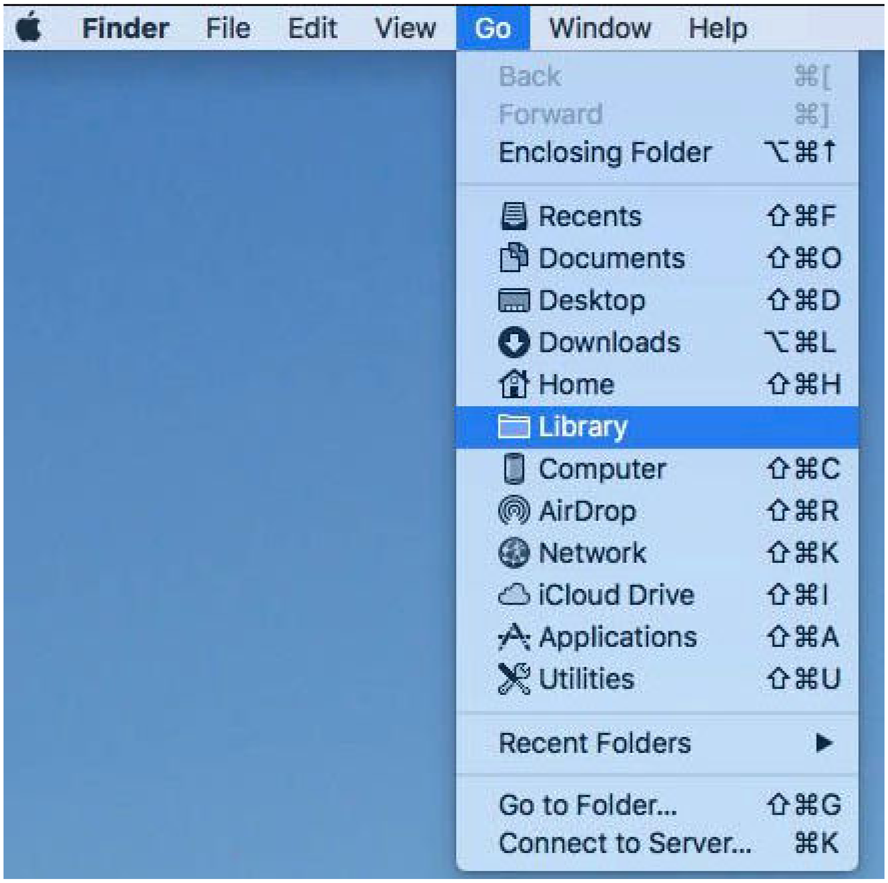


```
09.07.20 17:17:27 GetCfgDlInfos - No saved download infos available
09.07.20 17:17:27 GetCfgDlInfos - No saved download infos available
09.07.20 17:17:28 GetCfgDlInfos - No saved download infos available
09.07.20 17:17:28 GetCfgDlInfos - No saved download infos available
09.07.20 17:17:29 System: 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**.

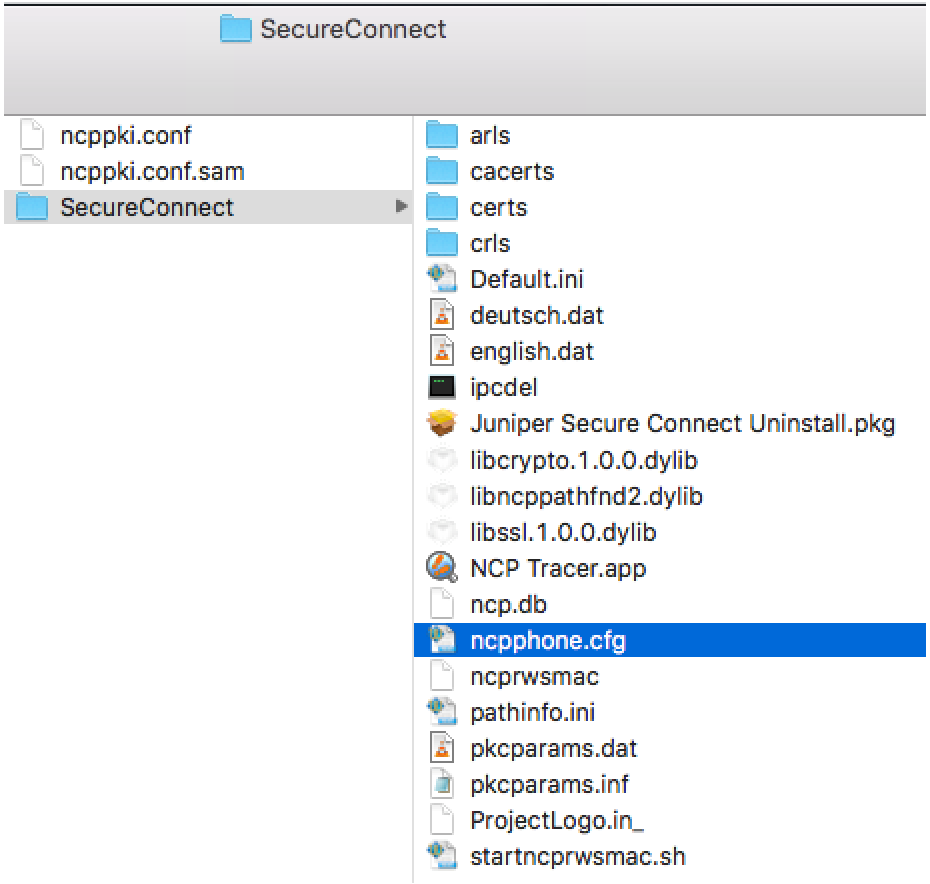
3. To locate the **ncpphone.cfg** file, open the **Finder** and select **Go** in the menu bar and at the same time press down the “Option” key on your keyboard.

Figure 102: Open File Library



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

Figure 103: Juniper Secure Connect Directory



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 104: Juniper Secure Connect Application Screen

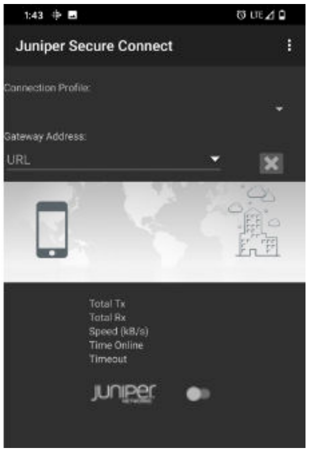
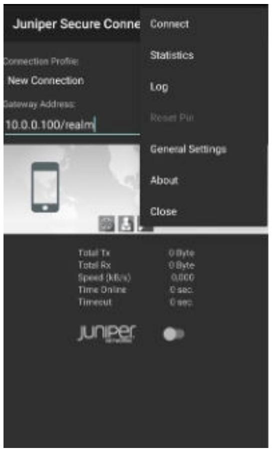


Figure 105: Log Menu Option



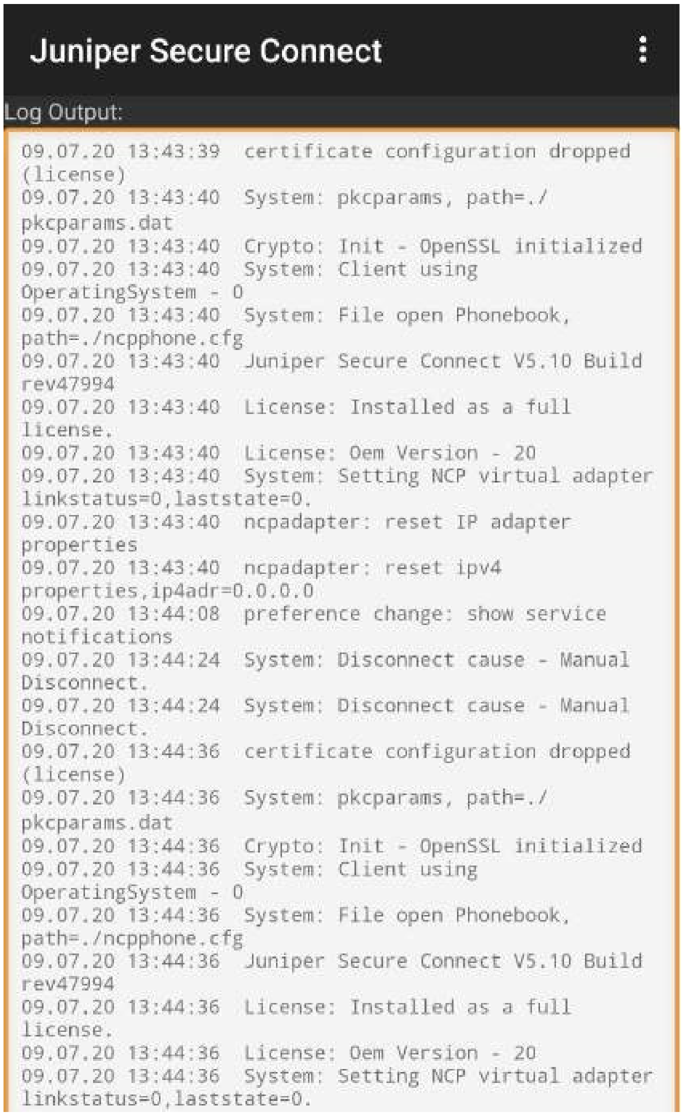
Connection Profile:
New Connection

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 106: Displaying Log Information

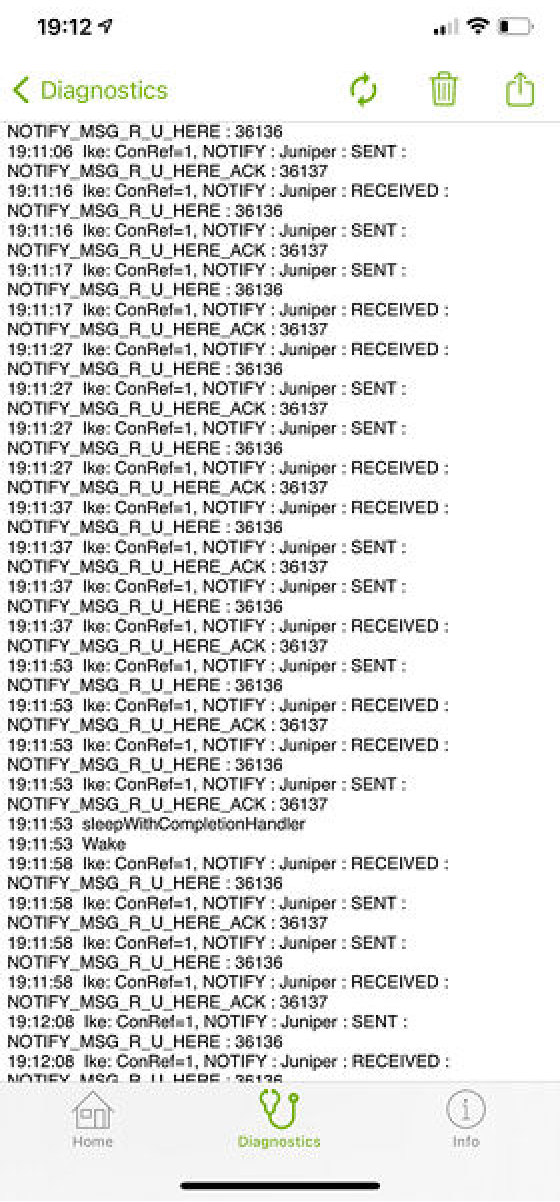


```
09.07.20 13:43:39  certificate configuration dropped
(license)
09.07.20 13:43:40  System: pkcparams, path=./
pkcparams.dat
09.07.20 13:43:40  Crypto: Init - OpenSSL initialized
09.07.20 13:43:40  System: Client using
OperatingSystem - 0
09.07.20 13:43:40  System: File open Phonebook,
path=./ncpphone.cfg
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 107: 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
```

RELATED DOCUMENTATION

Juniper Secure Connect Overview | 1

Local User Authentication Using Pre-shared Key | 164

External User Authentication Using RADIUS | 173

Juniper Secure Connect Integration with JIMS

SUMMARY

Read this topic to learn how SRX Series Firewalls use the push to identity management (PTIM) solution to send VPN connection state events to Juniper Identity Management Service (JIMS).

IN THIS SECTION

Juniper® Identity Management Service (JIMS) is a software application that runs on Microsoft Windows. JIMS collects user, device, and group information from different sources and maintains this information for SRX Series Firewalls. The firewall sends the remote access VPN connection state events to JIMS. From these log messages, JIMS extracts the remote access VPN username, mapped IP address, and domain name of Juniper Secure Connect for tracking and troubleshooting.

The firewall can send the log messages to JIMS in two ways:

- Syslog solution: JIMS receives the system logs (syslogs) related to each user's VPN connection state events, excluding the rekey state, from the SRX Series Firewall. JIMS parses the logs by using the custom regex that you define and stores the information in its database. SRX Series Firewall supports only the syslog solution until Junos OS Release 24.2R1. For more details, see JIMS Identity Producers Syslog Sources.

- Push to identity management (PTIM) solution: The firewall pushes the VPN connection state events, including the rekey state, along with the IP address and the domain name details of each user. The firewall sends the details directly to JIMS by using the PTIM solution without any interaction with the syslog. Starting from Junos OS Release 24.4R1 onwards, support for PTIM solution is available. We recommend that you use the PTIM solution instead of the syslog solution.

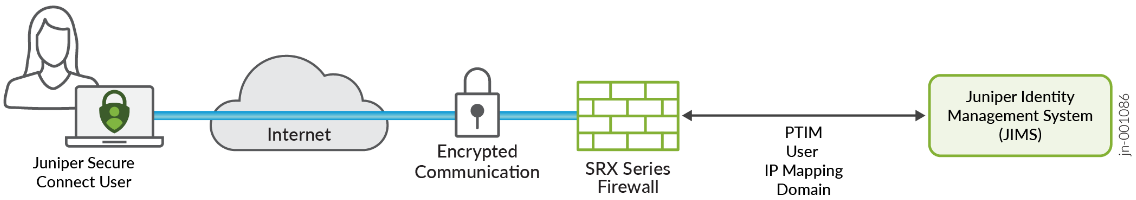
Read further to understand the PTIM solution.

Push to Identity Management Solution Overview

IN THIS SECTION

SRX Series Firewalls communicate with JIMS through an HTTP or HTTPS connection. Figure 108 on page 256 shows the setup between Juniper Secure Connect and JIMS.

Figure 108: Juniper Secure Connect Integration with JIMS


Juniper Secure Connect User
Internet
Encrypted Communication
SRX Series Firewall
PTIM User IP Mapping Domain
Juniper Identity Management System (JIMS)
jn-001086

Read the following information to understand how the PTIM solution works:

- To use the PTIM solution, you must run the IPsec VPN services that uses the iked process and configure the identity management service on the firewall.
- The PTIM solution directly reports the VPN connect states such as tunnel connect (`IKE_VPN_UP_ALARM_USER`), tunnel disconnect (`IKE_VPN_DOWN_ALARM_USER`), and tunnel rekey (`IKE_VPN_UP_ALARM_USER`) to JIMS.
- The solution doesn’t stop the iked process from sending the VPN connect state events to the syslog. The iked process sends these connection state events to both the JIMS server and the firewall's syslog.
- You cannot configure PTIM when the firewall runs the IPsec VPN service that uses the kmd process.

To enable PTIM, see "Enable Push to Identity Management" on page 257.

Benefits

- Reliability—Unlike the syslog solution, the PTIM solution supports IPsec VPN rekey events.
- Ease of integration—Provides an easy integration between Juniper Secure Connect and JIMS, as no additional infrastructure is required.
- Comprehensive solution—Shares information about context-based policies, such as the prelogon compliance policies that are used to validate the legitimacy of access.

Limitations

- The firewall sends the username, IP address, and domain name of each user but not the device ID, device OS, and hostname to JIMS.
- When you attach the same IPsec VPN object in two different remote access profiles, you must use the same domain alias name in the remote access profiles. Avoid configuring different domain alias names for different remote-access profiles that use the same IPsec VPN object. For more information about using domain names, see "Enable Push to Identity Management" on page 257.

SEE ALSO

Enable Push to Identity Management | **257**

Juniper Identity Management Service User Guide

Enable Push to Identity Management

Ensure you meet the following prerequisites on the SRX Series Firewall to send the VPN connect state events to JIMS using the PTIM solution:

- SRX Series Firewall with Junos OS Release 24.4R1 or later.
- SRX Series Firewall with the `junos-ike` package installed for IPsec VPN service. See IPsec VPN Feature Support with New Package.

To configure PTIM and verify the configuration:

1. Configure the identity management feature.

   Configure the `identity-management` statement at the `[edit services user-identification]` hierarchy level to enable the firewall to collect the identity information. Note that PTIM is enabled by default if you configure identity management on your firewall. See identity-management.

2. (Optional) Configure the domain alias name in the firewall if the Juniper Secure Connect application sends username only.

   Configure the `user-domain` *`user-domain`* statement at the `[edit security remote-access profile` *`realm-name`* `options]` hierarchy level separately for each of the remote access profiles.

   When you associate an IPsec VPN object in two different remote access profiles, you must use the same domain alias name in those remote access profiles. Avoid configuring different domain alias names for remote-access profiles using the same IPsec VPN object. For example, when you map the profiles hr and engineering with the same IPsec VPN object vpn1, use the same domain alias name example.com for both the profiles.

If the Juniper Secure Connect user doesn't disclose the domain alias name, the iked process sends the `missing-domain-secureconnect` message as part of the domain name to JIMS for all the tunnel states of that user. See profile (Juniper Secure Connect).

3. Verify the IPsec VPN tunnel event statistics for the count of the VPN connection state events sent to JIMS by using the PTIM solution.

   Use the command `show security ipsec tunnel-events statistics` to view the identity management statistics. See show security ipsec tunnel-events statistics.

4. Verify the IPsec VPN security associations (SAs) for the count and the sequence of events that the VPN gateway generates and sends to JIMS.

   Use the command `show security ipsec security-associations detail` to view the number of times the firewall sends a tunnel event to JIMS. For example, the firewall can send a tunnel create, tunnel delete, or tunnel rekey event to JIMS. See show security ipsec security-associations.

To disable PTIM on your SRX Series Firewall:

- Use the `no-push-to-identity-management` statement at the `[edit security ike gateway gateway-name aaa]` hierarchy level to disable the iked process communication with JIMS using the PTIM solution. See identity-management.

SEE ALSO

Push to Identity Management Solution Overview | **255**

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
24.4R1	We've introduced support for Juniper Secure Connect integration with JIMS using push to identity management (PTIM) solution in Junos OS Release 24.4R1.

6

CHAPTER

Migrate to Juniper Secure Connect

SUMMARY

Read this topic to migrate to Juniper Secure Connect.

IN THIS CHAPTER

If you are using an existing Dynamic VPN deployment, you must migrate to Juniper Secure Connect. See the following topic to migrate to Juniper Secure Connect:

- "How to Migrate to Juniper Secure Connect" on page 260

RELATED DOCUMENTATION

Get Started with Juniper Secure Connect | 10

How to Migrate to Juniper Secure Connect

SUMMARY

This topic is intended for the users who have existing dynamic VPN deployments and are planning to migrate to Juniper Secure Connect. If you are a new user of Juniper Secure Connect, you can skip this topic.

IN THIS SECTION

Before You Begin:

- Learn about feature comparison. See "Advantages of Juniper Secure Connect over Dynamic VPN" on page 261.
- Learn about feature enhancement. See "Juniper Secure Connect Overview" on page 1.

BEST PRACTICE: We recommend you that you back up the current working configuration if you need to rollback later or have rolled over the current configuration over your history of rollbacks for some reason.

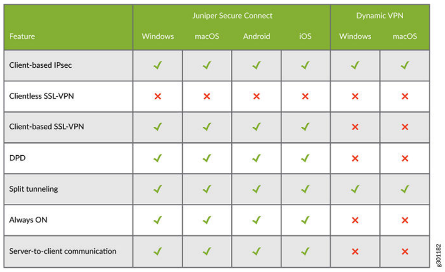
For more information, see Rescue and Recovery of Configuration File.

Advantages of Juniper Secure Connect over Dynamic VPN

Dynamic VPN is a legacy offering from Juniper Networks. Read this topic to understand the differences between Juniper Secure Connect and Dynamic VPN, and why Juniper Secure Connect is preferred over Dynamic VPN.

Figure 109 on page 261 shows the high-level comparison between Juniper Secure Connect and Dynamic VPN.

Figure 109: High-Level Feature Comparison Between Juniper Secure Connect and Dynamic VPN



	Juniper Secure Connect				Dynamic VPN	
Feature	Windows	macOS	Android	iOS	Windows	macOS
Client-based IPsec	✓	✓	✓	✓	✓	✓
Clientless SSL-VPN	✗	✗	✗	✗	✗	✗
Client-based SSL-VPN	✓	✓	✓	✓	✗	✗
DPD	✓	✓	✓	✓	✗	✗
Split tunneling	✓	✓	✓	✓	✓	✓
Always ON	✓	✓	✓	✓	✗	✗
Server-to-client communication	✓	✓	✓	✓	✗	✗

g301182

Table 26 on page 261 shows the connection feature related differences between Dynamic VPN and Juniper Secure Connect on SRX Series Firewalls:

Table 26: Differences Between Dynamic VPN and Juniper Secure Connect on SRX Series Firewalls

Connection Features	Dynamic VPN	Juniper Secure Connect
Connection mode	IPsec mode	IPsec is the preferred mode. Juniper Secure Connect automatically changes the protocol to SSL-VPN on need basis to bypass restrictive networks where IPsec traffic is blocked.
VPN connectivity mode	Policy-based VPN, which requires each firewall policy to define the connectivity and VPN establishment.	Route-based VPN connectivity. Allows you to define fine granular firewall policies including other services, such as Advanced Threat Prevention (ATP) Cloud, User Firewall, and so on.

NOTE: With Juniper Secure Connect offering more benefits, we do not provide Dynamic VPN as a solution for remote access VPN deployment. While we plan to discontinue support for Dynamic VPN, we recommend you to migrate existing Dynamic VPN deployments to Juniper Secure Connect. For migrating to Juniper Secure Connect, see Migrating from Junos OS Dynamic VPN to Juniper Secure Connect.

Licensing Requirements

As a first step, ensure that you have installed the license for Juniper Secure Connect if you need more than two concurrent users.

Licenses for Juniper Secure Connect

Configuration Requirements

NOTE: Dynamic VPN documentation is archived at Junos OS and Junos OS Evolved 23.1 Portable Library. To access the documentation, download and unzip the archived file. Locate the *vpn-ipsec.pdf* file in the unzipped folder and navigate to *Remote Access VPN* chapter.

Complete the following Dynamic VPN tasks:

- Update the firewall policies used for Dynamic VPN:
  - Verify the `from-zone` option in the current Dynamic VPN policies. The `from-zone` option will be the source-zone used in the Juniper Secure Connect VPN wizard.
  - Remove firewall policies that refer to Dynamic VPN.
- Delete IKE and IPsec configurations created for the Dynamic VPN configuration under `edit security dynamic-vpn`, `edit security ike`, and `edit security ipsec` hierarchies.

J-Web Wizard for Migration

You can use J-Web wizard for Juniper Secure Connect configuration.

We recommend that you start with a new deployment of Juniper Secure Connect because you may overlook one or more values when you migrate the current settings. When you set up a new Juniper Secure Connect:

- Check whether you have any split tunneling rules. These rule specify remote protected resources behind the SRX Series Firewall that the client communicates with over the VPN tunnel. You can check your rules at the [`set security dynamic-vpn clients configuration-name remote-protected-resources`] hierarchy-level. The same split tunnel definitions are used in the Secure Connect VPN wizard as protected networks.

- Start a new deployment in the J-Web deployment wizard. We recommend enabling the **Auto-create Firewall Policy** option to create a firewall policy automatically.

- You can reuse the access profiles and address-assignment pool in this workflow.

- If you already have a route from your network pointing to the SRX Series Firewalls and have included that IP address in the address assignment pool or have defined through the RADIUS, you can disable the use of source NAT.

- Now you are ready to start configuring Juniper Secure Connect.

RELATED DOCUMENTATION

Get Started with Juniper Secure Connect | **10**

Deploy Certificates for Juniper Secure Connect | **14**

7

CHAPTER

Juniper Secure Connect for Windows

SUMMARY

Learn about Juniper Secure Connect application for Windows.

IN THIS CHAPTER

Juniper Secure Connect application is a client-based SSL VPN software that can run on Microsoft Windows endpoint. It ensures that you securely access resources in your corporate network. To complete the setup of Juniper Secure Connect application, your system administrator must first configure remote access on the SRX Series Firewall. After the remote access is configured, you can connect to your secured corporate resources using the Juniper Secure Connect application.

Read the following topics to understand and use Juniper Secure Connect application for Windows:

- "Install Juniper Secure Connect on Windows" on page 265
- "Juniper Secure Connect GUI Elements" on page 274
- "Connection Menu" on page 281
- "View Menu" on page 295
- "Help Menu" on page 304

RELATED DOCUMENTATION

Get Started with Juniper Secure Connect | **10**

Install Juniper Secure Connect on Windows

SUMMARY

Learn about how to create rollout packages for Juniper Secure Connect application software and step-by-step procedures to install Juniper Secure Connect on Windows. If you want to install Juniper Secure Connect application, see "Manual Installation of Juniper Secure Connect" on page 266. If you are an administrator, see "Create Installation Packages for Juniper Secure Connect Rollout" on page 271 section to prepare the installer for software rollout.

IN THIS SECTION

What's Next

Download the Juniper Secure Connect application software from here. See release notes for more details.

For more information on Juniper Secure Connect GUI elements, see "Juniper Secure Connect GUI Elements" on page 274.

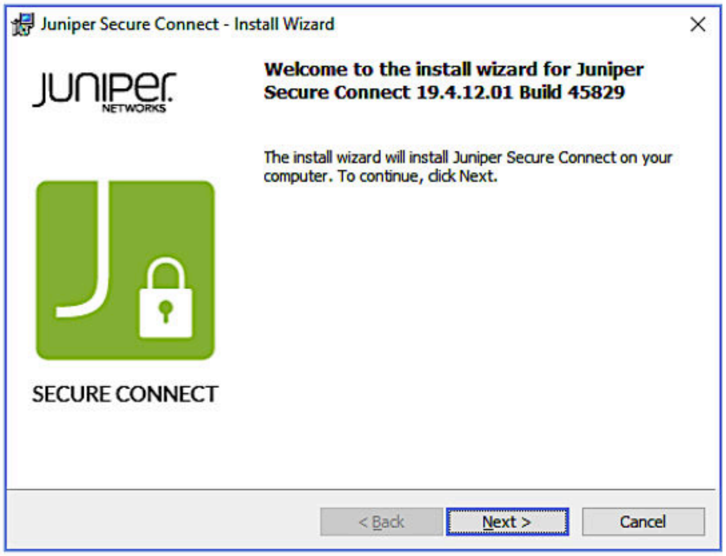
For more information on Juniper Secure Connect features and how to configure the options, see "Connection Menu" on page 281, "View Menu" on page 295, and "Help Menu" on page 304.

Manual Installation of Juniper Secure Connect

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

1. Run the Windows installer (.exe) for Juniper Secure Connect . See Figure 110 on page 266. The version that you see on the figure is dependent on the Juniper Secure Connect application release number.

Figure 110: Installer Welcome Window



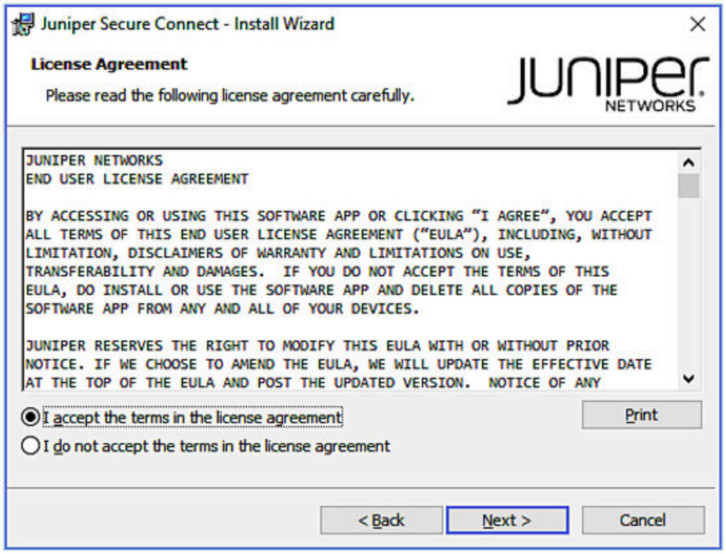
Juniper Secure Connect - Install Wizard

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 111 on page 267.

Figure 111: License Agreement Window



Juniper Secure Connect - Install Wizard

License Agreement

Please read the following license agreement carefully.

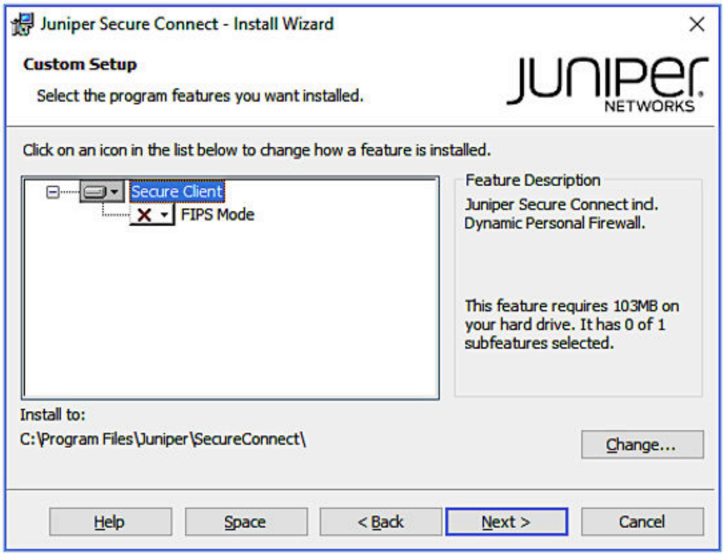
```
JUNIPER NETWORKS
END USER LICENSE AGREEMENT

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 112 on page 267.

Figure 112: 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.

Secure Client
FIPS Mode

Feature Description

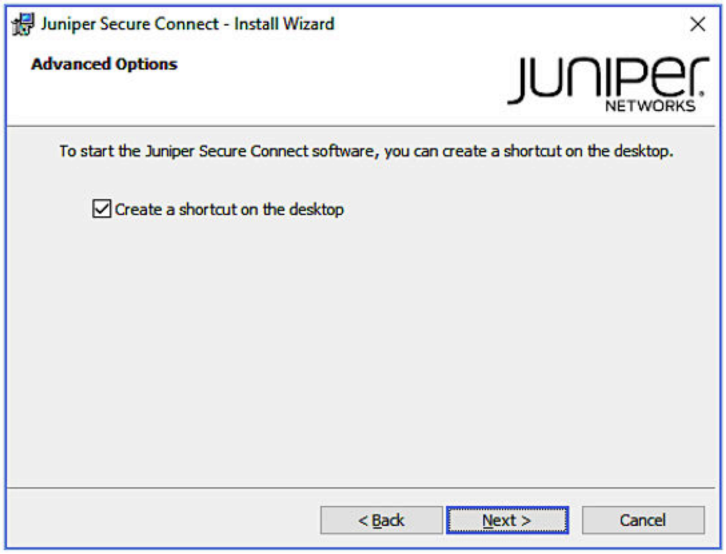
Juniper Secure Connect incl. Dynamic Personal Firewall.

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 113 on page 268.

Figure 113: Create Juniper Secure Connect Shortcut on Desktop



Juniper Secure Connect - Install Wizard

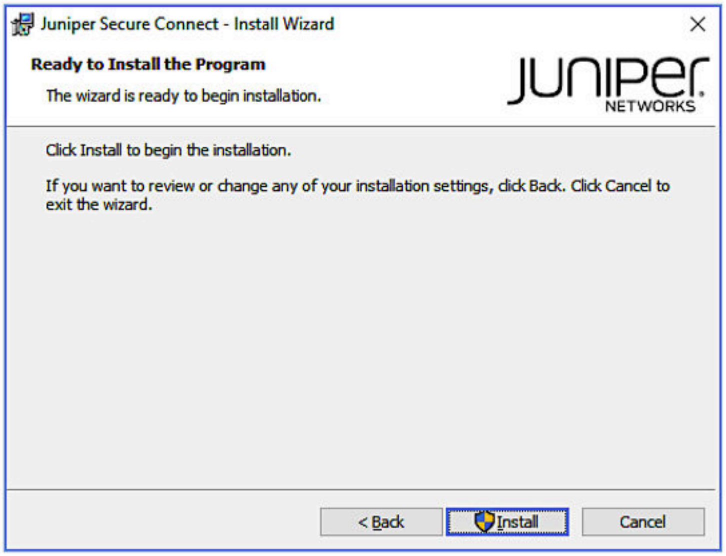
Advanced Options

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 114 on page 268.

Figure 114: Start Juniper Secure Connect Installation



Juniper Secure Connect - Install Wizard

Ready to Install the Program

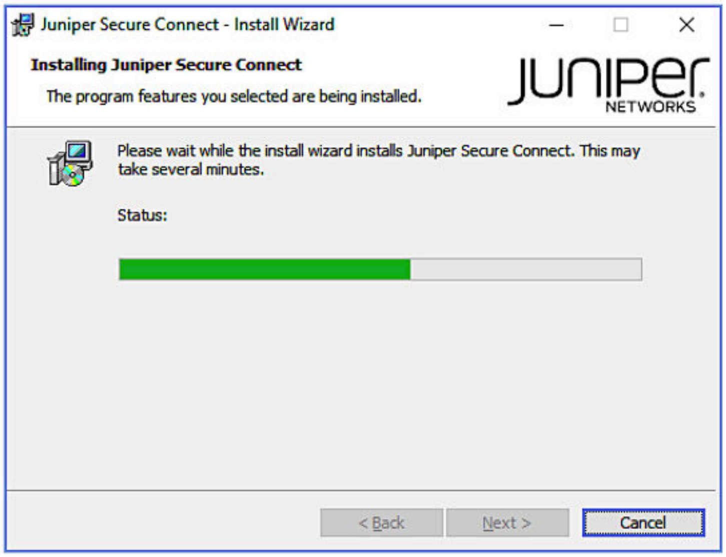
The wizard is ready to begin installation.

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 115 on page 269.

Figure 115: Juniper Secure Connect Installation Status Display


Juniper Secure Connect - Install Wizard

Installing Juniper Secure Connect

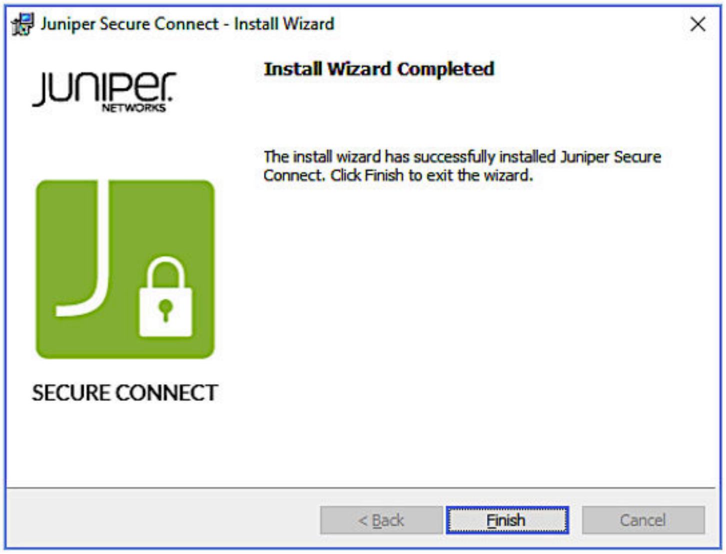
The program features you selected are being installed.

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 116 on page 269.

Figure 116: Juniper Secure Connect Installation Completed


Juniper Secure Connect - Install Wizard

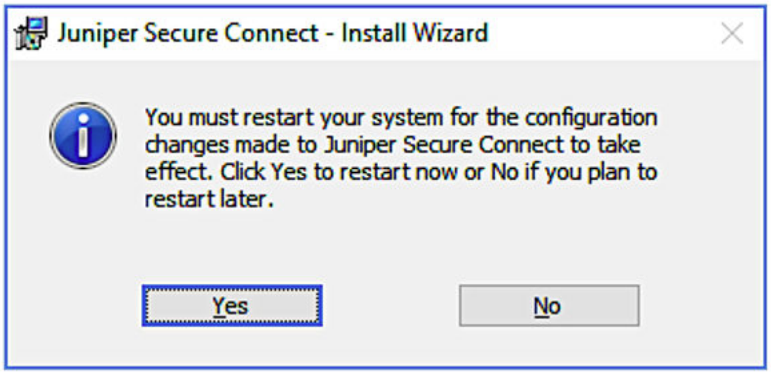
Install Wizard Completed

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

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

7. To use the application, you must first restart your system. See Figure 117 on page 270.

Figure 117: System Restart Notification



Juniper Secure Connect - Install Wizard

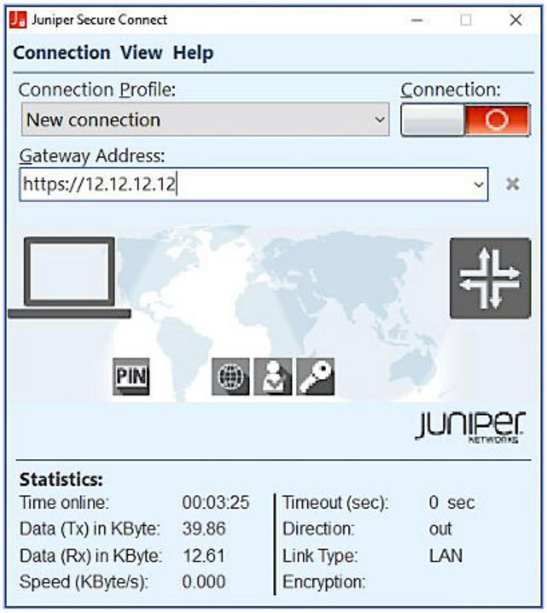
You must restart your system for the configuration changes made to Juniper Secure Connect to take effect. Click Yes to restart now or No if you plan to restart later.

8. You can now launch the Juniper Secure Connect and enter the **Gateway Address** URL to connect with the SRX Series Firewall. Figure 118 on page 270 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.example.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 118: Launch Juniper Secure Connect



Connection Profile: New connection

Gateway Address: https://12.12.12.12

Statistics:

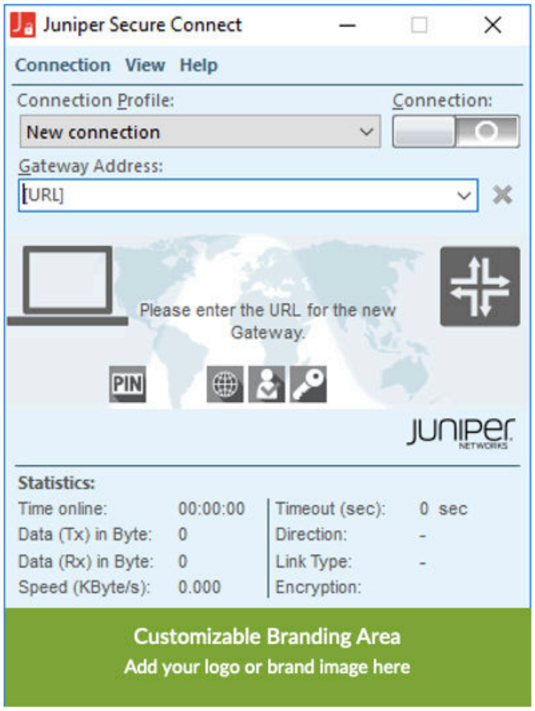
Time online:	00:03:25	Timeout (sec):	0 sec
Data (Tx) in KByte:	39.86	Direction:	out
Data (Rx) in KByte:	12.61	Link Type:	LAN
Speed (KByte/s):	0.000	Encryption:	

Custom Branding Option

Juniper Secure Connect for windows allows you to add your own logo or branding image. It also allows you to add HTML page for the branding image that would open when you click on the branding area in the Juniper Secure Connect. The HTML page is optional where you can provide any information you want. You should customise the installation package for branding your client. For detailed instructions, see Create Installation Packages for Juniper Secure Connect Rollout (Windows).

Figure 119 on page 271 is the sample screen, where the customizable branding area is highlighted:

Figure 119: Custom Branding Option (Windows)



Connection Profile: New connection

Connection:

Gateway Address: [URL]

Please enter the URL for the new Gateway.

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:	

Customizable Branding Area
Add your logo or brand image here

Create Installation Packages for Juniper Secure Connect Rollout

As a system administrator, you can also build your own rollout packages, if required. Building the rollout packages is an optional step. When you create rollout packages for Juniper Secure Connect application, you can install the application across the organization. Read the following steps to learn how you, as a system administrator can prepare the Juniper Secure Connect installer for the software rollout.

You can use an installation package for easy rollout of the Juniper Secure Connect application. You must be assigned the privileges of a system administrator to perform the following steps:

1. Install the Juniper Secure Connect application manually on one device. After the installation is complete, initiate a connection to the profiles to be saved for the users.

2. Create a folder with name **JuniperSecureConnect** including the sub-directories as shown below (all directory are case-sensitive):

   C:\JuniperSecureConnect

   C:\JuniperSecureConnect\ImportDir\cacerts

   C:\JuniperSecureConnect\ImportDir\certs

   C:\JuniperSecureConnect\ImportDir\config

   C:\JuniperSecureConnect\ImportDir\Data

3. Copy the **ncpphone.cfg** file from **C:\ProgramData\Juniper\SecureConnect\Data** folder to the following folder:

   C:\JuniperSecureConnect\ImportDir\Data

4. Copy your CA certificates to the following folder:

   C:\JuniperSecureConnect\ImportDir\cacerts

5. Copy the **Name_of_juniper_secure_connect_filename.exe** to the following folder:

   C:\JuniperSecureConnect

6. Open the command prompt using **cmd** command and navigate to **C:\JuniperSecureConnect** folder path and execute the following command:

   ```
   Name_of_juniper_secure_connect_filename.exe /s /b"C:\JuniperSecureConnect" /v"/qn
   EXTRACT_MSI_ONLY=1"
   ```

7. (Optional) To add a custom branding option, follow these steps:

   - Create an **.ini** file named **cbo.ini** that contains the following information:

     ```
     [GENERAL]
     Picture=C:\ProgramData\Juniper\SecureConnect\config\cbo.bmp
     HtmlLocal=C:\ProgramData\Juniper\SecureConnect\config\cbo.html
     ```

- Create a logo in **.bmp** file format and with **cbo.bmp** filename. The width of the image must be 328 pixels only. You can adjust the height of the image from 24 pixels and above.

- You can optionally create an HTML file with **cbo.html** as a filename that will open if the user clicks the logo in the application.

- Now copy these three files (**cbo.ini**, **cbo.bmp**, and **cbo.html**) into the following folder:

  C:\JuniperSecureConnect\ImportDir\config

8. Skip this step, if you are using preshared key (PSK) authentication method.

   For EAP-TLS authentication, you must save the user certificates only with name **user.p12** in below directory.

   C:\JuniperSecureConnect\ImportDir\certs

   Ensure that user certificate is unique for each installation package.

9. You can optionally start the installation using the **.exe** or the **.msi** installer. Based on your choice you can also remove one of the installers (**.exe** or **.msi**) from the folder if you want to reduce the amount of data distributed:

   C:\JuniperSecureConnect\

   - **exe** installer prompts for an interactive installation

   - **msi** installer can be silent. Following are your options for the **msi** installer:

     Table 27: msi Installer Options

Function/Parameters	Description
`msiexec.exe /I`	Install the application
`msiexec.exe /uninstall`	Uninstall the application
`xxx.msi`	MSI installer package
`/qn`	Silent installation
`ProductLanguage=1033`	English

Table 27: msi Installer Options *(Continued)*

Function/Parameters	Description
NCP_CREATE_DESKTOPICON=1	0=No shortcut on desktop, 1=Shortcut on desktop
/log path	Path for installation log
/forcerestart	Forces a reboot of the system automatically without any user notification
/norestart	Prevents a reboot from happening, a reboot is mandatory to use the application
/promptrestart	Users will be prompted to reboot their device, a reboot is mandatory to use the application

Following is the example syntax to install the client silently with a forced reboot and save a shortcut to the application on the desktop:

```
msiexec.exe /I Juniper_Secure_Connect_Windows_x86-64.msi ProductLanguage=1033
NCP_CREATE_DESKTOPICON=1 /qn /log c:\RemoteAccess\installlog.log /forcerestart
```

Juniper Secure Connect GUI Elements

SUMMARY

Juniper Secure Connect GUI elements provides a quick display of additional information about your remote access connection.

IN THIS SECTION

The Juniper Secure Connect window provides a quick view of:

- Connection profile
- SRX Series Firewalls gateway address

- Connection status
- Connection statistics

Table 28 on page 275 provides the details of Juniper Secure Connect GUI elements.

Table 28: GUI Elements in Juniper Secure Connect display window

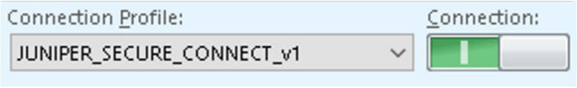
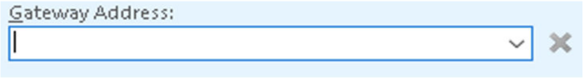
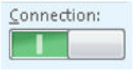
Element	Description
Connection Profile dropdown list  Connection Profile: JUNIPER_SECURE_CONNECT_v1 	Location—Below the menu bar. Click the dropdown list to view the currently added connection profile. You can access a different SRX Series Firewalls, by choosing **New Connection** in the connection profiles to download a new configuration.
Gateway Address dropdown list  Gateway Address:	Location—Below the **Connection Profile** dropdown list. Enter the SRX Series Firewall URL for a new connection. You must enter the URL provided by your administrator for **Gateway Address** field. For example, let's consider an URL https://12.12.12.12 that does not include the realm name. Another example https://12.12.12.12/engineering, where engineering refers to realm name. If your administrator provides you the URL with realm name, it must be entered as it is.
Connection Button  	Location—Next to **Connection Profile** dropdown list. Click this button to connect or disconnect a VPN connection.

Table 28: GUI Elements in Juniper Secure Connect display window *(Continued)*

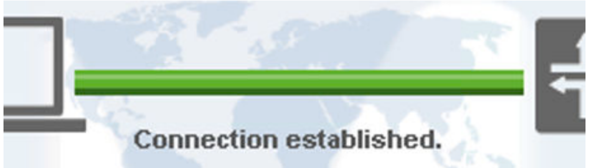
Element	Description
Connection status bar  Connection established.	Location—Center of Juniper Secure Connect window. The color of the connection bar changes from yellow to green during connection. These colors represents: • Thin yellow bar: Juniper Secure Connect is trying to contact the VPN gateway and establish phase 1 of the VPN session. • Thick yellow bar: Juniper Secure Connect has established phase 1 of the VPN session and is establishing phase 2. • Green bar: Juniper Secure Connect has established the VPN connection. • Broken green bar: Juniper Secure Connect has lost Internet connection and will try to reconnect the VPN connection as soon as internet is available.
PIN Icon PIN	Location—Below the connection status bar. • If the PIN icon is gray, the PIN has not been entered to access the user certificate or the user certificate can not be found. • If the PIN icon is green, the PIN for the user certificate has been entered, and Juniper Secure Connect is able to use the user certificate.
World Icon 🌐	Location—Below the connection status bar. • If the world icon is gray, the Juniper Secure Connect is not trying to connect. • If the world icon is blue, the Juniper Secure Connect is trying to connect the VPN gateway. • If the world icon is green, the Juniper Secure Connect was able to communicate with the VPN gateway.

Table 28: GUI Elements in Juniper Secure Connect display window *(Continued)*

Element	Description
Person or checkmark Icon	Location—Below the connection status bar. - If the person icon is gray, the Juniper Secure Connect is not trying to connect. - If the person icon is blue, the Juniper Secure Connect is trying to authenticate the user. - If the person icon is green, the Juniper Secure Connect was able to authenticate the user.
Key Icon	Location—Below the connection status bar. - If the key icon is gray, the Juniper Secure Connect is not trying to connect. - If the key icon is blue, the Juniper Secure Connect is trying to establish the VPN session (phase2). - If the key icon is green, the Juniper Secure Connect application was able to establish phase 2 and the complete VPN session.
Arrow or U-Turn Icon	Location—Below the connection status bar. If the Arrow or U-Turn icon is green, the Juniper Secure Connect has detected an issue with the IPsec connection and has automatically switched over to SSL VPN.

Table 28: GUI Elements in Juniper Secure Connect display window *(Continued)*

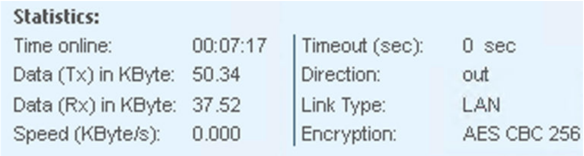
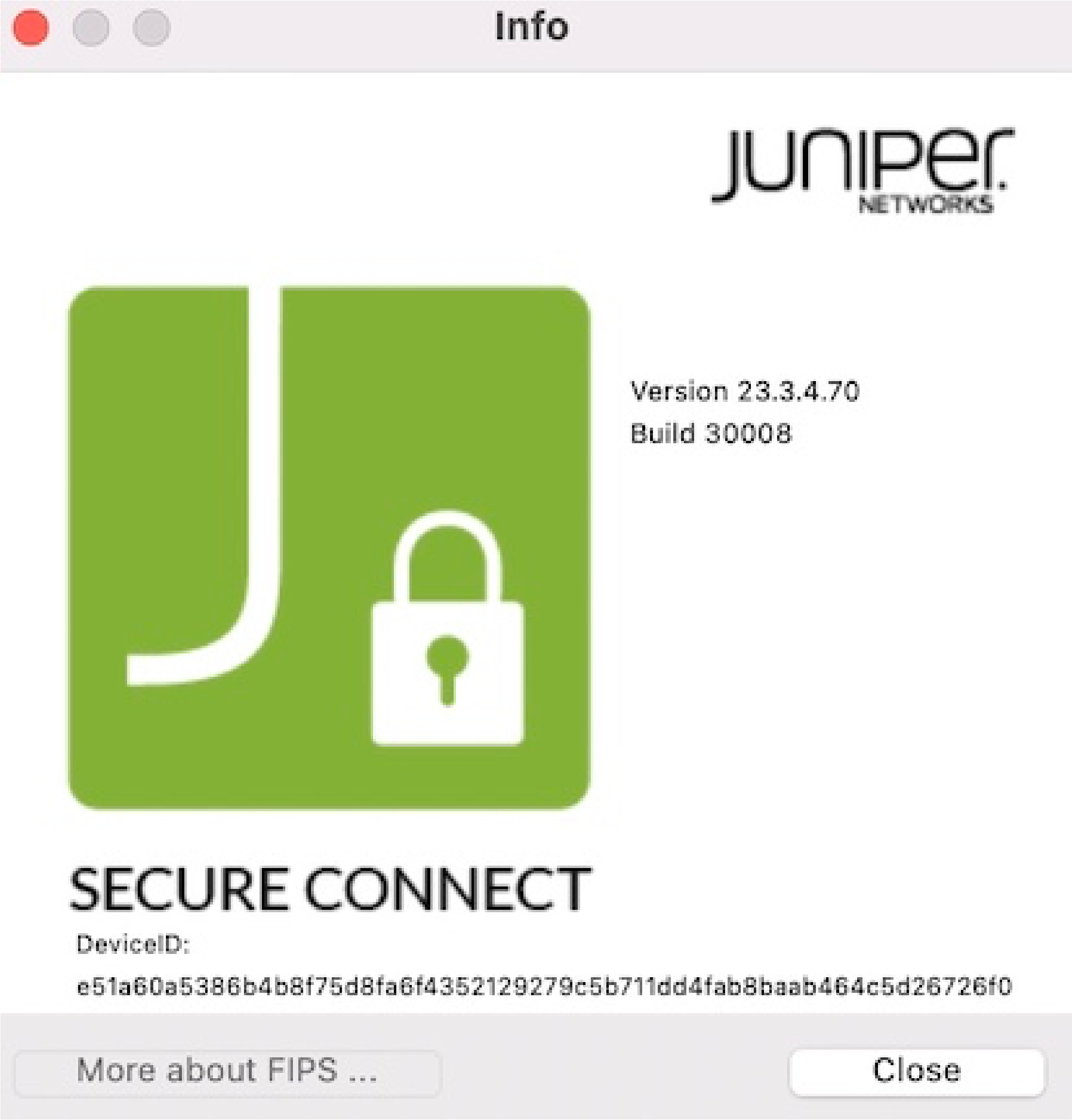
Element	Description
Connection Statistics  Statistics: Time online: 00:07:17 Data (Tx) in KByte: 50.34 Data (Rx) in KByte: 37.52 Speed (KByte/s): 0.000 Timeout (sec): 0 sec Direction: out Link Type: LAN Encryption: AES CBC 256	Location—Bottom of the Juniper Secure Connect window. Juniper Secure Connect window displays the following connection statistics: • **Time online**—Shows the time a user has been connected with the same connection profile. Restarting the Juniper Secure Connect or changing the connection profile resets this value. • **Data (Tx) in Byte**—Shows the data sent or transmitted over the VPN tunnel into the remote network while being connected to the same connection profile. Restarting the Juniper Secure Connect or changing the connection profile resets this value. • **Data (Rx) in Byte**—Shows the data received over the VPN tunnel into the remote network while being connected to the same connection profile. Restarting the Juniper Secure Connect or changing the connection profile resets this value. • **Speed**—Shows the average speed calculated using the connection time, Data (Tx), and Data (Rx). Restarting the Juniper Secure Connect or changing the connection profile resets this value. • **Timeout**—This value shows `0 sec`, if no timeout for the VPN session is used. If a timeout is used, the timeout shows the amount of seconds. The Juniper Secure Connect starts count down for the timeout as soon as no data is received over the VPN tunnel and resets as soon as data is received of the VPN tunnel. • **Direction**—The Juniper Secure Connect can only establish outgoing connection. The value will show “out”.

Table 28: GUI Elements in Juniper Secure Connect display window *(Continued)*

Element	Description
	• **Link Type**—The Juniper Secure Connect shows “LAN”. This means the Juniper Secure Connect does not act as a internet dialer, but only establishes the VPN connection. • **Encryption**—This value shows the encryption used in phase 2.

The Juniper Secure Connect displays Device ID information from May 2023 application release. To know about the Device ID information, navigate to **About Juniper Secure Connect**.

Figure 120: Displays Juniper Secure Connect Device ID Information



Version 23.3.4.70
Build 30008

DeviceID:
e51a60a5386b4b8f75d8fa6f4352129279c5b711dd4fab8baab464c5d26726f0

WHAT'S NEXT

For more information on Juniper Secure Connect features and how to configure the options on Windows, see "Connection Menu" | 281, "View Menu" | 295, and "Help Menu" | 304.
For more information on Juniper Secure Connect features and how to configure the options on macOS, see "Connection Menu" | 347, "View Menu" | 354, "Log Menu" | 357, and "Help Menu" | 359.

Connection Menu

SUMMARY

Juniper Secure Connect **Connection** menu provides you the options to establish remote access connection and secure the connection with certificates. Use the **Connection** menu for connection related options to view the certificates, enter PIN, reset PIN, or change PIN.

IN THIS SECTION

WHAT'S NEXT

For more information on Juniper Secure Connect GUI elements, see "Juniper Secure Connect GUI Elements" | 274.
For more information on Juniper Secure Connect features and how to configure the options, see "View Menu" | 295 and "Help Menu" | 304.

Connect Menu Option

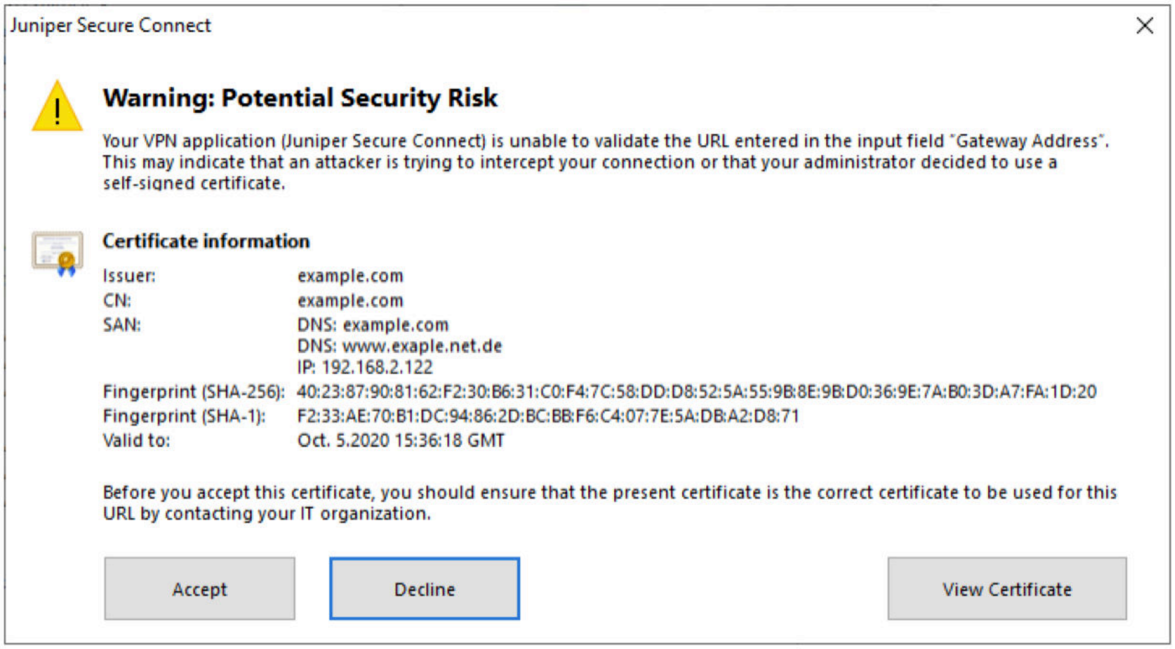
Following are the steps to establish a connection:

1. You must first define and select a profile to establish a connection for that profile. Click on the **Connection Profile** dropdown list and select a profile for which you want to establish a connection.
2. 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 as shown in Figure 122 on page 283.

⚠ **WARNING**: If the following the warning message is displayed, your application is missing the CA certificate from the VPN gateway (SRX Series Firewall). If you are a remote user, contact your IT organization for appropriate action. If you are a system administrator, place the cacerts in the respective location for the platform.

Figure 121 on page 282 is a sample warning message on Windows platform that is displayed when CA certificate is not present.

Figure 121: Sample Certificate Warning Message on Windows Platform



Juniper Secure Connect

Warning: Potential Security Risk

Your VPN application (Juniper Secure Connect) is unable to validate the URL entered in the input field "Gateway Address". This may indicate that an attacker is trying to intercept your connection or that your administrator decided to use a self-signed certificate.

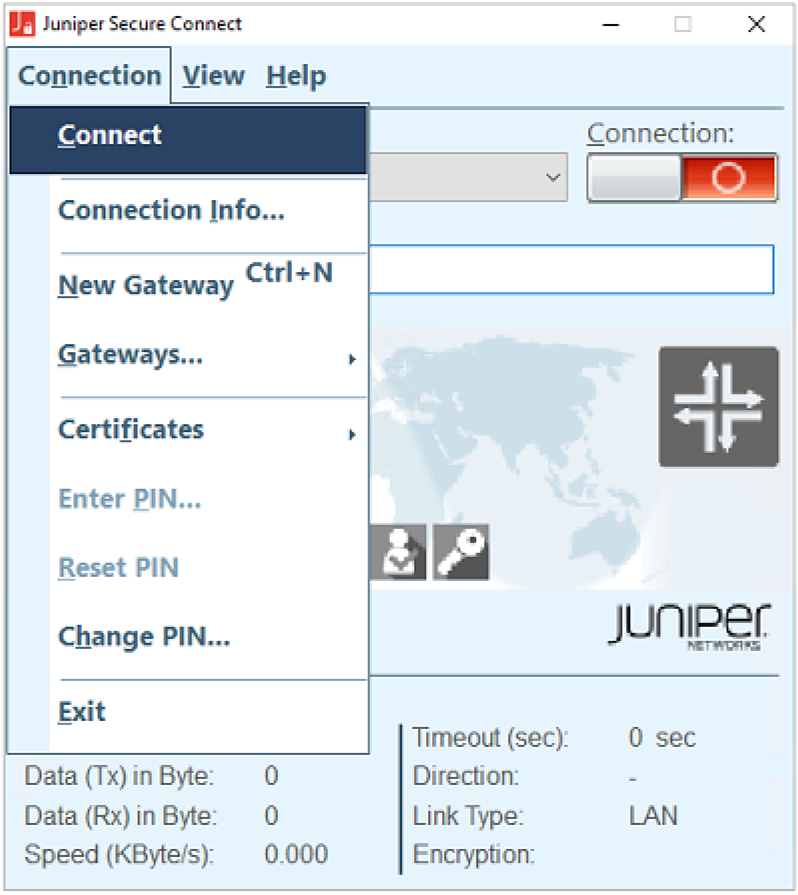
Certificate information

Issuer:	example.com
CN:	example.com
SAN:	DNS: example.com DNS: www.exaple.net.de IP: 192.168.2.122
Fingerprint (SHA-256):	40:23:87:90:81:62:F2:30:B6:31:C0:F4:7C:58:DD:D8:52:5A:55:9B:8E:9B:D0:36:9E:7A:B0:3D:A7:FA:1D:20
Fingerprint (SHA-1):	F2:33:AE:70:B1:DC:94:86:2D:BC:BB:F6:C4:07:7E:5A:DB:A2:D8:71
Valid to:	Oct. 5.2020 15:36:18 GMT

Before you accept this certificate, you should ensure that the present certificate is the correct certificate to be used for this URL by contacting your IT organization.

3. To disconnect the existing connection, go to **Connection > Disconnect**, or use the **Connection** toggle button.

Figure 122: Connect Menu Option



Data (Tx) in Byte: 0
Data (Rx) in Byte: 0
Speed (KByte/s): 0.000

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

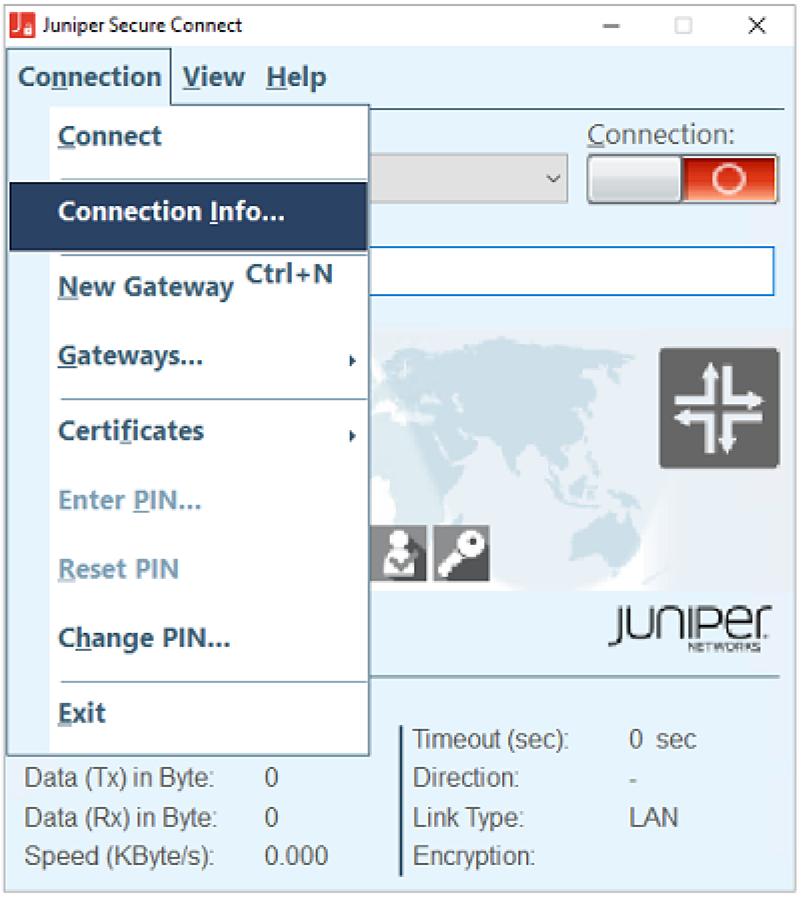
Connection Info Menu Option

In the menu bar, navigate to **Connect** > **Connection Info** to get the following information on your connection as shown in Figure 123 on page 284:

- Name of the currently selected profile
- Statistics information (for example, time online and value of timeout)
- IP addresses (VPN IP address, DNS server, VPN Endpoint)
- Security mode
- Security keys used
- Quality of Service provides the following information:

- QoS groups available for the currently selected profile. You can switch on or off the QoS groups.
- Graphical representation of the bandwidth used.

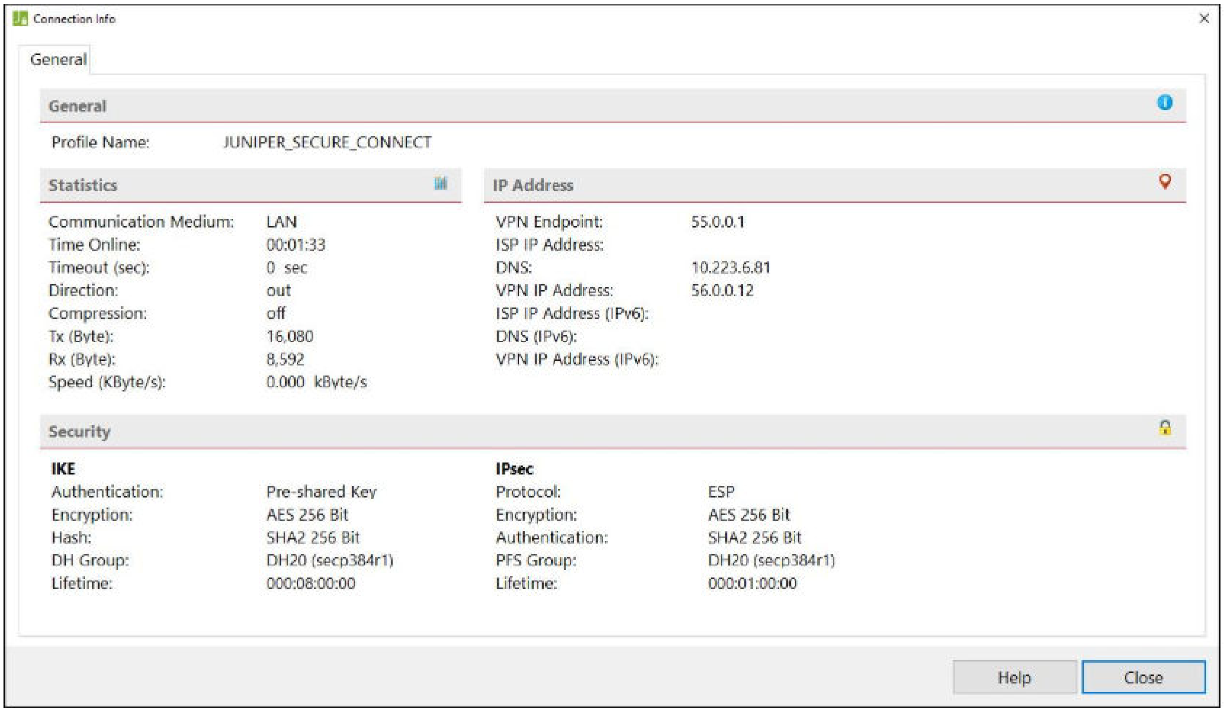
Figure 123: Connect Info Menu Option



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

Figure 124 on page 285 shows an example of connection information for a VPN connection.

Figure 124: Connection Information



General

Profile Name: JUNIPER_SECURE_CONNECT

Statistics

Communication Medium:	LAN
Time Online:	00:01:33
Timeout (sec):	0 sec
Direction:	out
Compression:	off
Tx (Byte):	16,080
Rx (Byte):	8,592
Speed (KByte/s):	0.000 kByte/s

IP Address

VPN Endpoint:	55.0.0.1
ISP IP Address:	
DNS:	10.223.6.81
VPN IP Address:	56.0.0.12
ISP IP Address (IPv6):	
DNS (IPv6):	
VPN IP Address (IPv6):	

Security

IKE		IPsec	
Authentication:	Pre-shared Key	Protocol:	ESP
Encryption:	AES 256 Bit	Encryption:	AES 256 Bit
Hash:	SHA2 256 Bit	Authentication:	SHA2 256 Bit
DH Group:	DH20 (secp384r1)	PFS Group:	DH20 (secp384r1)
Lifetime:	000:08:00:00	Lifetime:	000:01:00:00

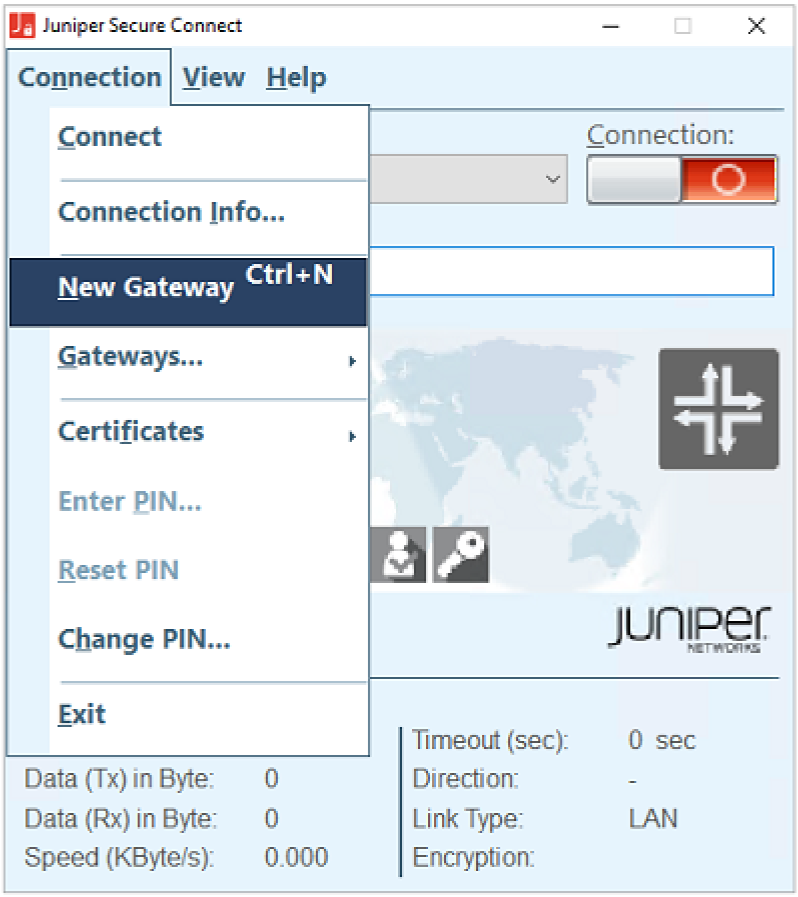
New Gateway Menu Option

When you first launch the Juniper Secure Connect application, you'll be able to view only the **Connection Profile** option.

To connect to a new gateway:

- Navigate to **Connection** > **New Gateway** from the **Connection** menu. See Figure 125 on page 286.
- When you select **New Gateway** option, the **Gateway Address** field appears. Enter the URL for the new gateway address. Alternatively, you can also press **Ctrl+N** to enter the gateway address.
- After entering the gateway address, click on the **Connection** button to establish the connection to the specified SRX gateway address.

Figure 125: New Gateway Menu Option



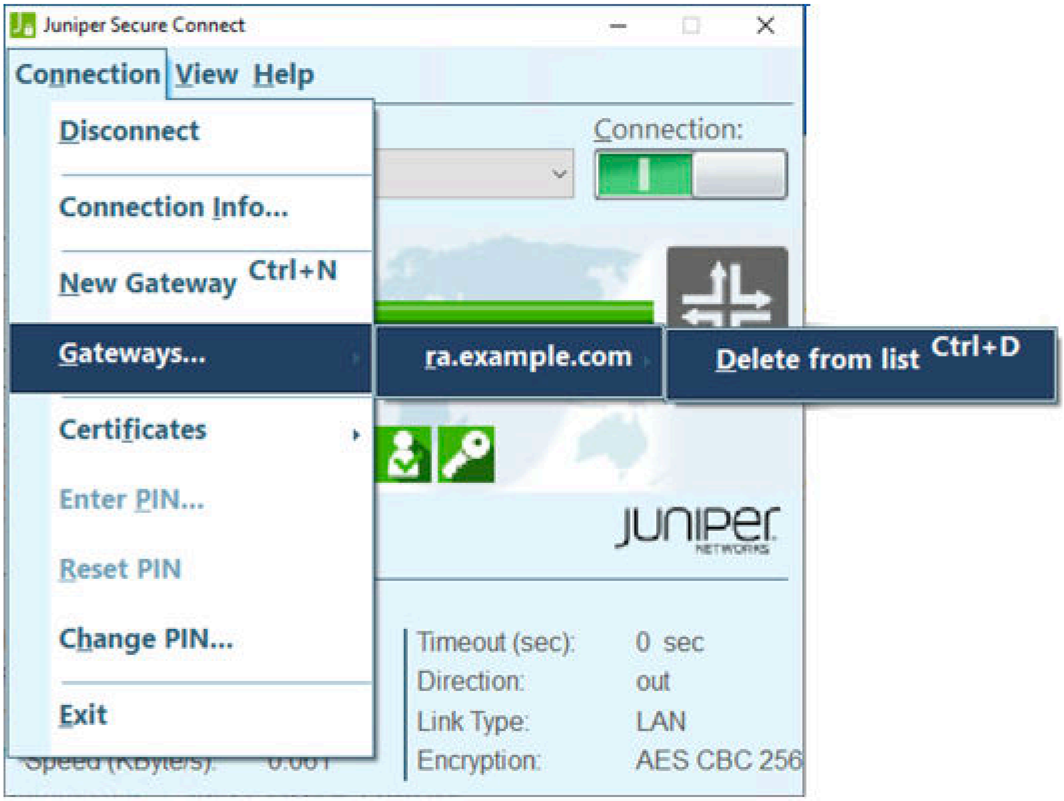
Data (Tx) in Byte: 0
Data (Rx) in Byte: 0
Speed (KByte/s): 0.000
Timeout (sec): 0 sec
Direction: -
Link Type: LAN
Encryption:

Gateways Menu Option

If you wish to remove a gateway address from the gateways list, follow these steps:

- Navigate to **Connection** > **Gateways** from the **Connection** menu. See Figure 126 on page 287.
- Select **Gateways** and the list of gateway address appears.
- Select the gateway address you wish to remove from the list and select **delete from the list**. Alternatively, you can also delete the gateway address from the list by pressing **Ctrl+D**.

Figure 126: Delete Gateways



Certificates Menu Option

Certification Authority (CA) (also referred as the Issuer) creates and issues certificates using a PKI manager (software) and stores as a soft certificate.

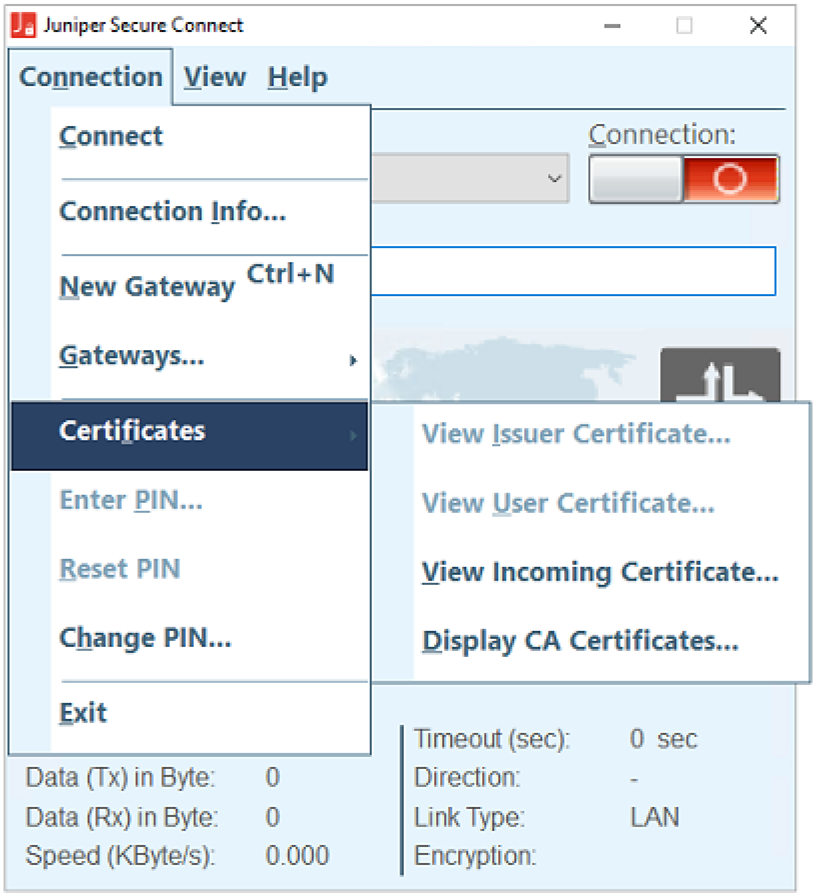
User and CA certificates are stored in the following directory locations:

- User certificates are stored as a **PKCS#12** file under **C:\ProgramData\Juniper\SecureConnect\certs** directory, like **C:\ProgramData\Juniper\SecureConnect\certs\user.p12**.
- CA or issuer certificates are stored under **C:\ProgramData\Juniper\SecureConnect\cacerts**.

Juniper Secure Connect supports ***.pem** and ***.crt** formats for CA certificates.

As shown in Figure 127 on page 288, navigate to **Connection** > **Certificates** to view certificates related menu options.

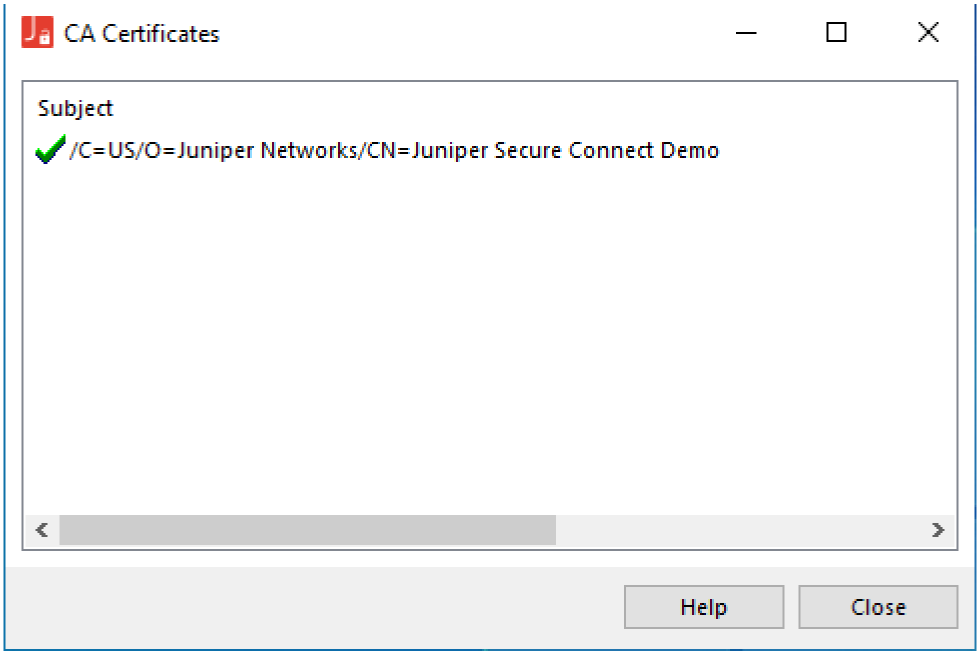
Figure 127: Certificates Menu Option



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

Figure 128 on page 289 shows an example of **CA certificates** window, after selecting **Display CA Certificates** option from the **Certificates** menu.

Figure 128: View CA Certificates



Subject

✓ /C=US/O=Juniper Networks/CN=Juniper Secure Connect Demo

Enter PIN Menu Option

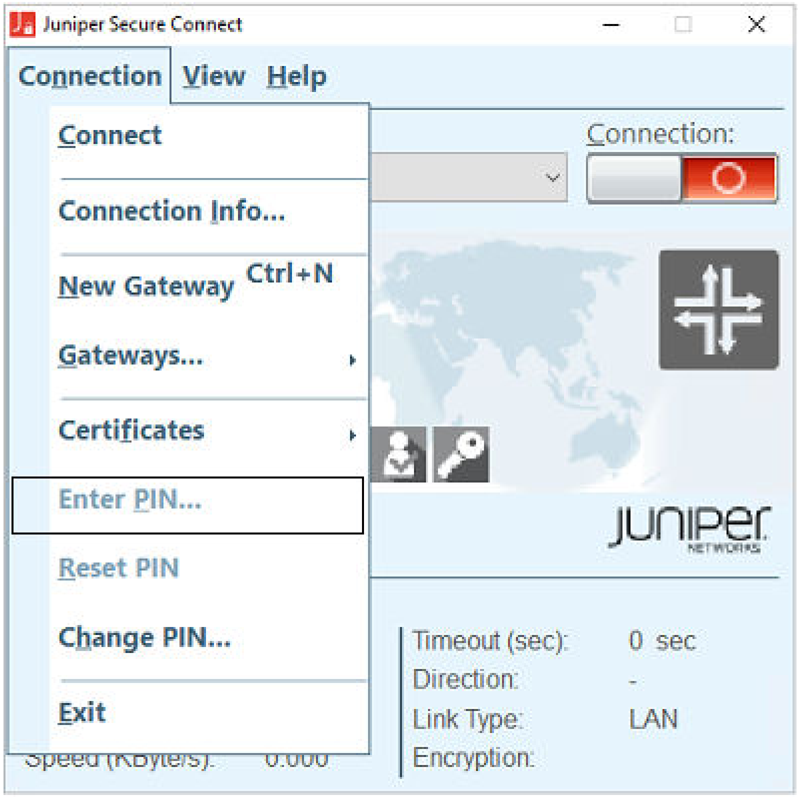
You can enter the PIN after starting the Juniper Secure Connect and before establishing a connection. If you want to establish a connection using a certificate at a later time, then you can skip the PIN entry unless the certificate configuration requires it.

To enter your PIN:

1. Navigate to **Connection> Enter PIN** from the menu. See Figure 129 on page 290.
2. Enter the PIN. PIN must be a minimum of six digits in length.
3. Click **OK**.

You need a PIN to establish the connection with certificates successfully. At the first time of establishing a connection manually, you must enter the PIN. For subsequent manual connections, you can skip entering the PIN again. A correct PIN entry is indicated by a green PIN symbol.

Figure 129: Enter PIN Menu Option



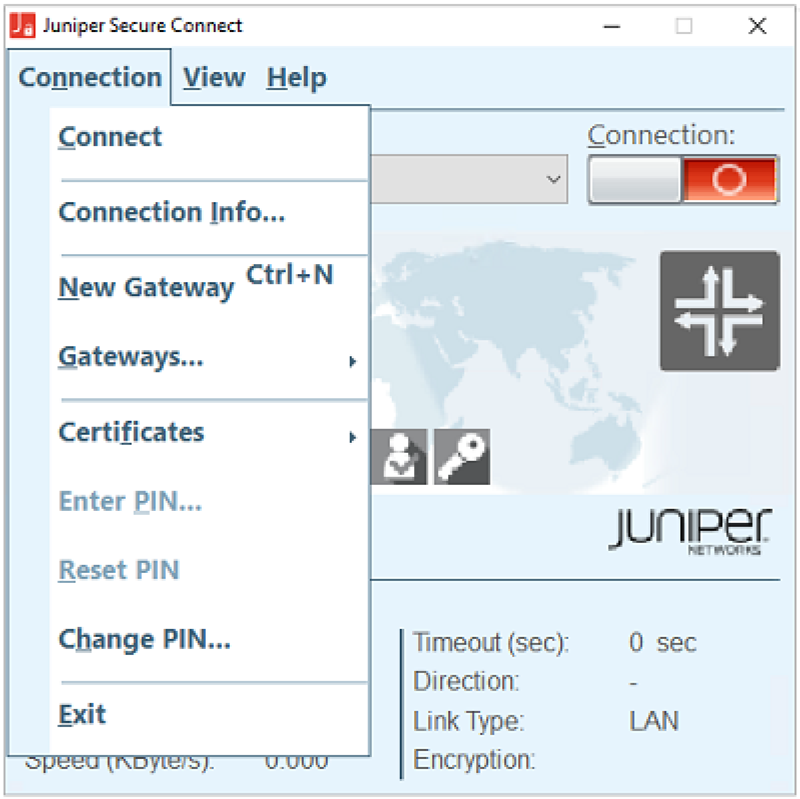
Change PIN Menu Option

In Juniper Secure Connect, if you want to enter the PIN only before establishing the connection, your administrator needs to enable **PIN request at each connection** option for **Certificate Based** Authentication method. Administrator can enable **PIN request at each connection** option to prevent an unauthorized user from setting up an unauthorized connection when the PIN has already been entered. When **PIN request at each connection** option is enabled, whenever you establish a connection, you are prompted to enter the PIN.

If you select **Connection** > **Change PIN**, the PIN that has already been requested in connection with other functions is no longer used, that is, when setting up a connection, or in the **Enter PIN** connection menu. Instead you can always select the **Connection** > **Change PIN** and the new PIN will be automatically reset immediately after the change. This ensures that when configuring **PIN request at each connection** (by your administrator) on an unauthorized Juniper Secure Client, an unauthorized user's PIN cannot be used at anytime to establish a connection.

Figure 130 on page 291 shows the connection menu options.

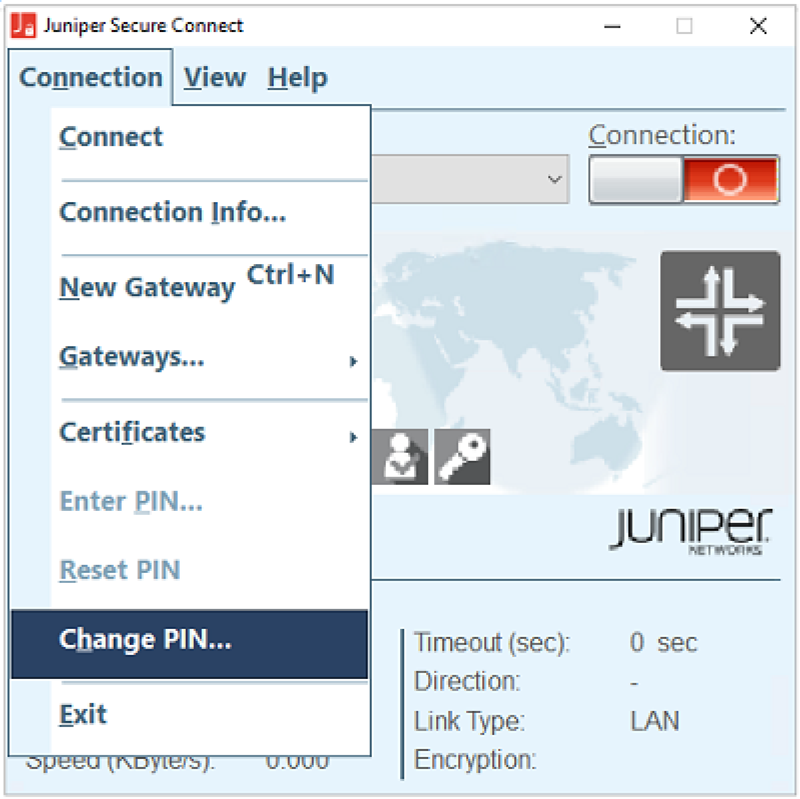
Figure 130: Connection Menu



To change your PIN for a smartcard or token or soft certificate:

1. Navigate to **Connection** > **Change PIN** in the menu bar. See Figure 131 on page 292.
2. Enter the correct PIN number has been entered previously.
3. Enter your new PIN and confirm it by repeating it.
4. Click on **OK**. You have now changed your PIN.

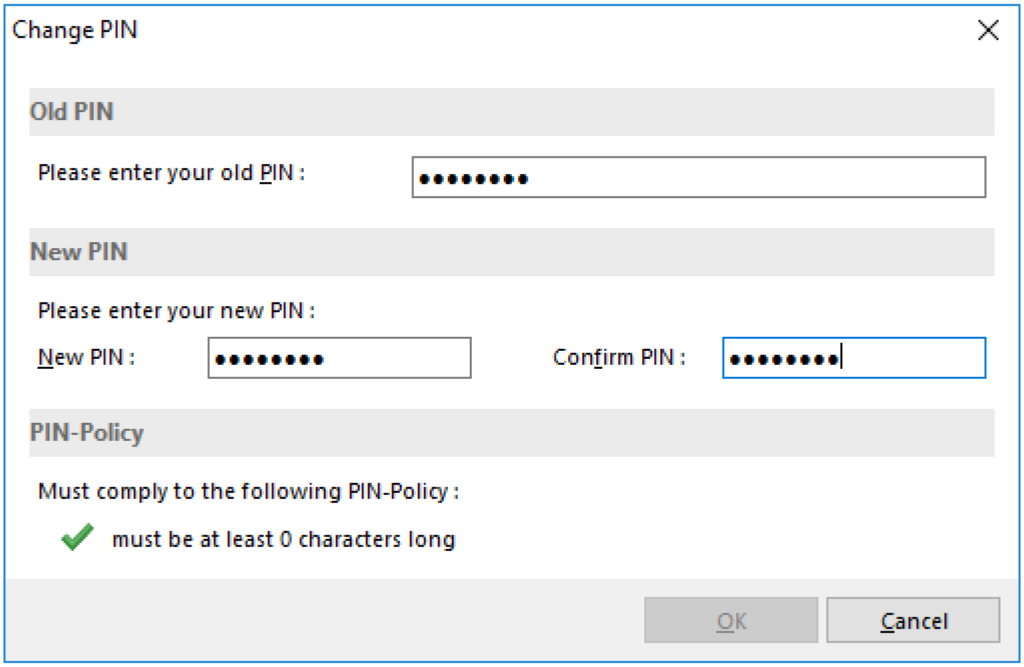
Figure 131: Change PIN Menu Option



Timeout (sec): 0 sec
Direction: -
Link Type: LAN
Encryption:
Speed (KBytes/s): 0.000

Figure 132 on page 293 shows an example **Change PIN** window.

Figure 132: Change To New PIN



Please enter your old PIN : •••••••••

Please enter your new PIN :

New PIN : •••••••••

Confirm PIN : •••••••••

Must comply to the following PIN-Policy :

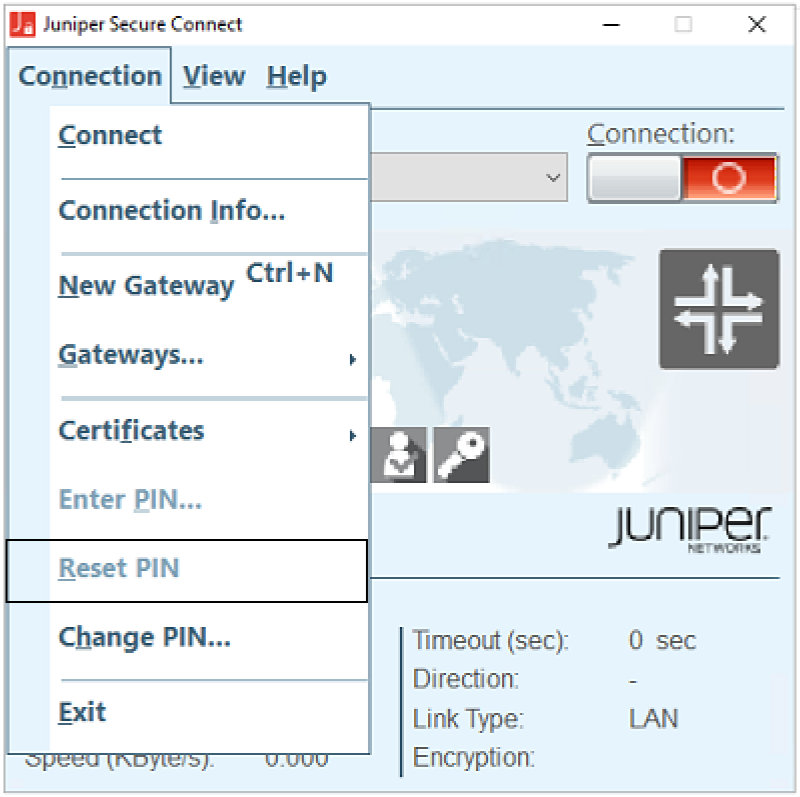
✓ must be at least 0 characters long

Reset PIN Menu Option

To reset your PIN:

1. You can select **Connection** > **Reset PIN** to reset the PIN. See Figure 133 on page 294.
2. You must enter the correct PIN to reset the PIN, because, the certificate is used to establish the connection.
3. If the PIN is reset, you cannot use this certificate to establish a connection, until the correct PIN is entered again.

Figure 133: Reset PIN Menu Option



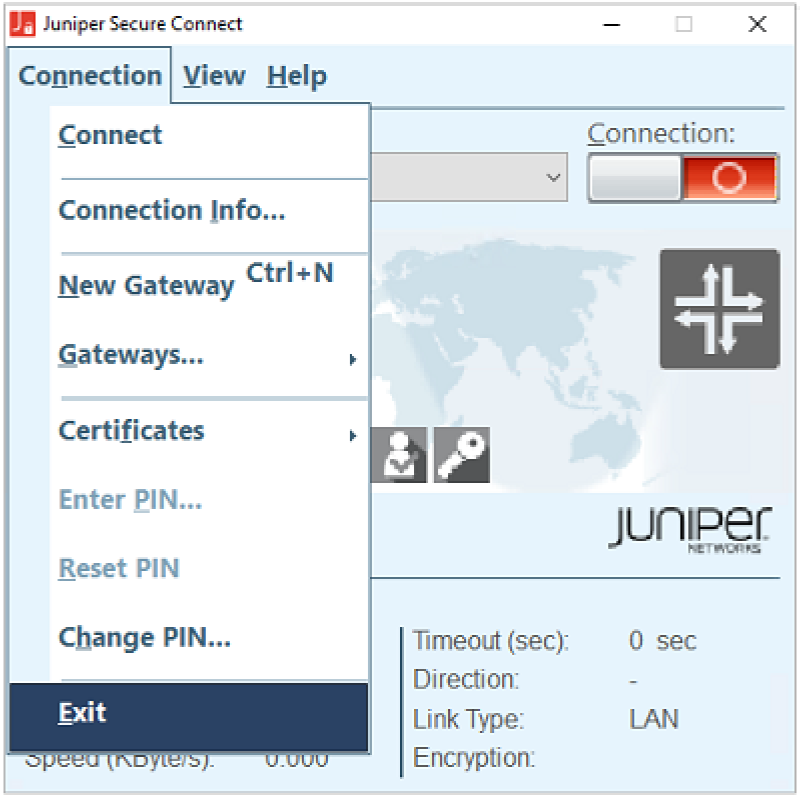
Exit Menu Option

To exit Juniper Secure Connect:

1. If you've already disconnected the VPN connection, navigate to **Connection** > **Exit** in the menu bar as shown in Figure 134 on page 295 or click the close button at the top right corner to exit Juniper Secure Connect.
2. If a connection is currently active, navigate to **Connection** > **Exit** in the menu bar or click the close button at the top right corner to exit Juniper Secure Connect. Note that an existing connection will not be automatically disconnected. You will get a confirmation message whether to close the connection, you must select **Yes** if you want the potentially chargeable connection to remain established even though the monitor is being exited.

   If you select **No**, then your desktop does not display any icon and you won't be notified that the link is active and that charges may be incurred. In such a case, you must restart the Juniper Secure Connect to disconnect the connection properly.

Figure 134: Exit Menu Option



View Menu

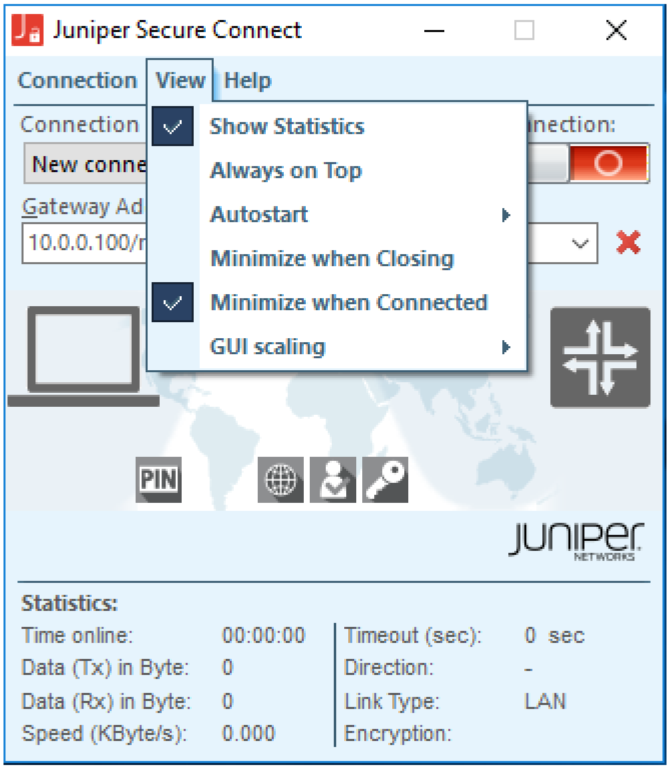
SUMMARY

Juniper Secure Connect **View** menu provides you the options to change the appearance or display of Juniper Secure Connect application.

IN THIS SECTION

You can use the **View** menu options (see Figure 135 on page 296) to show or hide various information and statistics fields.

Figure 135: View Menu

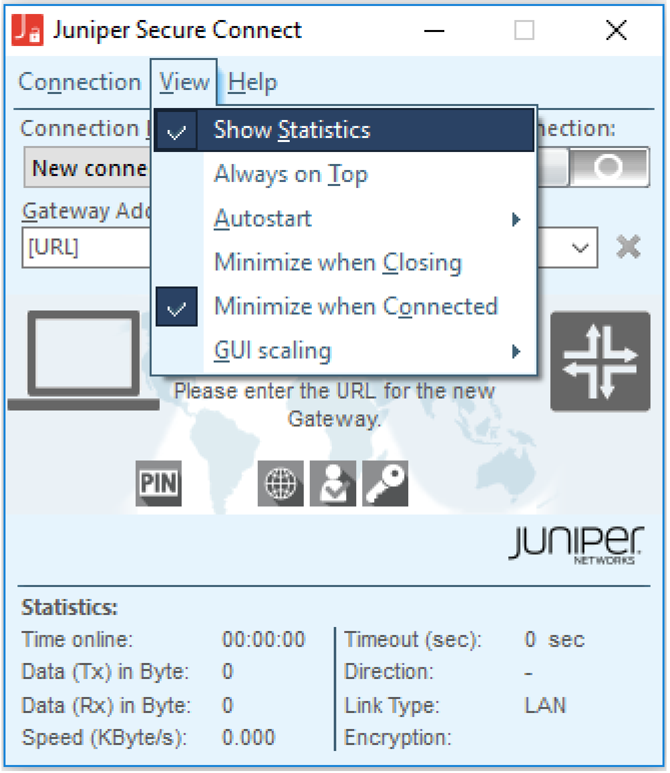


Statistics:

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

- Navigate to **View** > **Show Statistics** as shown in Figure 136 on page 297 to get additional information about the connection, like, time online, transferred data, timeout, and so on. The **Show Statistics** menu option is enabled by default.

Figure 136: Show Statistics Menu Option

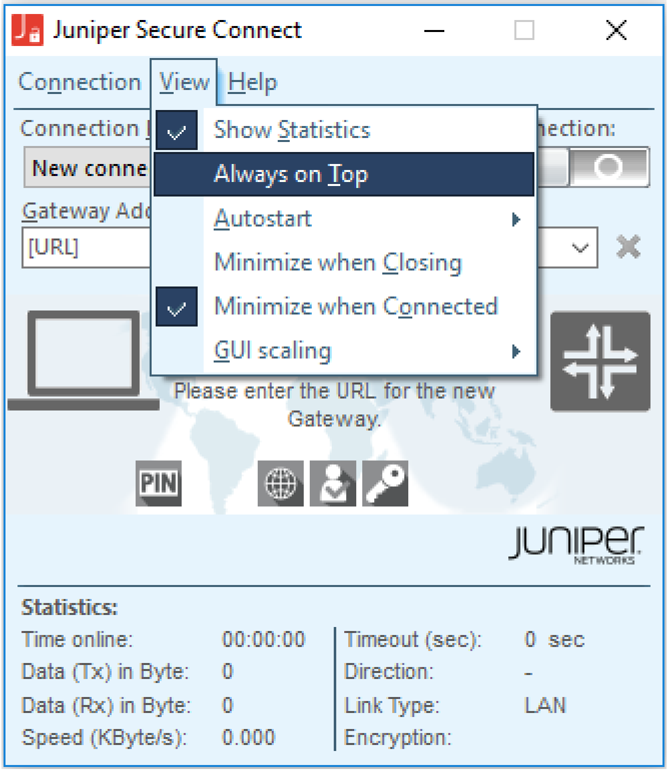


Statistics:

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

- Navigate to **View > Always on Top** as shown in Figure 137 on page 298 to display the Juniper Secure Connect application always in the foreground of your desktop regardless of the currently active application.

Figure 137: Always on Top Menu Option



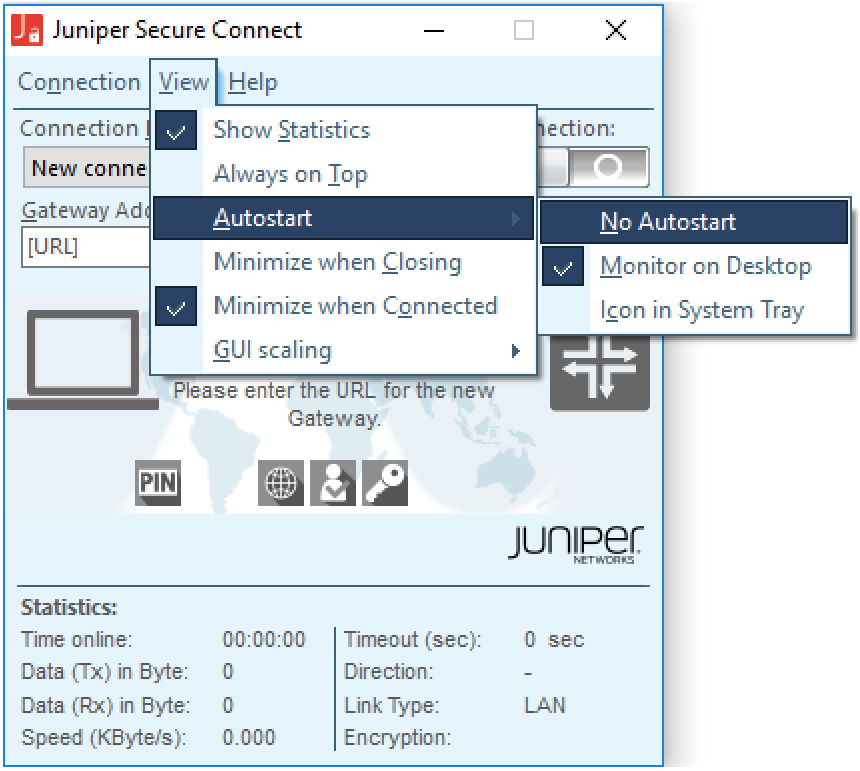
Please enter the URL for the new Gateway.

Statistics:

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

- Navigate to **View** > **Autostart** option. Following are the sub-options you can select:
    - **No Autostart**: If you select this option, after the system boots, you must start the Juniper Secure Connect manually. See Figure 138 on page 299.

Figure 138: No Autostart Menu Option



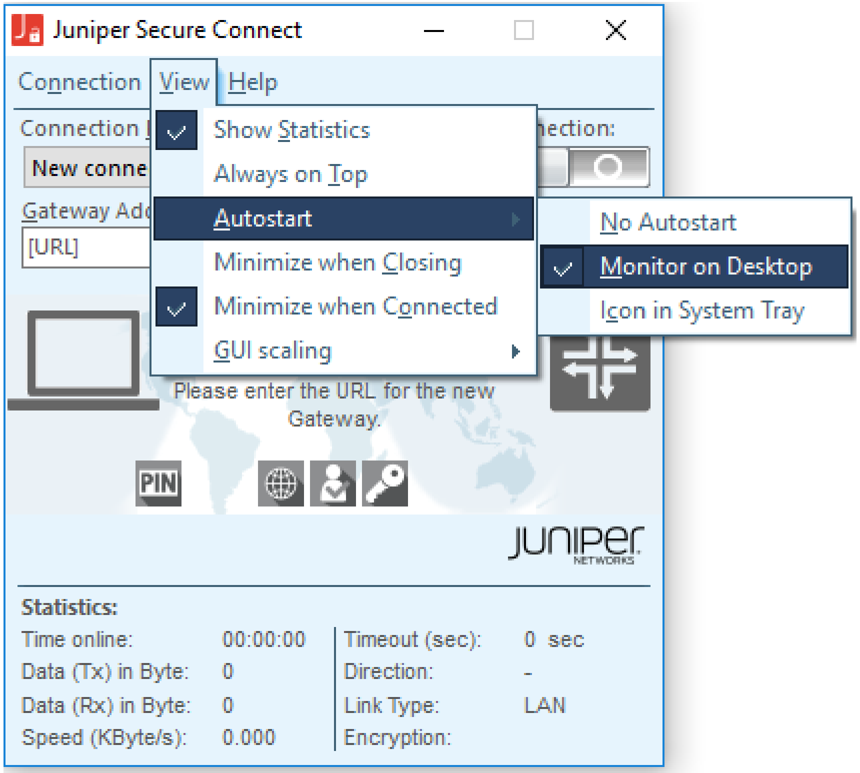
Please enter the URL for the new Gateway.

Statistics:

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

- **Monitor on the Desktop**: If you select this option, after the system boots, the Juniper Secure Connect start and displays in its normal size. See Figure 139 on page 300.

Figure 139: Monitor on Desktop Menu Option



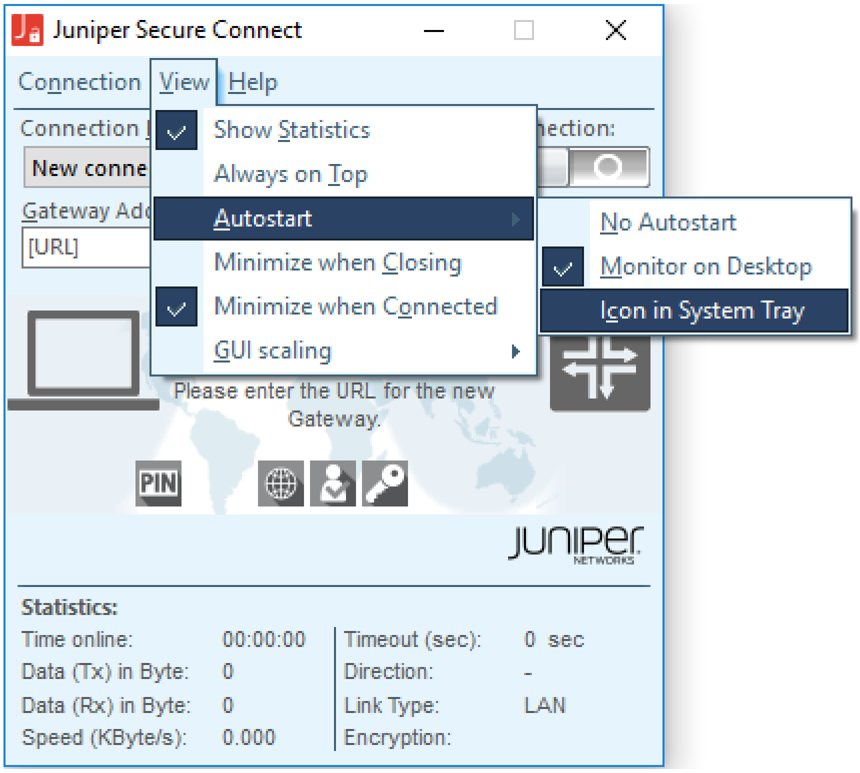
Statistics:

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

- **Icon in System Tray**: If you select this option, after the system boots, the Juniper Secure Connect starts and minimizes as an icon in the system tray.

  If you use Juniper Secure Connect often and need the information displayed, you should select the **Autostart** > **Monitor on Desktop** option as show in Figure 140 on page 301. However, it is not mandatory to start Juniper Secure Connect to communicate with the remote gateway; none of the **Autostart** settings interrupt the establishment of a VPN connection.

Figure 140: Icon in System Tray Menu Option



Statistics:

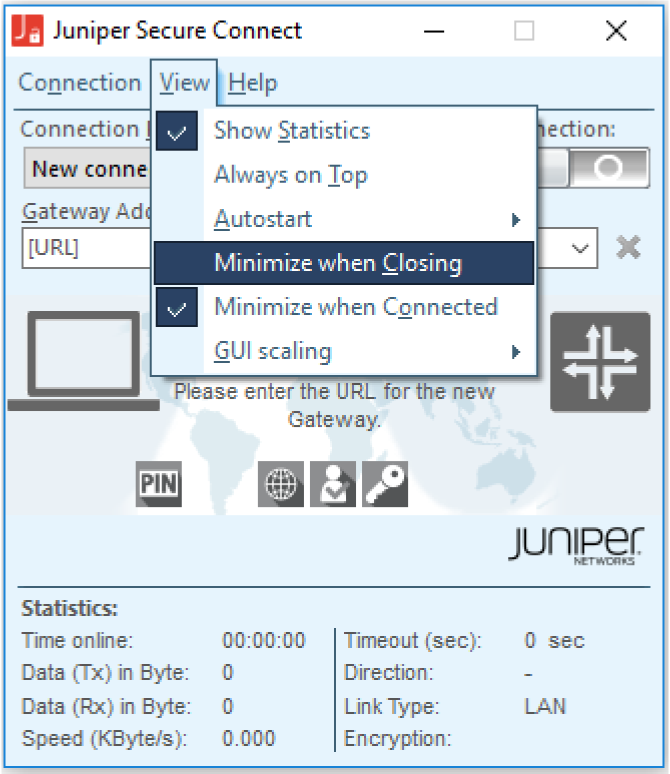
Time online:	00:00:00	Timeout (sec):	0 sec
Data (Tx) in Byte:	0	Direction:	-
Data (Rx) in Byte:	0	Link Type:	LAN
Speed (KByte/s):	0.000	Encryption:	

- You can click the close button at the top-right corner or press Alt+F4 to close the Juniper Secure Connect window.

  If you want to minimize the Juniper Secure Connect window to system tray while closing, navigate to **View** > **Minimize when Closing** option as shown in Figure 141 on page 302. Juniper Secure Connect appears as a VPN icon in the system tray and shows the current state of connection.

  If **Minimize when Closing** option is not enabled, Juniper Secure Connect application window is no longer visible if you close the window. Even if the connection is active, you can no longer view the connection status.

Figure 141: Minimize when Closing Menu Option

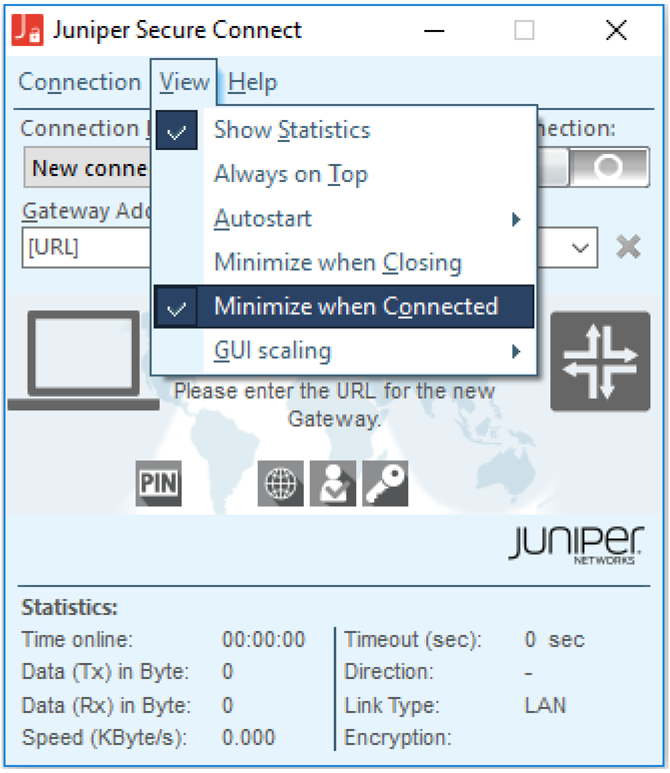


Statistics:

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

- If you want to minimize Juniper Secure Connect window to system tray when you have an active connection, navigate to **View** > **Minimize when Connected** as shown in Figure 142 on page 303, and select **Minimize when Connected** option.

Figure 142: Minimize when Connected Menu Option



Connection |
New conne
Gateway Add
[URL]
nection:

Please enter the URL for the new Gateway.

Statistics:

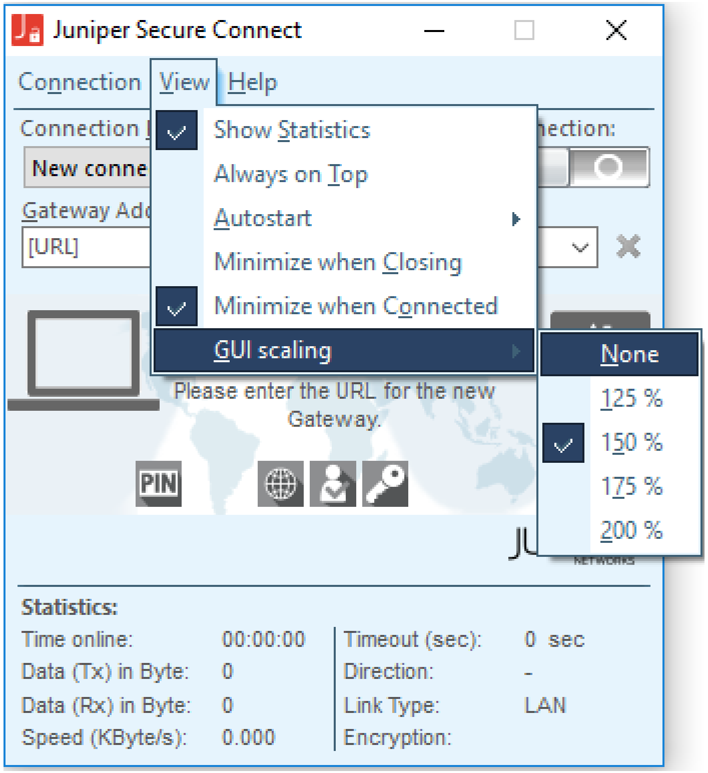
Time online: 00:00:00 | Timeout (sec): 0 sec
Data (Tx) in Byte: 0 | Direction: -
Data (Rx) in Byte: 0 | Link Type: LAN
Speed (KByte/s): 0.000 | Encryption:

- On high definition tablets, you can adjust the size and operate the Juniper Secure Connect on a touch screen. To do this, navigate to **View > GUI scaling** as shown in Figure 143 on page 304. By default, the scaling degree is configured to 150%. Double-click on the logo to adjust the scaling and update the display size to 100, 125, 150, 175, or 200% .

  Press the key combination CTRL+ or CTRL- to change the scaling dynamically. You can only change the size of connection build-up and statistics dialog box. The settings are saved in the **config/ ncpmon.ini** file under the following section:

```
[GENERAL]
Scaled=0
ScaleFactor=150
```

Figure 143: GUI Scaling 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:	LAN
Speed (KByte/s):	0.000	Encryption:	

WHAT'S NEXT

For more information on Juniper Secure Connect GUI elements, see "Juniper Secure Connect GUI Elements" | 274.
For more information on Juniper Secure Connect features and how to configure the options, see "Connection Menu" | 281 and "Help Menu" | 304.

Help Menu

SUMMARY

Juniper Secure Connect **Help** menu provides you the log related options and configuration tips to use the Juniper Secure Connect effectively.

IN THIS SECTION

WHAT'S NEXT

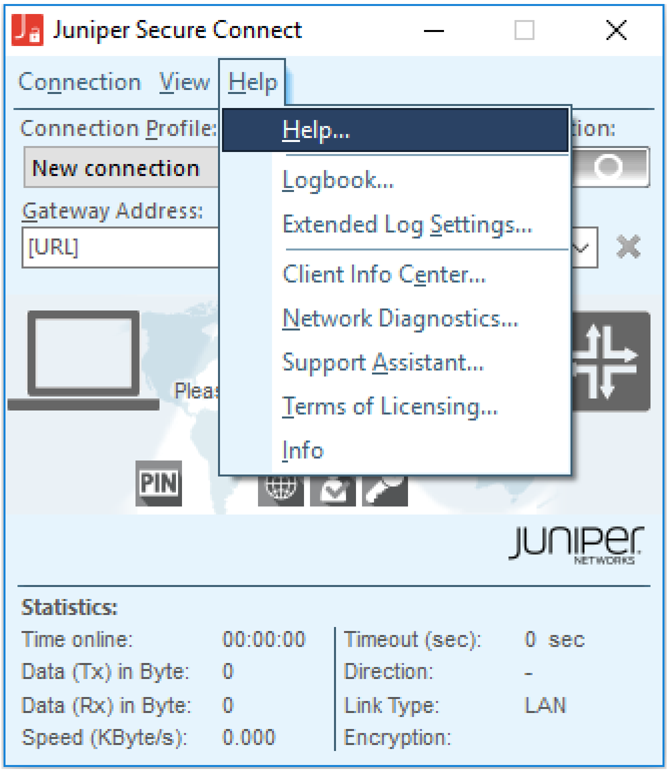
For more information on Juniper Secure Connect GUI elements, see "Juniper Secure Connect GUI Elements" | 274.

For more information on Juniper Secure Connect features and how to configure the options, see "Connection Menu" | 281 and "View Menu" | 295.

Help Menu Option

The **Help** menu displays all available information on the Juniper Secure Connect, regarding the help file, including the product description. See Figure 144 on page 306.

Figure 144: Help 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:	LAN
Speed (KByte/s):	0.000	Encryption:	

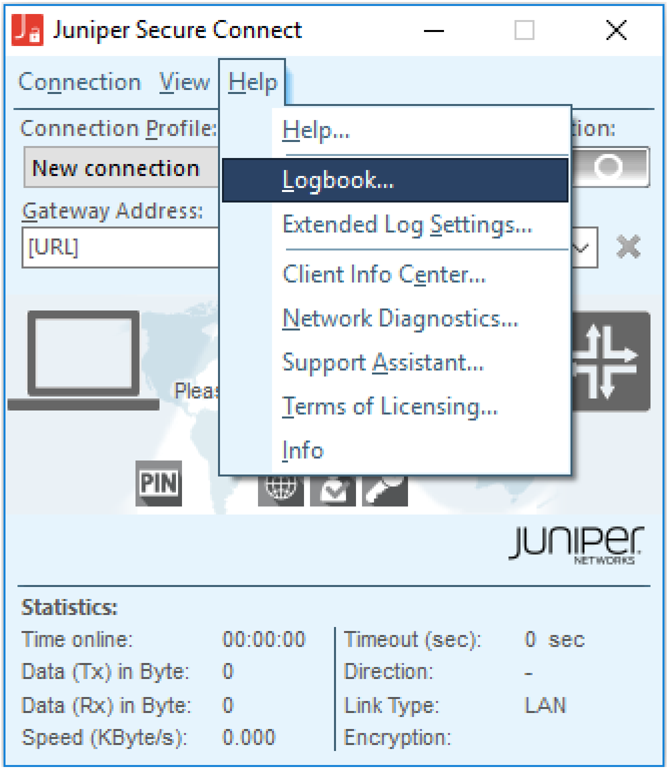
Logbook Menu Option

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 **log** folder when the communication process is completed. The log file is named in **ncpyymmdd.log** format, where yy=year, mm=month, dd=date. You can change the storage time for log files in **Extended Log Settings** option. You can open and analyze the log files using a text editor.

Open the **Log** windows to view and follow the current log messages. In the log window, you can manually save or search for specific events.

Figure 145 on page 307 shows the **Help** menu options with **Logbook** option selected.

Figure 145: Logbook Menu Option

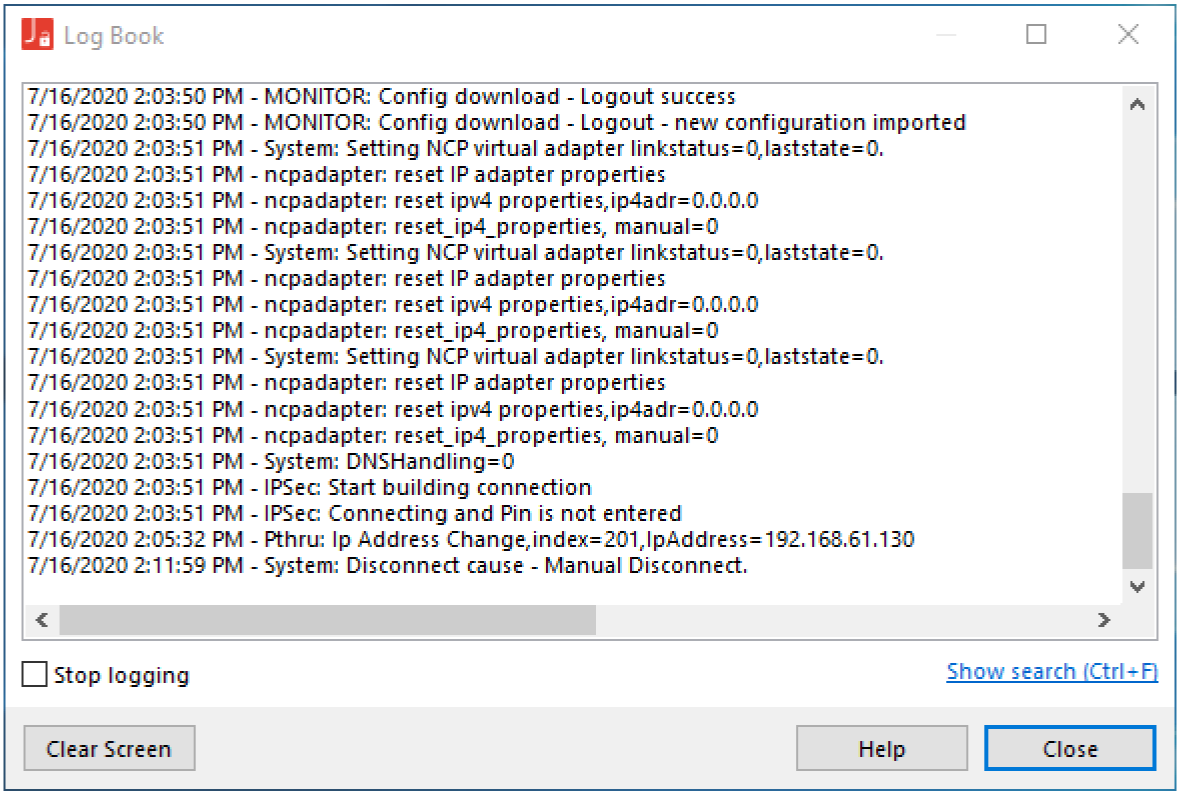


Statistics:

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

Figure 146 on page 308 shows an example of log messages for a VPN connection when **Logbook** option is selected from the **Help** menu.

Figure 146: Displays Log Messages



```
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.
```

Table 29 on page 308 lists options in the **Logbook** window.

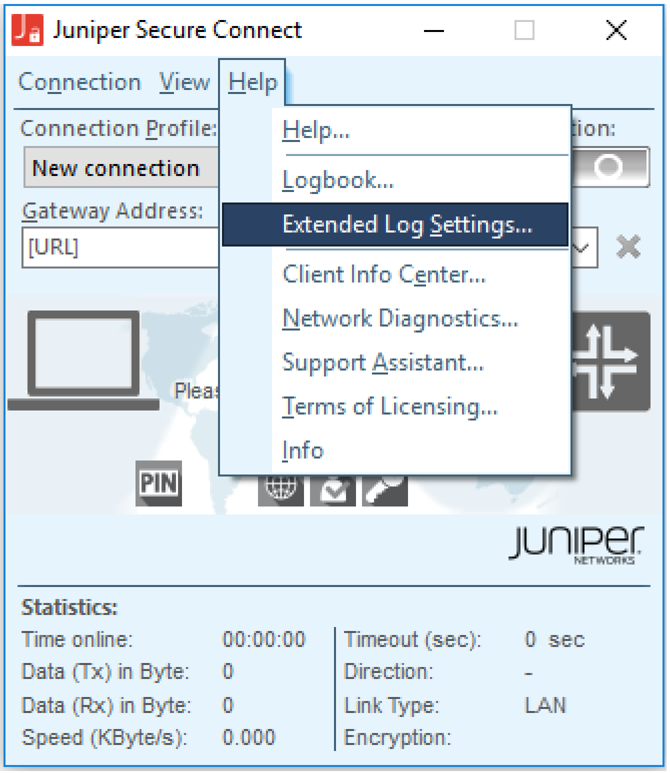
Table 29: Logbook Options and Description

LogBook Option	Action
Close	Closes the **Logbook** window and saves the log entries in to a file. When you close the **Logbook** window, the log information is captured continuously and you can view the latest logs when you open the log file from the **Log** folder.
Clear Screen	Clears the log entries in the log window.
Show Search	Searches for strings and expressions in the log text.

Extended Log Settings Menu Option

In the **Extended Log Settings** window, you can enable the additional log settings. See Figure 147 on page 309.

Figure 147: Extended Log Settings Menu Option



Juniper Secure Connect

Connection Profile:

New connection

Gateway Address:

[URL]

Statistics:

Time online: 00:00:00

Data (Tx) in Byte: 0

Data (Rx) in Byte: 0

Speed (KByte/s): 0.000

Timeout (sec): 0 sec

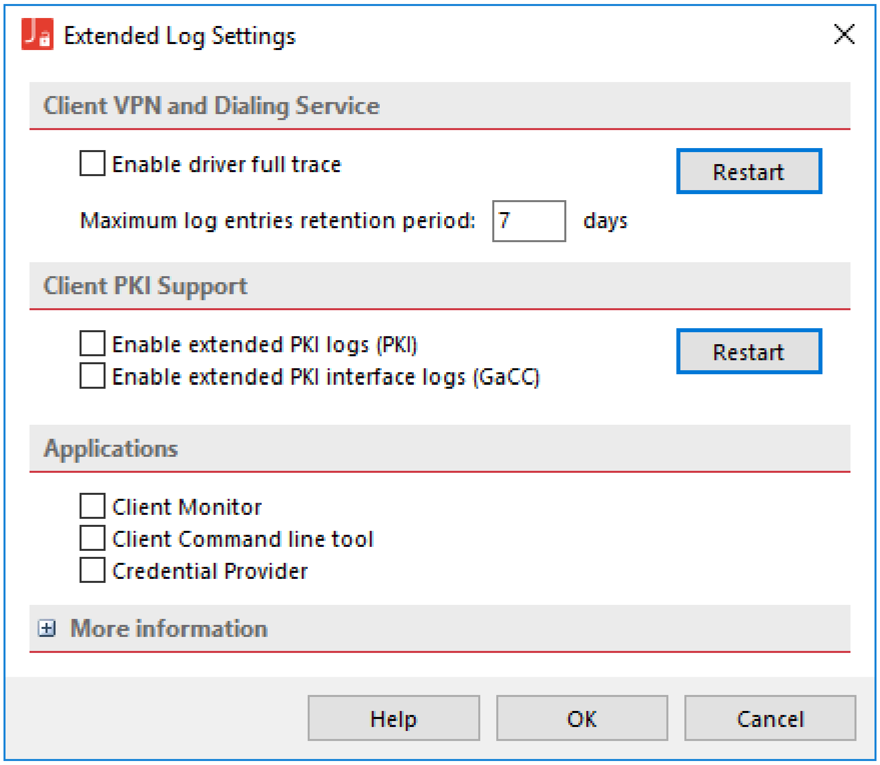
Direction: -

Link Type: LAN

Encryption:

Figure 148 on page 310 shows an example of the **Extended Log Settings** window.

Figure 148: 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

You can collect additional log details for the following client PKI support functions:

- PKI logs (PKI)
- PKI interface logs (GaCC)

You can view the log information for PKI modules (or application) only if they are enabled at:

- Client Monitor
- Client Command line tool
- Credential Provider

You can enable also log settings for the modulated applications, such as client monitor, RWSCMD, and credential providers. If you enable the **Extended Log Settings** options, a flashing message appears in the Juniper Secure Connect window. Double-click on the flashing text to open the **Extended Log Settings** screen.

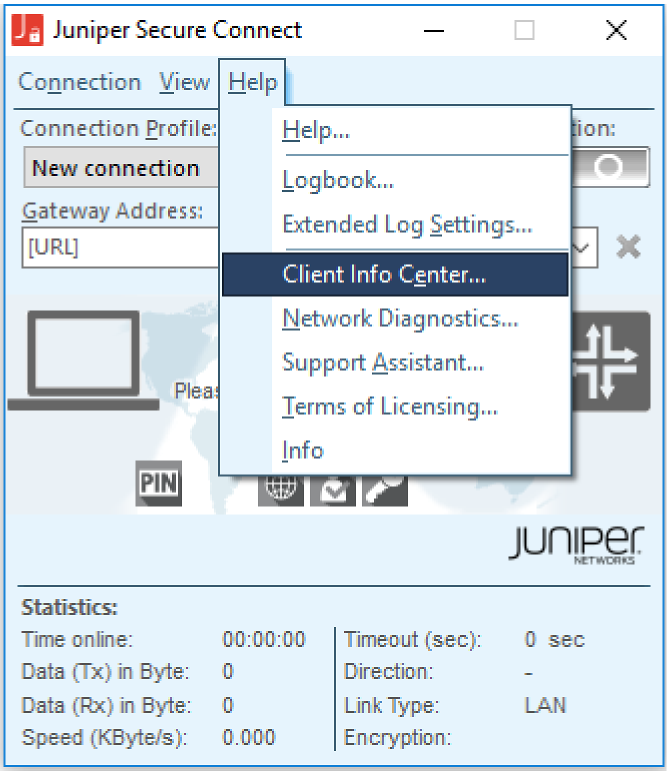
When you activate or deactivate log for a service, you must click corresponding **Restart** button to restart that particular service. Only that service restarts and not the system.

To restart a particular service, you do not need administrator rights.

Client Info Center Menu Option

Figure 149 on page 311 shows the **Client Info Center** in the **Help** menu options.

Figure 149: Client Info Center 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:	LAN
Speed (KByte/s):	0.000	Encryption:	

The **Client Info Center** optimizes your support at user helpdesk. The overview provides the following general information:

- Client Version (including Build Number)
- Current Connection Status (connected, disconnected, and interrupted due to error)
- Client Service Status
- Current Certification Configuration (including Lifespan)
- VPN User ID

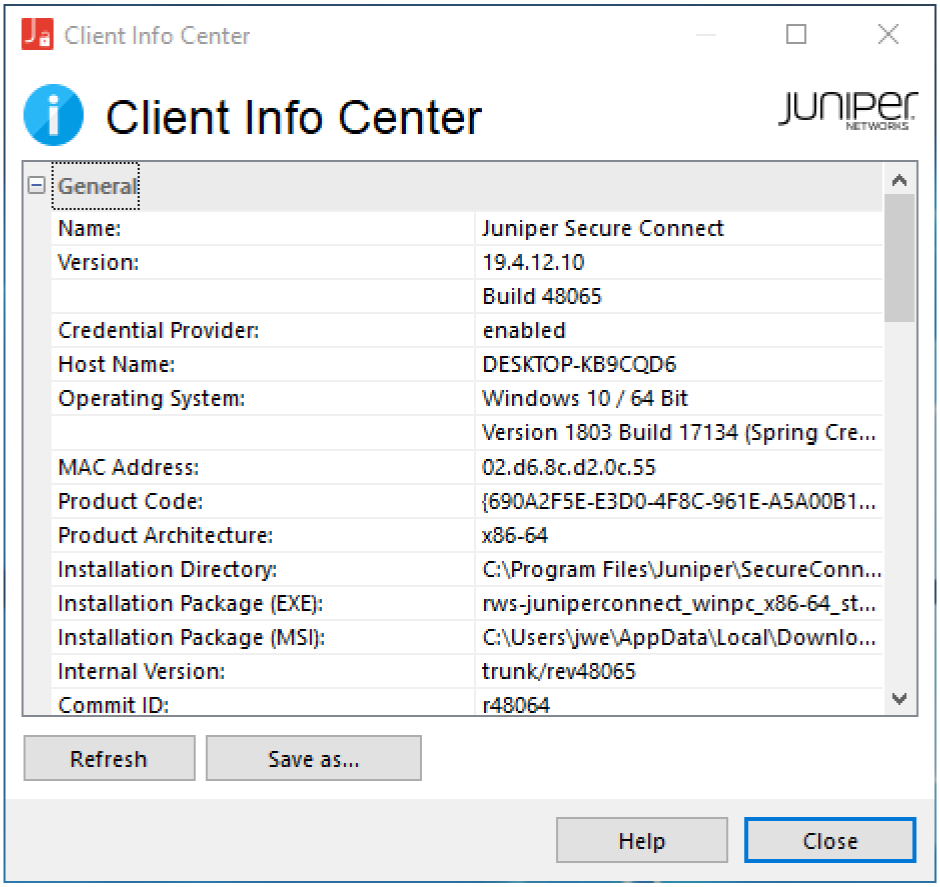
Following additional informations are also displayed:

- Connections
- Services

- Certificate Configuration
- Network Adapters

Figure 150 on page 312 shows an example of the **Client Info Center** window.

Figure 150: Displays Client Info Center



⊟ General

Name:	Juniper Secure Connect
Version:	19.4.12.10
	Build 48065
Credential Provider:	enabled
Host Name:	DESKTOP-KB9CQD6
Operating System:	Windows 10 / 64 Bit
	Version 1803 Build 17134 (Spring Cre...
MAC Address:	02.d6.8c.d2.0c.55
Product Code:	{690A2F5E-E3D0-4F8C-961E-A5A00B1...
Product Architecture:	x86-64
Installation Directory:	C:\Program Files\Juniper\SecureConn...
Installation Package (EXE):	rws-juniperconnect_winpc_x86-64_st...
Installation Package (MSI):	C:\Users\jwe\AppData\Local\Downlo...
Internal Version:	trunk/rev48065
Commit ID:	r48064

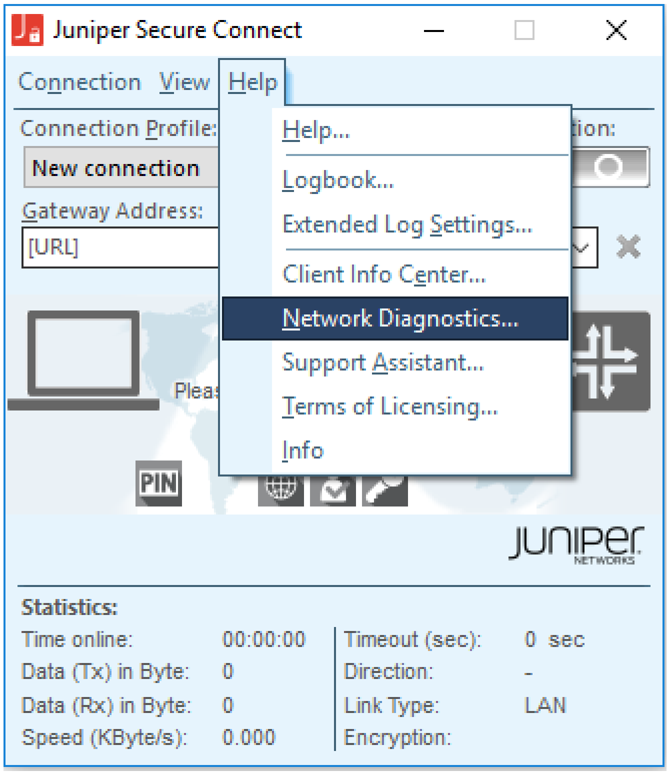
You can click the **Save to file** button at the bottom of **Client Info Center** screen to export the data to a text file. Irrespective of Juniper Secure Connect's operational state, you can also run the can following RWSCMD command to export the information:

```
rwscmd /writeClientInfoCenterData [OutFileName].
```

Network Diagnostics Menu Option

Navigate to **Help** > **Network Diagnostics** as shown in Figure 151 on page 313 to conduct network tests or test internet availability. Juniper Secure Connect supports both PING to an IP address in the Internet as well as resolution of an Internet Domain Name to an IP address. Enter the domain name in **name.com** format.

Figure 151: Network Diagnostics Menu Option

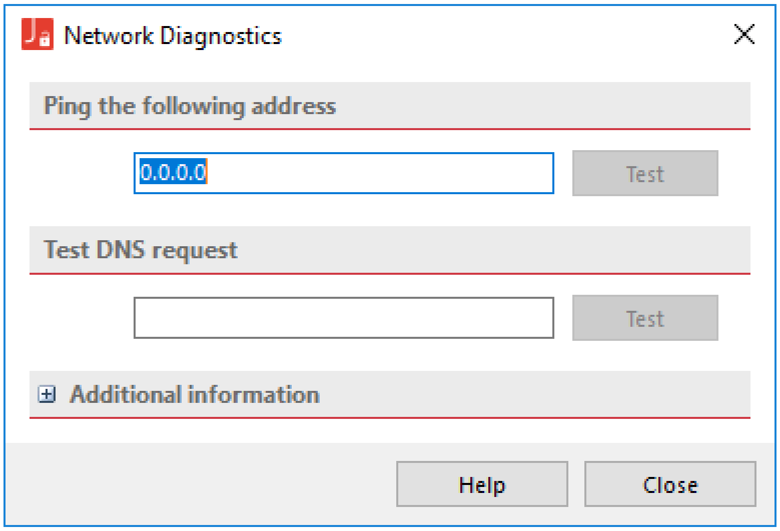


Statistics:

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

Figure 152 on page 314 shows an example how to test the availability of a host in a network.

Figure 152: Test Internet Connectivity



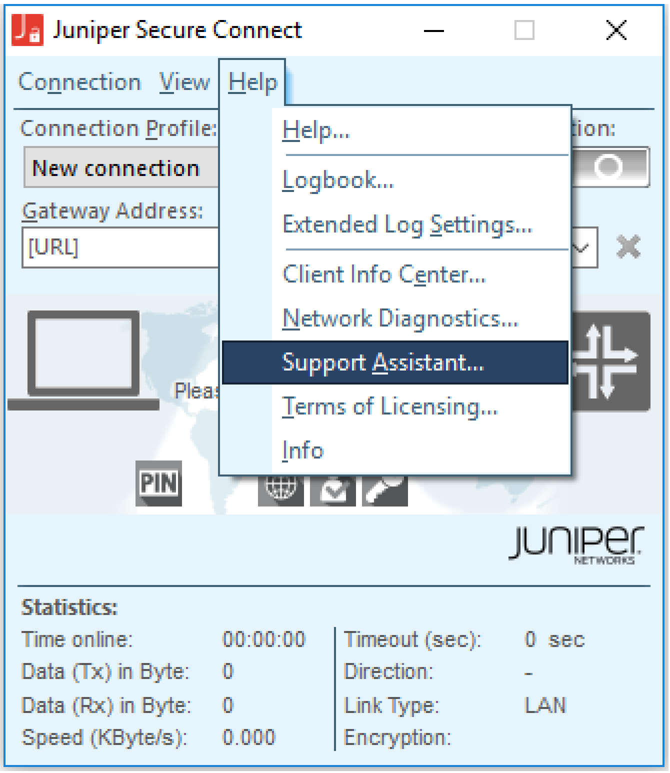
To conduct network test:

1. Enter the address and click the **Test** button.
2. If the test is successful, the **Network Diagnostics** window displays a green tick symbol and if the test fails, the **Network Diagnostics** window displays a red cross symbol. Additional details are displayed in a clear text log. This test is particularly useful for testing firewall rules for DNS requests and outgoing connections to the internet.

Support Assistant Menu Option

Use the **Support Assistant** as show in Figure 153 on page 315 to collect the extended log data and any appropriate system information.

Figure 153: Support Assistant Menu Option



Connection Profile: New connection

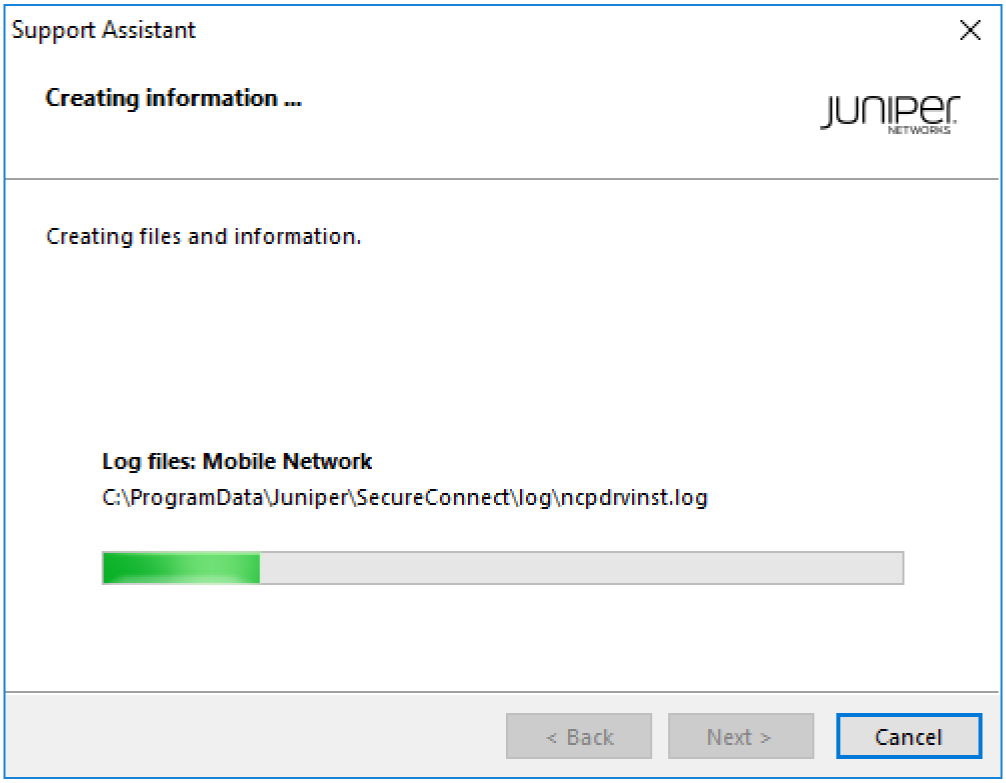
Gateway Address: [URL]

Statistics:

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

Select **Support Assistant** from the **Help** menu to create a log file as shown in Figure 154 on page 316.

Figure 154: Create Log File



Creating files and information.

Log files: Mobile Network

C:\ProgramData\Juniper\SecureConnect\log\ncpdrvinst.log

Terms of Licensing Menu Option

Navigate to **Help** > **Terms of Licensing** as shown in Figure 155 on page 317 to view the license terms of Juniper Secure Connect.

Figure 155: Terms of Licensing Menu Option

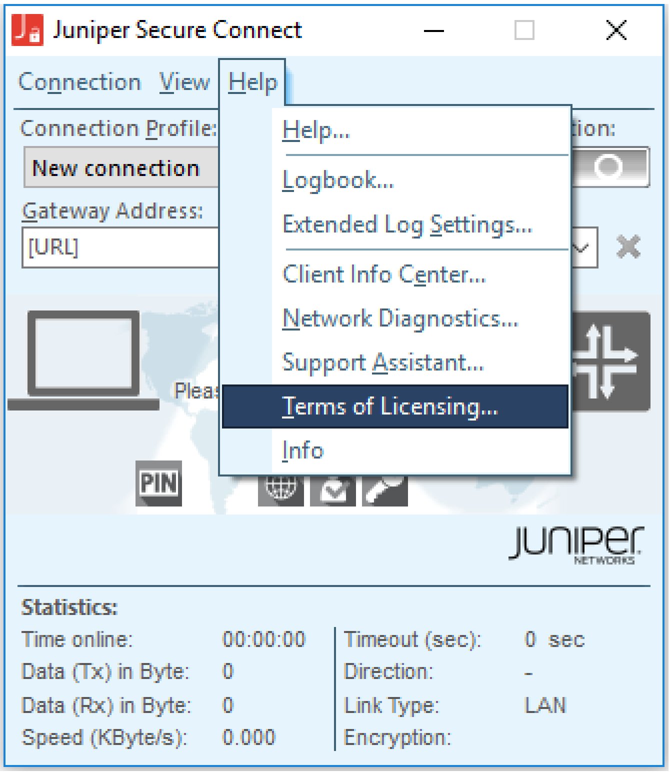
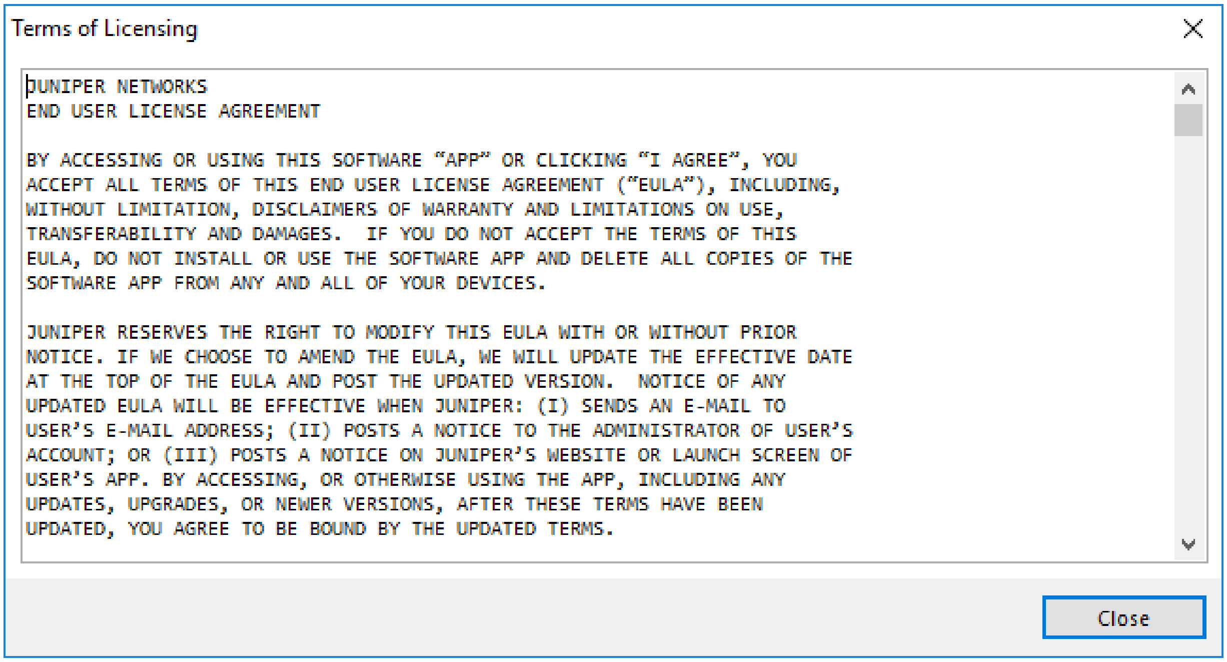


Figure 156 on page 318 shows the **Terms of Licensing** window.

Figure 156: Licensing Agreement Window



JUNIPER NETWORKS
END USER LICENSE AGREEMENT

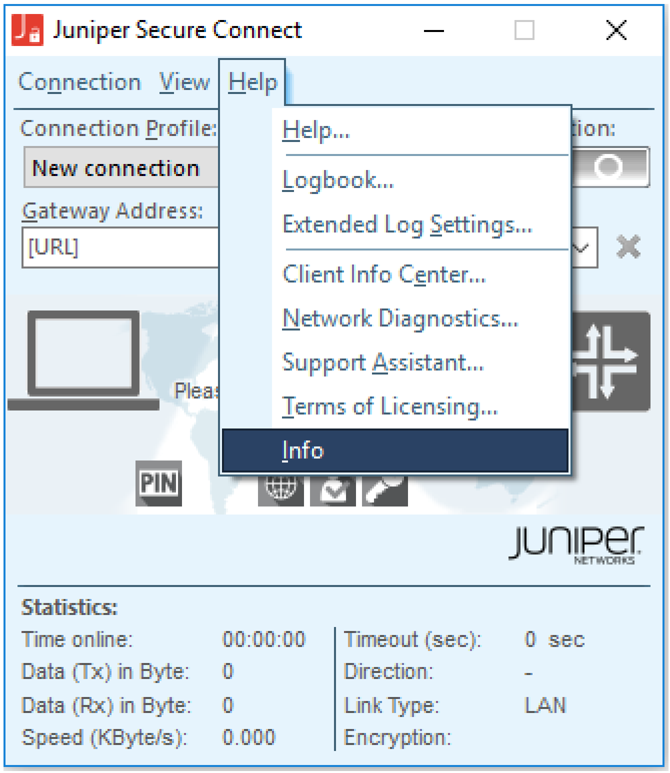
BY ACCESSING OR USING THIS SOFTWARE "APP" OR CLICKING "I AGREE", YOU ACCEPT ALL TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"), INCLUDING, WITHOUT LIMITATION, DISCLAIMERS OF WARRANTY AND LIMITATIONS ON USE, TRANSFERABILITY AND DAMAGES. IF YOU DO NOT ACCEPT THE TERMS OF THIS EULA, DO NOT INSTALL OR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

Info Menu Option

The **Info** window displays Juniper Secure Connect product label and version number (as show in Figure 158 on page 320) you've currently installed. See Figure 157 on page 319. See Figure 159 on page 321 for Device ID details. Device ID is available for Juniper Secure Connect application released on or after March 2023.

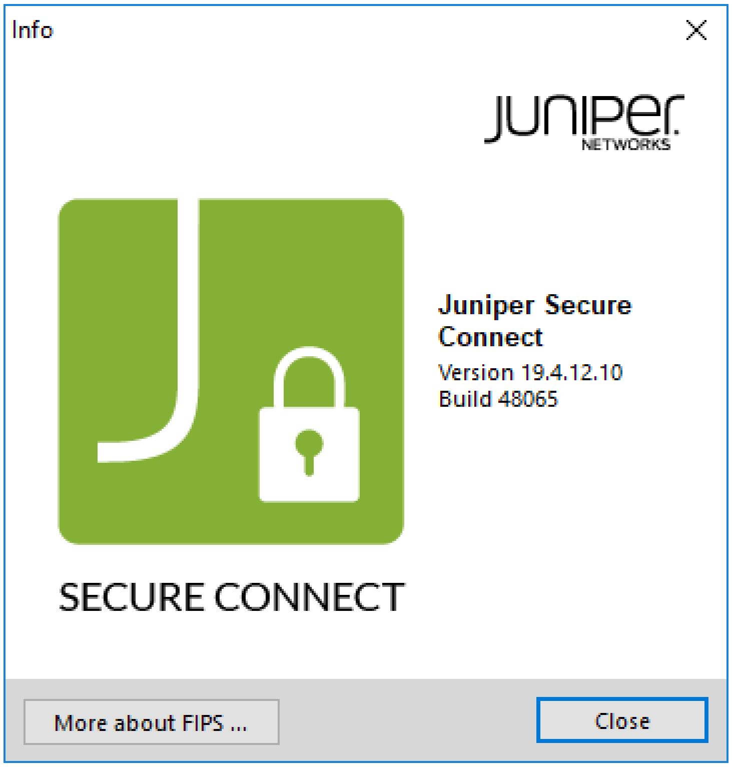
Figure 157: Info Menu Option



Statistics:

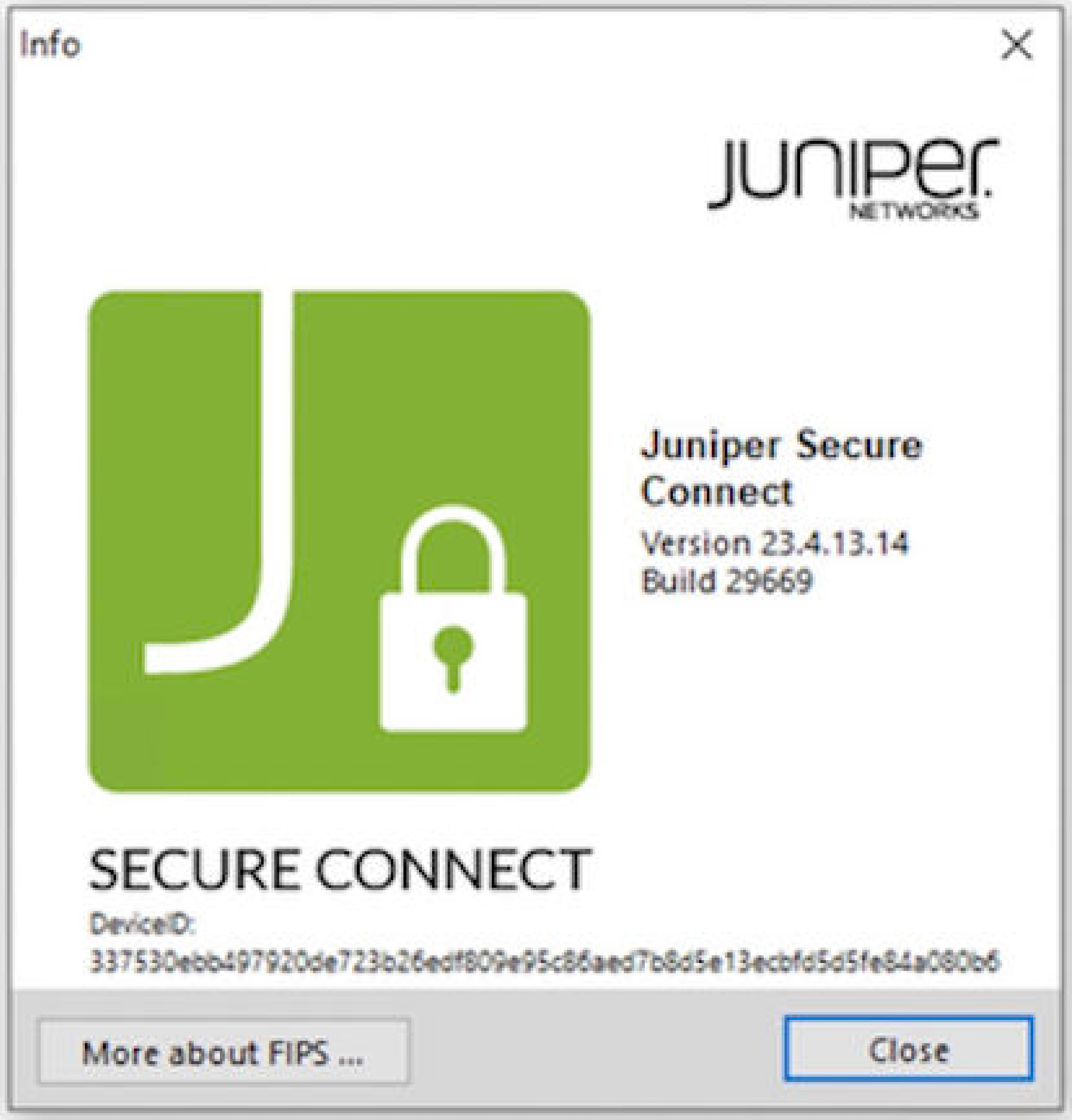
Time online:	00:00:00	Timeout (sec):	0 sec
Data (Tx) in Byte:	0	Direction:	-
Data (Rx) in Byte:	0	Link Type:	LAN
Speed (KByte/s):	0.000	Encryption:	

Figure 158: Displays Juniper Secure Connect Version Information



Juniper Secure Connect
Version 19.4.12.10
Build 48065

Figure 159: Displays Juniper Secure Connect Device ID Information



Info

Juniper Secure Connect

Version 23.4.13.14

Build 29669

SECURE CONNECT

DeviceID:

337530ebb497920de723b26edf809e95c86aed7b8d5e13ecbfd5d5fe84a080b6

8

CHAPTER

Juniper Secure Connect for macOS

SUMMARY

Learn about Juniper Secure Connect application for macOS.

IN THIS CHAPTER

Juniper Secure Connect application is a client-based SSL VPN software that can run on macOS. It ensures that you securely access resources in your corporate network. To complete the setup of Juniper Secure Connect application, your system administrator must first configure remote access on the SRX Series Firewall. After the remote access is configured, you can connect to your secured corporate resources using the Juniper Secure Connect application.

Read the following topics to install and use Juniper Secure Connect application for macOS:

- "Install Juniper Secure Connect on macOS" on page 323
- "Juniper Secure Connect GUI Elements" on page 274
- "Connection Menu" on page 347
- "View Menu" on page 354
- "Log Menu" on page 357
- "Help Menu" on page 359

RELATED DOCUMENTATION

Get Started with Juniper Secure Connect | 10

Install Juniper Secure Connect on macOS

SUMMARY

Learn about how to create rollout packages for Juniper Secure Connect application software and step-by-step procedures to install Juniper Secure Connect on macOS platform. If you want to install Juniper Secure Connect application, see "Manual Installation of Juniper Secure Connect" on page 324. If you are an administrator, see "Create Rollout Packages for Juniper Secure Connect Installation" on page 335 section to prepare the installer for software rollout.

IN THIS SECTION

What's Next

Download the Juniper Secure Connect application software from here. See release notes for more details.

For more information on Juniper Secure Connect GUI elements, see "Juniper Secure Connect GUI Elements" on page 274.

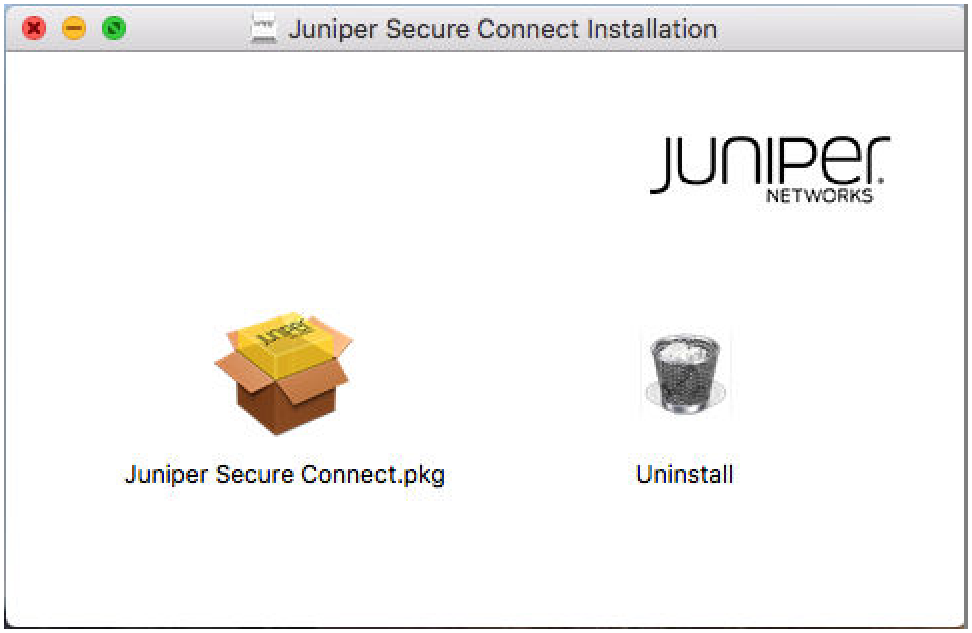
For more information on Juniper Secure Connect features and how to configure the options, see "Connection Menu" on page 347, "View Menu" on page 354, "Log Menu" on page 357, and "Help Menu" on page 359.

Manual Installation of Juniper Secure Connect

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

1. Run the Juniper Secure Connect installer (.dmg file). To start the installation, click on **Juniper Secure Connect.pkg**. See Figure 160 on page 324.

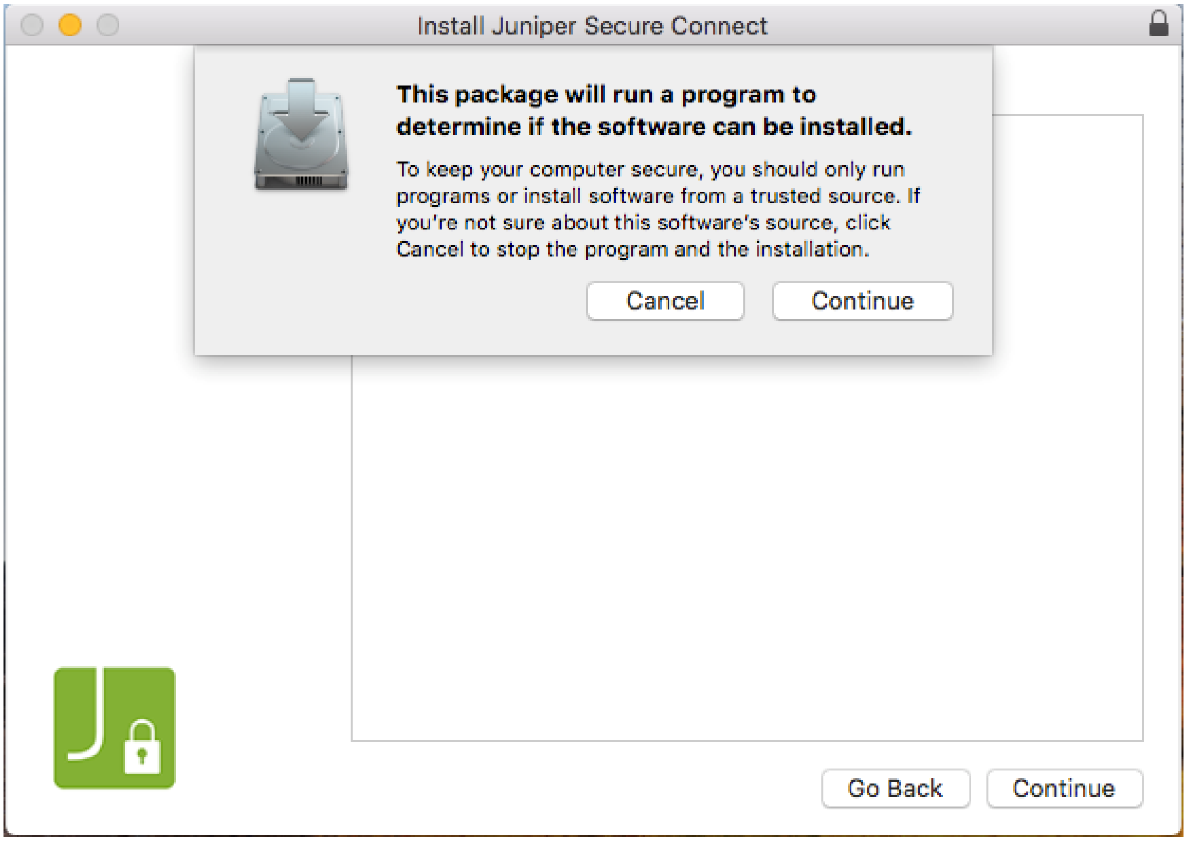
Figure 160: Juniper Secure Connect Installer



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

2. A pop-up window appears as shown in Figure 161 on page 325 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 161: Trusted Resource Verification Pop-up Window

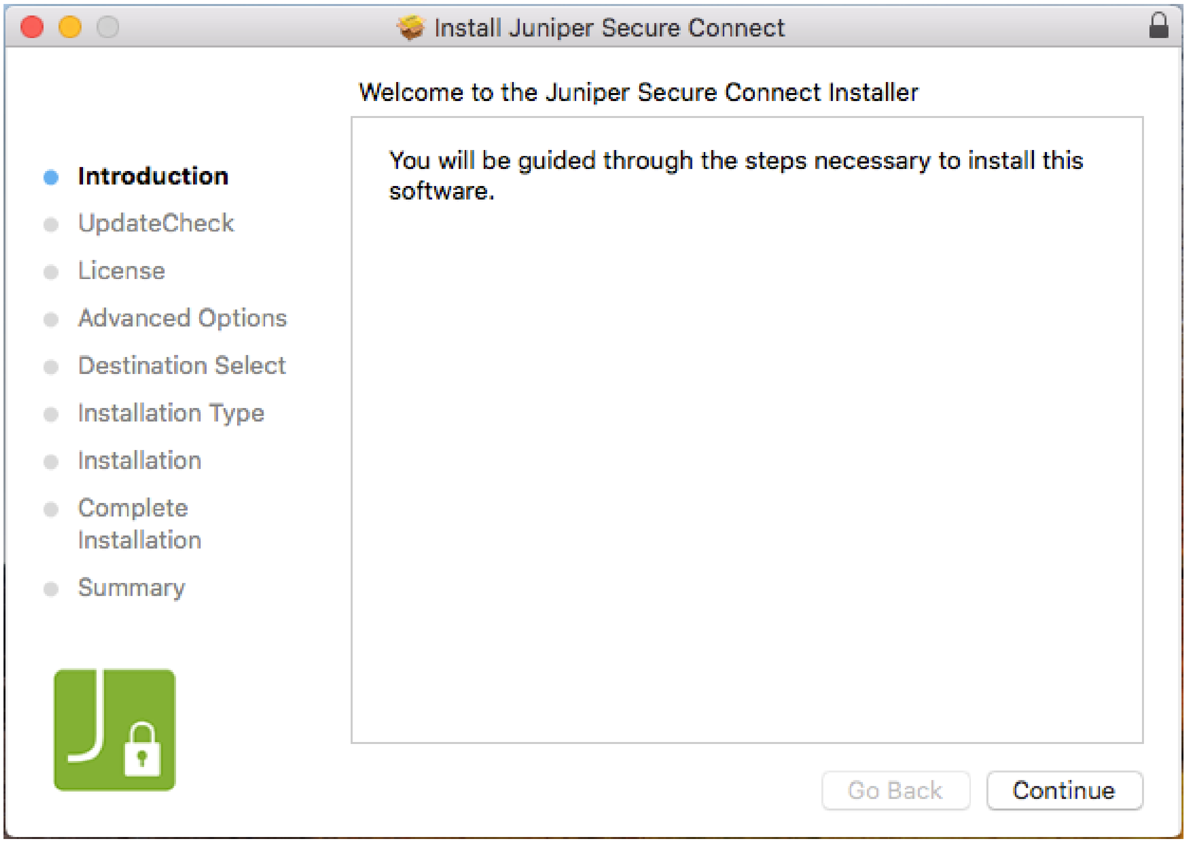


This package will run a program to determine if the software can be installed.

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 162 on page 326. Click **Continue**.

Figure 162: Installer Welcome Window

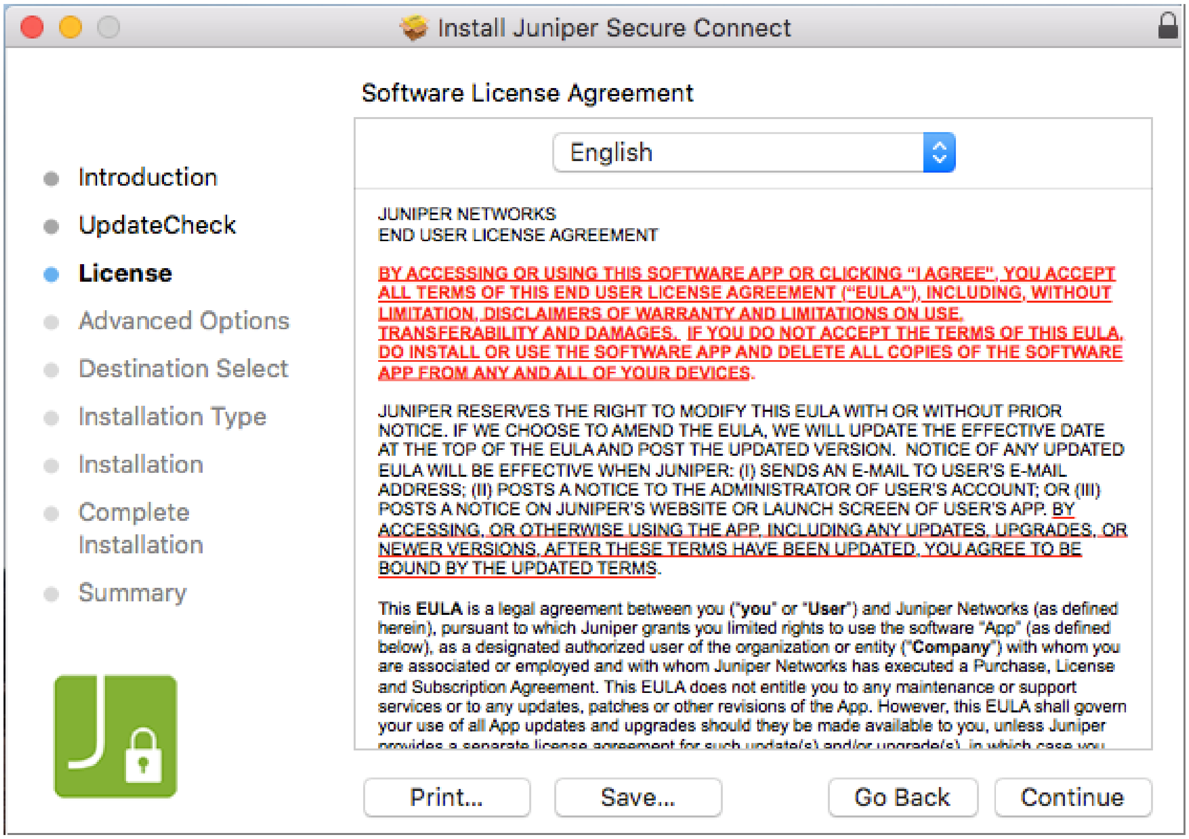


Welcome to the Juniper Secure Connect Installer

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

4. Juniper Secure Connect **Software License Agreement** page appears. See Figure 163 on page 327.

Figure 163: 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.

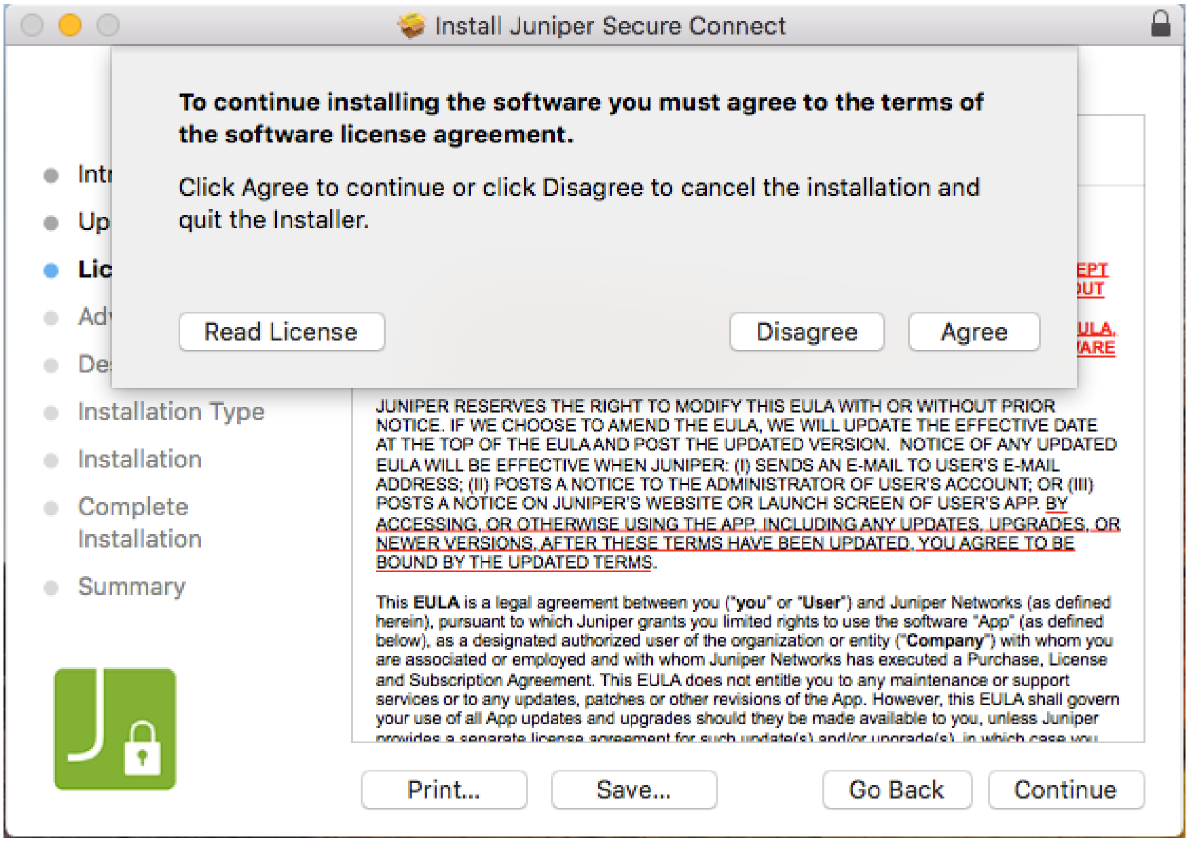
JUNIPER RESERVES THE RIGHT TO MODIFY THIS EULA WITH OR WITHOUT PRIOR NOTICE. IF WE CHOOSE TO AMEND THE EULA, WE WILL UPDATE THE EFFECTIVE DATE AT THE TOP OF THE EULA AND POST THE UPDATED VERSION. NOTICE OF ANY UPDATED EULA WILL BE EFFECTIVE WHEN JUNIPER: (I) SENDS AN E-MAIL TO USER'S E-MAIL ADDRESS; (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 164 on page 328.

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 164: Agree or Cancel License Agreement



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

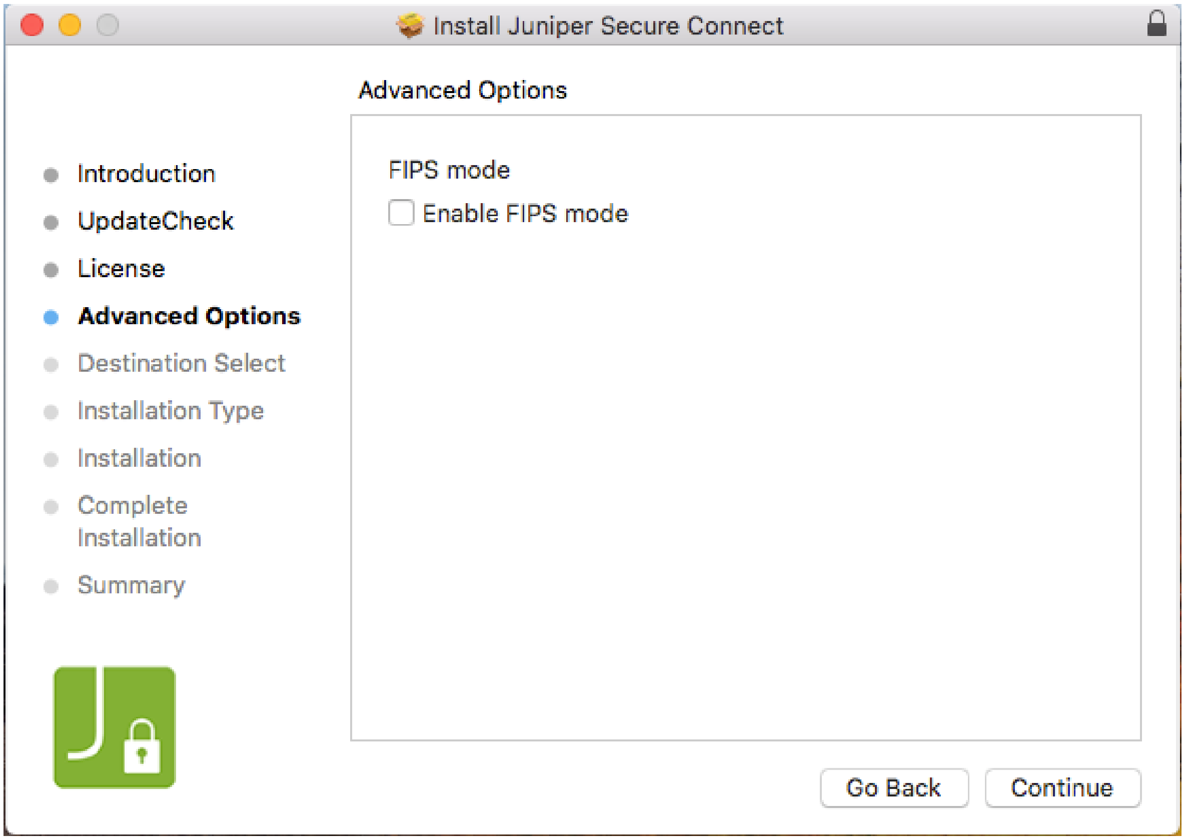
Click Agree to continue or click Disagree to cancel the installation and quit the Installer.

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 165 on page 329. Click **Continue**.

Figure 165: Configure FIPS Mode Option



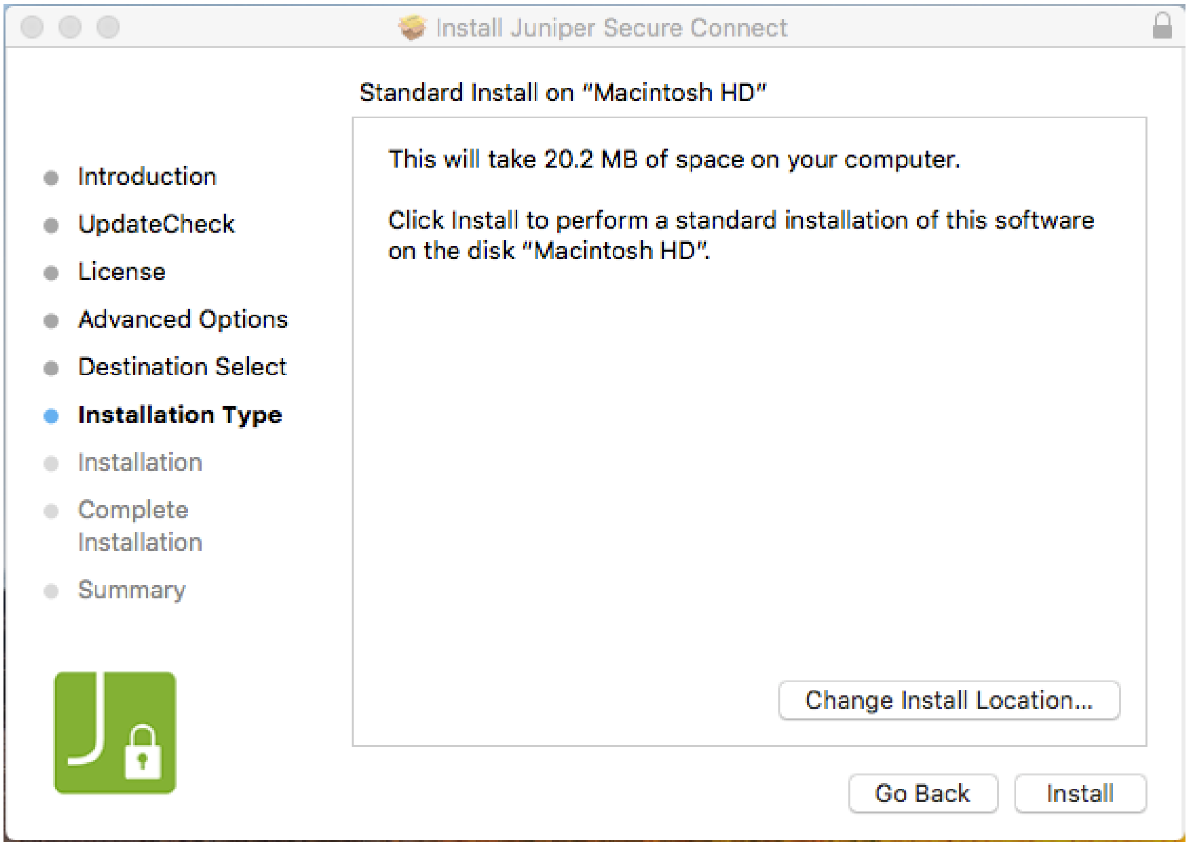
FIPS mode

□ Enable FIPS mode

NOTE: The SRX Series Firewall and the Juniper Secure Connect application are independent FIPS compliant products. For remote access VPN solution on FIPS evaluated SRX 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 166 on page 330.

Figure 166: Start Juniper Secure Connect Installation



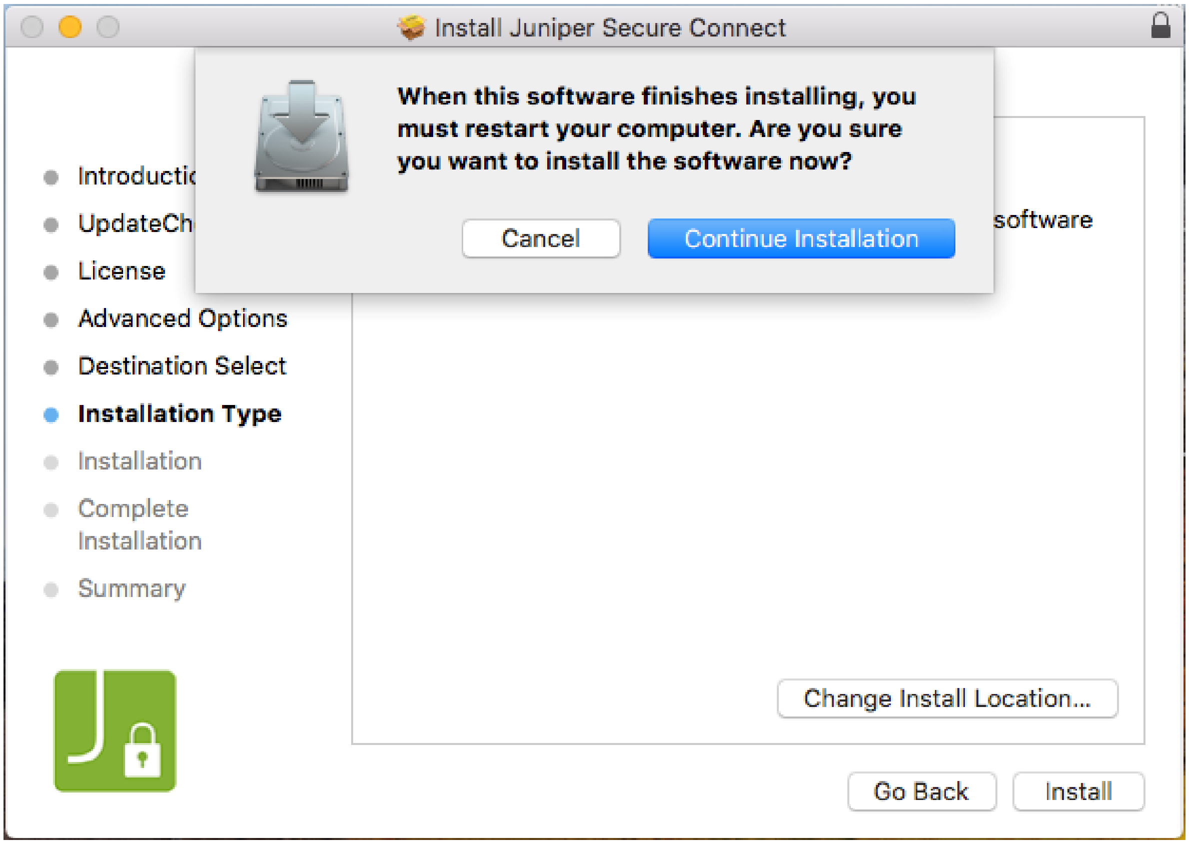
Standard Install on "Macintosh HD"

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 167 on page 331 is displayed to confirm restarting the computer when the installation is complete. Click **Continue Installation** to confirm restart.

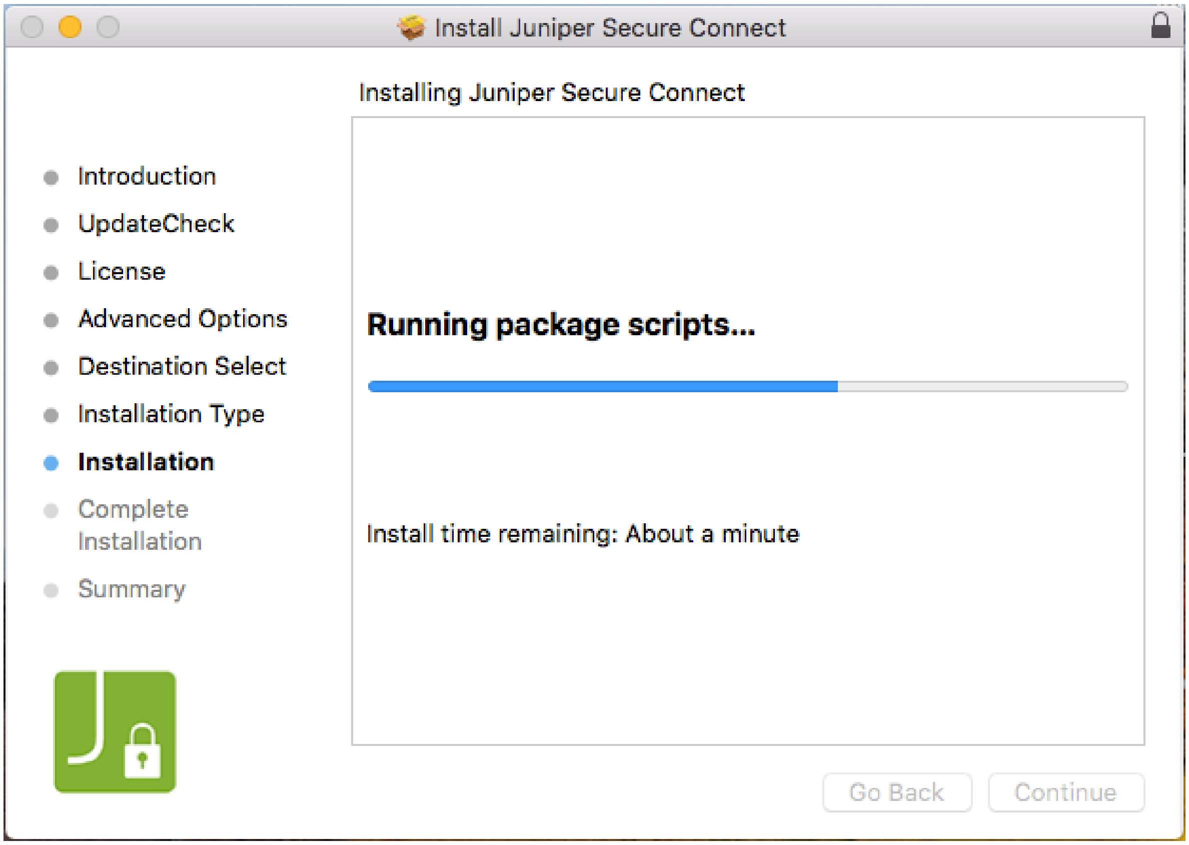
Figure 167: Confirm Restart after Installation



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 168 on page 332.

Figure 168: Running Juniper Secure Connect Installation Package



Install Juniper Secure Connect

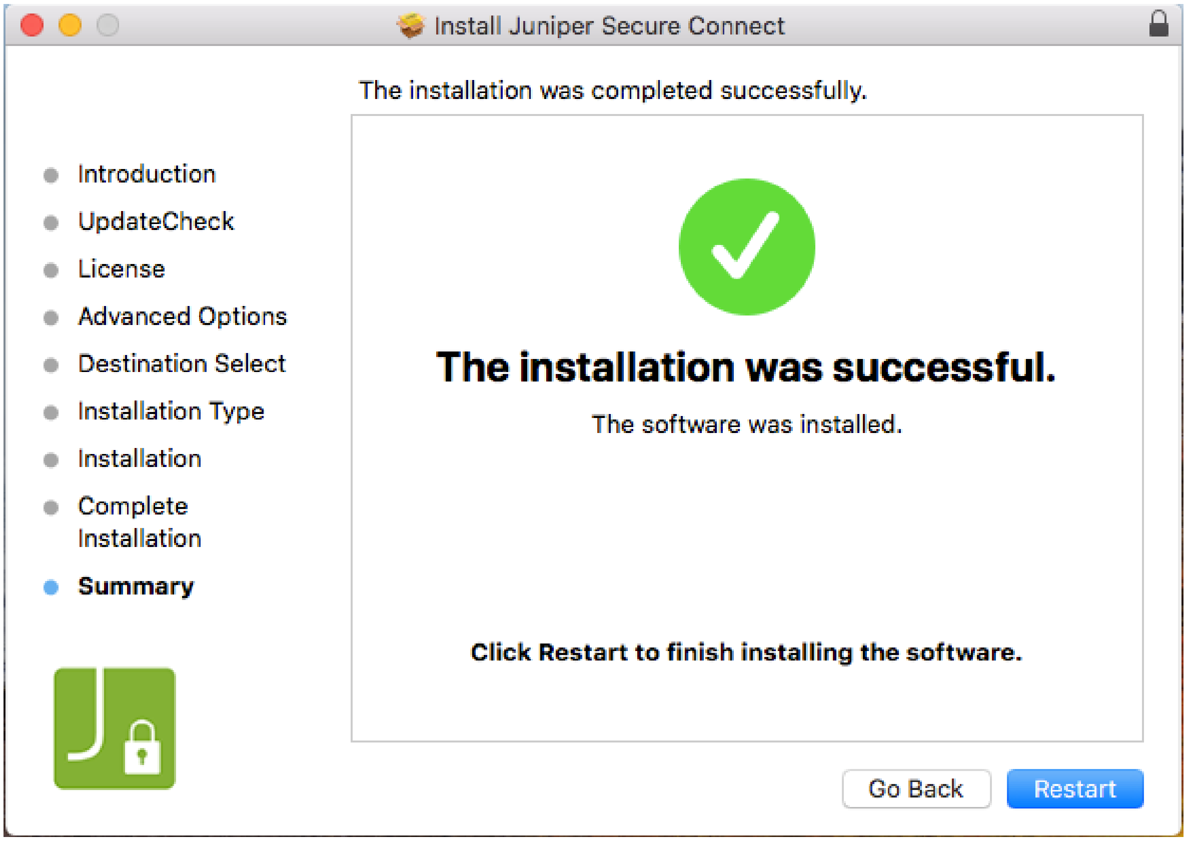
Installing Juniper Secure Connect

Running package scripts...

Install time remaining: About a minute

Figure 169 on page 333 shows an example of the Juniper Secure Connect installation window when the installation is successfully completed.

Figure 169: Juniper Secure Connect Installation Completed



Install Juniper Secure Connect

The installation was completed successfully.

The installation was successful.

The software was installed.

Click Restart to finish installing the software.

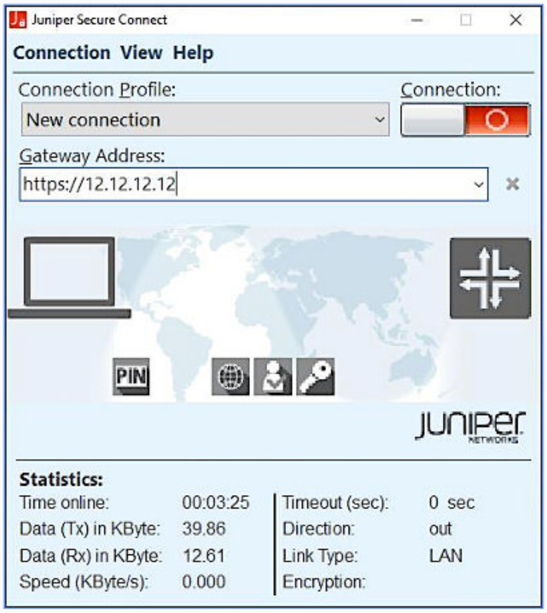
Congratulations! The Juniper Secure Connect application is successfully installed in your Mac.

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 170 on page 334 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.example.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 170: Launch Juniper Secure Connect



Connection Profile: New connection

Gateway Address: https://12.12.12.12

Statistics:

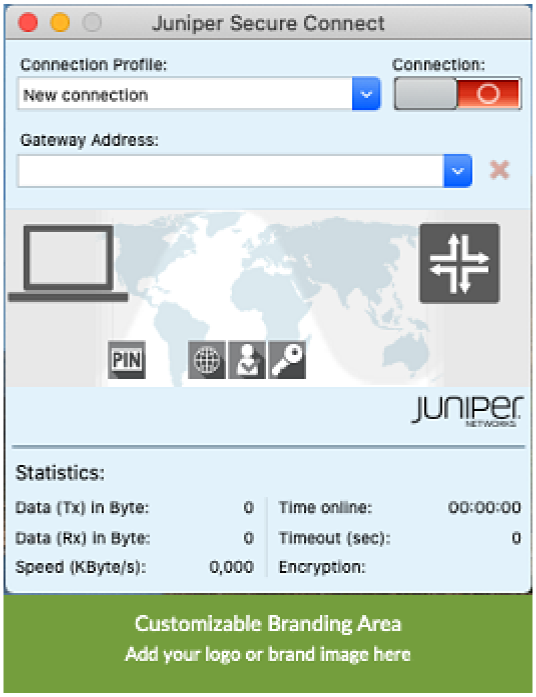
Time online:	00:03:25	Timeout (sec):	0 sec
Data (Tx) in KByte:	39.86	Direction:	out
Data (Rx) in KByte:	12.61	Link Type:	LAN
Speed (KByte/s):	0.000	Encryption:	

Custom Branding Option (macOS)

Juniper Secure Connect for macOS allows you to add your own logo or branding image. It also allows you to add HTML page for the branding image that would open when you click on the branding area in the Juniper Secure Connect. The HTML page is optional where you can provide any information you want. You should customise the installation package for branding your client. For detailed instructions, see "Create Rollout Packages for Juniper Secure Connect Installation (macOS)" on page 335 .

Figure 171 on page 335 is the sample screen, where the customizable branding area is highlighted:

Figure 171: Custom Branding Option (macOS)



Juniper Secure Connect

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:

Customizable Branding Area
Add your logo or brand image here

Create Rollout Packages for Juniper Secure Connect Installation

As a system administrator, you can also build your own rollout packages, if required. Building the rollout packages is an optional step. When you create rollout packages for Juniper Secure Connect application, you can install the application across the organization. Read the following steps to learn how you, as a system administrator can prepare the Juniper Secure Connect installer for the software rollout.

Juniper Secure Connect provides the installer for macOS as a disk image (**.dmg**) file. First you need to mount the package that is located inside the **.dmg** file. To do this, double-click its icon in the **Finder**. It should then mount the image and display its contents. You can see the installer package and the uninstall program when you double-click the image file in the **Finder** window.

Note that the **.dmg** file is write-protected and as a system administrator you must first convert the **.dmg** file into a read or write format. You also must convert and resize the image before distributing the installer to users.

1. Install the Juniper Secure Connect application manually on one device. After the installation is complete, initiate a connection to the profiles to be saved for the users.
2. Create a folder with name **JuniperSecureConnect** including the sub-directories as shown below (all directory are case-sensitive):

   \Users\...\Documents\JuniperSecureConnect\ImportDir

\Users\...\Documents\JuniperSecureConnect\ImportDir\cacerts

\Users\...\Documents\JuniperSecureConnect\ImportDir\certs

3. Copy the **ncpphone.cfg** file from **\Library\Application Support\Juniper\SecureConnect\** folder to the following folder:

   \Users\...\Documents\JuniperSecureConnect\ImportDir

4. Copy your CA certificates to the following folder:

   \Users\...\Documents\JuniperSecureConnect\ImportDir\cacerts\

5. (Optional) To add a custom branding option, follow these steps:

   - Create an **.ini** file named **ProjectLogo.ini** that contains the following information:

     ```
     [GENERAL]
     Picture=\Users\...\Documents\JuniperSecureConnect\ImportDir\cbo.png
     HtmlLocal=\Users\...\Documents\JuniperSecureConnect\ImportDir\cbo.html
     ```

   - Create a logo in **.bmp** file format and with **cbo.png** file name. The width of the image must be 328 pixels only. The height of the image can be adjusted from 24 pixels and above.

   - You can optionally create an HTML file with **cbo.html** as a file name that will open if the user clicks on the logo in the application.

   - Now copy these three files (**ProjectLogo.ini**, **cbo.png**, and **cbo.html**) into the following folder:

     \Users\...\Documents\JuniperSecureConnect\ImportDir\

6. Skip this step, if you are using pre-shared key authentication method.

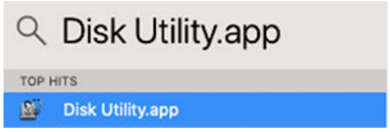
   For EAP-TLS authentication, you must save the user certificates only with name **user.p12** in below directory.

   \Users\...\Documents\JuniperSecureConnect\ImportDir\certs\

   Ensure that user certificate is unique for each installation package.

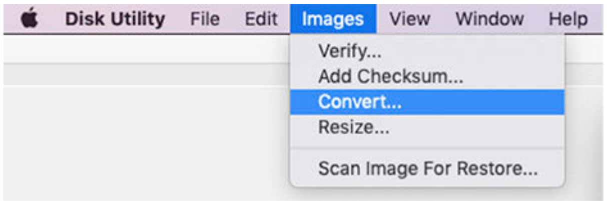
7. On macOS, open the **Disk Utility.app** as shown in Figure 172 on page 336.

   Figure 172: Disk Utility

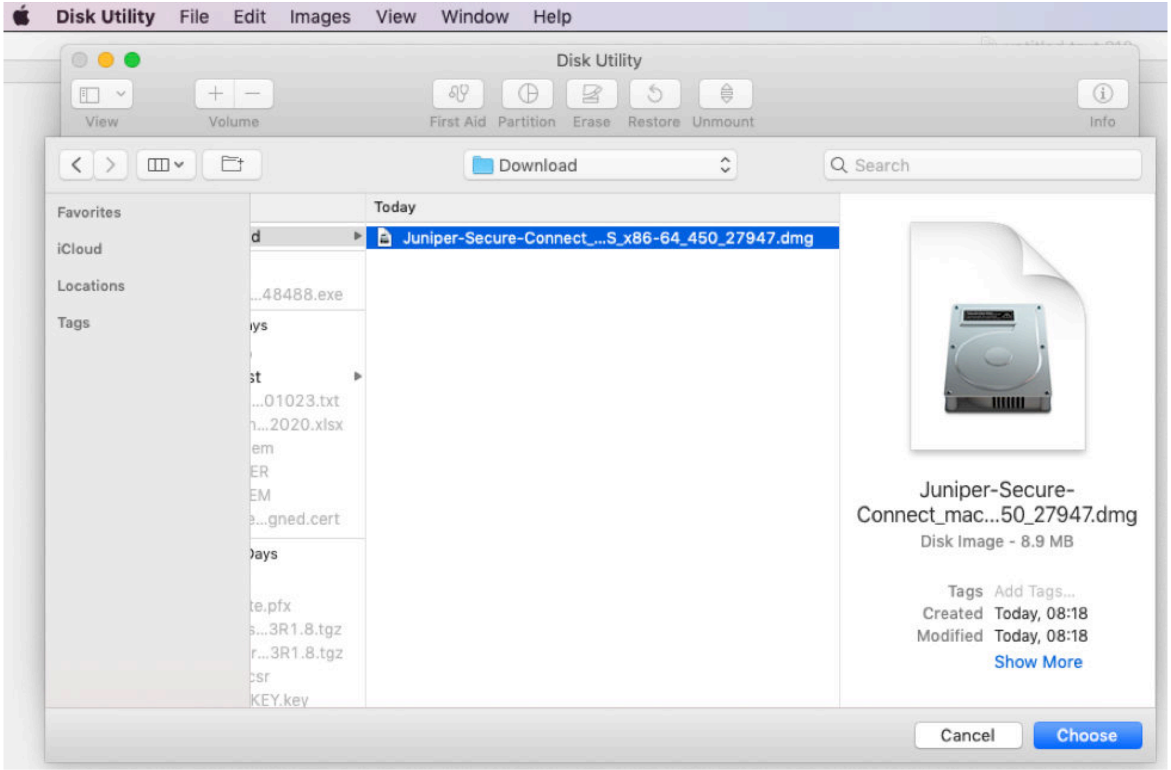
8. In the menu bar, select **Images** > **Convert** as shown in Figure 173 on page 337.

Figure 173: Convert an Image



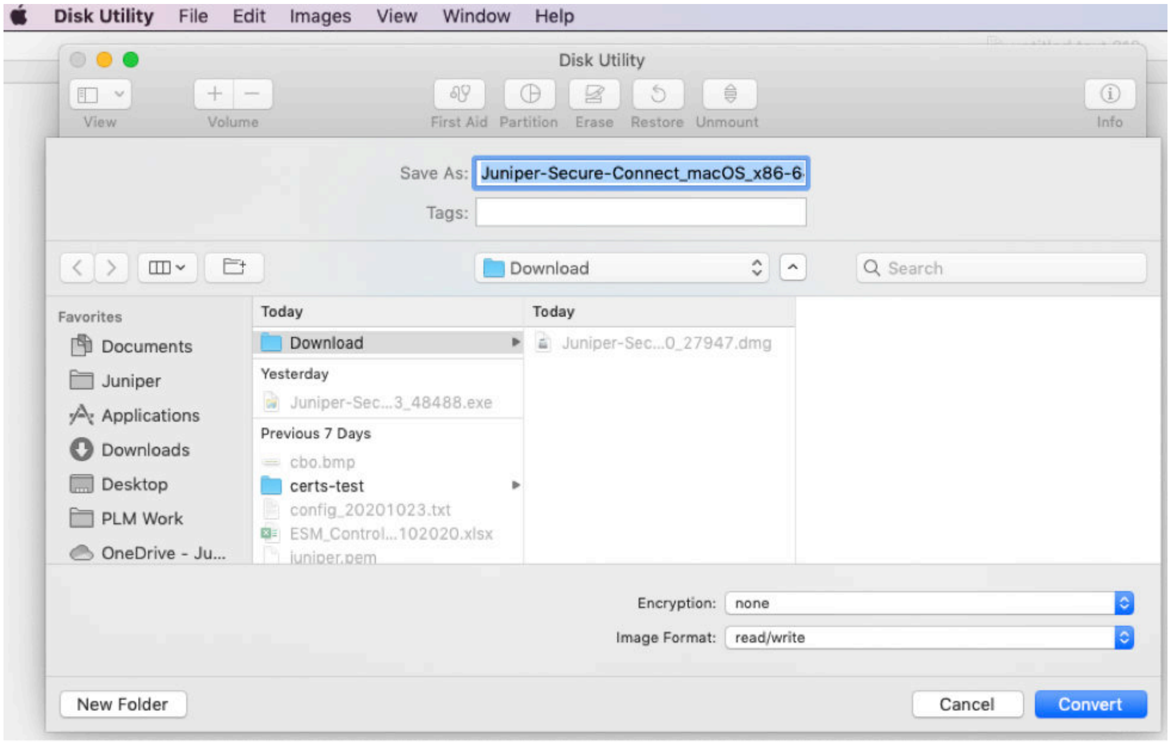
9. Select the image that you would like to use as shown in Figure 174 on page 337.

Figure 174: Select Juniper Secure Connect Image



10. Select the folder location and save this image with the name of your choice. Change the **Image Format** to **read/write** and click **Convert** as shown in Figure 175 on page 338.

Figure 175: Update Image Format



Save As: Juniper-Secure-Connect_macOS_x86-6

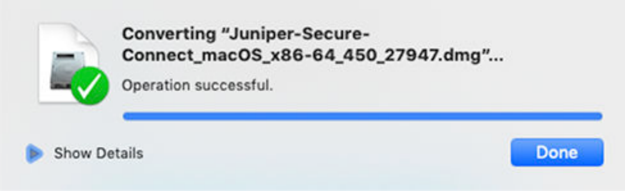
Tags:

Encryption: none

Image Format: read/write

11. Once the conversion is successful, click **Done** as shown in Figure 176 on page 338. The version that you see on the figure is dependent on the Juniper Secure Connect application release number.

Figure 176: Image Conversion Process

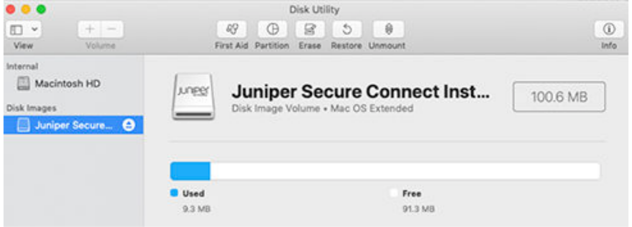


Converting “Juniper-Secure-Connect_macOS_x86-64_450_27947.dmg”...

Operation successful.

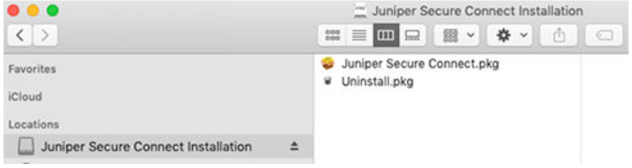
12. Unmount this disk in the **Disk Utility** tool as shown in Figure 177 on page 339.

Figure 177: Unmount Process



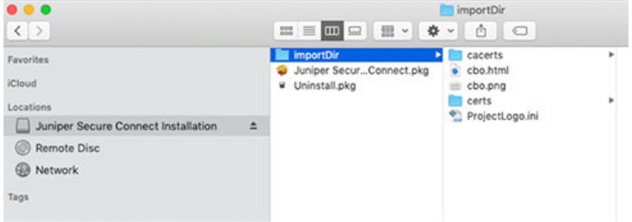
13. Double-click on the newly created image to get it mounted as shown in Figure 178 on page 339.

Figure 178: Mount the new Image


Juniper Secure Connect Installation
Favorites
iCloud
Locations
Juniper Secure Connect Installation
Juniper Secure Connect.pkg
Uninstall.pkg

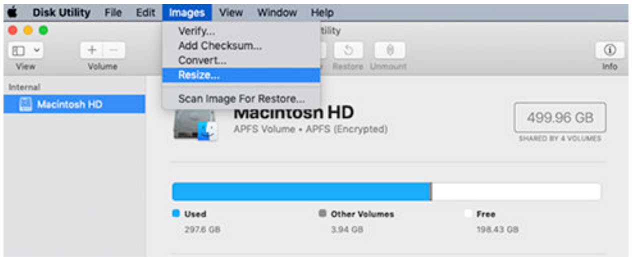
14. Copy the **ImportDir** directory to this mounted drive as shown in Figure 179 on page 339.

Figure 179: Copy ImportDir Folder To Mount Drive



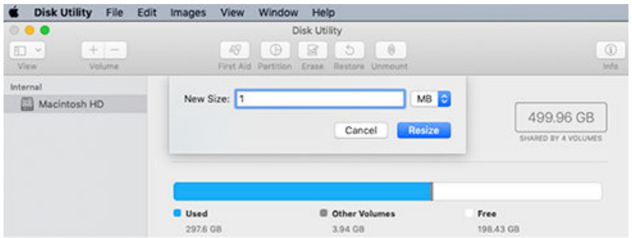
15. Navigate back to the **Disk Utility** tool. In the menu bar, select **Images > Resize...** and then select the file as shown in Figure 180 on page 339.

Figure 180: Navigate to Resize Image Option



16. Set the **New Size** to **1MB**, and click **Resize** as shown in Figure 181 on page 340.

Figure 181: Resize Image



New Size: 1 MB

You've successfully created the rollout package and ready to distribute Juniper Secure Connect installer. The newly created **.dmg** file is the installer.

Juniper Secure Connect GUI Elements

SUMMARY

Juniper Secure Connect GUI elements provides a quick display of additional information about your remote access connection.

IN THIS SECTION

The Juniper Secure Connect window provides a quick view of:

- Connection profile
- SRX Series Firewalls gateway address
- Connection status
- Connection statistics

Table 30 on page 341 provides the details of Juniper Secure Connect GUI elements.

Table 30: GUI Elements in Juniper Secure Connect display window

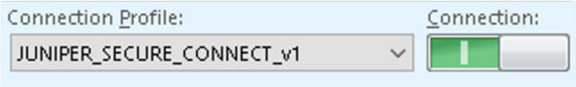
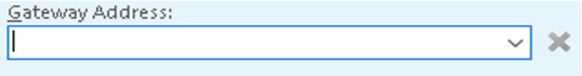
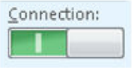
Element	Description
Connection Profile dropdown list  Connection Profile: JUNIPER_SECURE_CONNECT_v1 Connection:	Location—Below the menu bar. Click the dropdown list to view the currently added connection profile. You can access a different SRX Series Firewalls, by choosing **New Connection** in the connection profiles to download a new configuration.
Gateway Address dropdown list  Gateway Address:	Location—Below the **Connection Profile** dropdown list. Enter the SRX Series Firewall URL for a new connection. You must enter the URL provided by your administrator for **Gateway Address** field. For example, let's consider an URL https://12.12.12.12 that does not include the realm name. Another example https://12.12.12.12/engineering, where engineering refers to realm name. If your administrator provides you the URL with realm name, it must be entered as it is.
Connection Button  Connection:	Location—Next to **Connection Profile** dropdown list. Click this button to connect or disconnect a VPN connection.

Table 30: GUI Elements in Juniper Secure Connect display window *(Continued)*

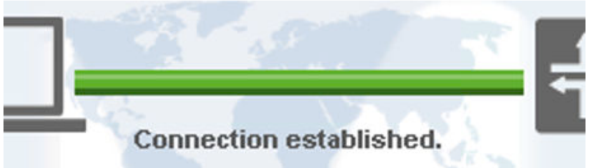
Element	Description
Connection status bar  Connection established.	Location—Center of Juniper Secure Connect window. The color of the connection bar changes from yellow to green during connection. These colors represents: • Thin yellow bar: Juniper Secure Connect is trying to contact the VPN gateway and establish phase 1 of the VPN session. • Thick yellow bar: Juniper Secure Connect has established phase 1 of the VPN session and is establishing phase 2. • Green bar: Juniper Secure Connect has established the VPN connection. • Broken green bar: Juniper Secure Connect has lost Internet connection and will try to reconnect the VPN connection as soon as internet is available.
PIN Icon PIN	Location—Below the connection status bar. • If the PIN icon is gray, the PIN has not been entered to access the user certificate or the user certificate can not be found. • If the PIN icon is green, the PIN for the user certificate has been entered, and Juniper Secure Connect is able to use the user certificate.
World Icon 🌐	Location—Below the connection status bar. • If the world icon is gray, the Juniper Secure Connect is not trying to connect. • If the world icon is blue, the Juniper Secure Connect is trying to connect the VPN gateway. • If the world icon is green, the Juniper Secure Connect was able to communicate with the VPN gateway.

Table 30: GUI Elements in Juniper Secure Connect display window *(Continued)*

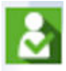
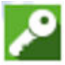
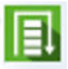
Element	Description
Person or checkmark Icon 	Location—Below the connection status bar. - If the person icon is gray, the Juniper Secure Connect is not trying to connect. - If the person icon is blue, the Juniper Secure Connect is trying to authenticate the user. - If the person icon is green, the Juniper Secure Connect was able to authenticate the user.
Key Icon 	Location—Below the connection status bar. - If the key icon is gray, the Juniper Secure Connect is not trying to connect. - If the key icon is blue, the Juniper Secure Connect is trying to establish the VPN session (phase2). - If the key icon is green, the Juniper Secure Connect application was able to establish phase 2 and the complete VPN session.
Arrow or U-Turn Icon 	Location—Below the connection status bar. If the Arrow or U-Turn icon is green, the Juniper Secure Connect has detected an issue with the IPsec connection and has automatically switched over to SSL VPN.

Table 30: GUI Elements in Juniper Secure Connect display window *(Continued)*

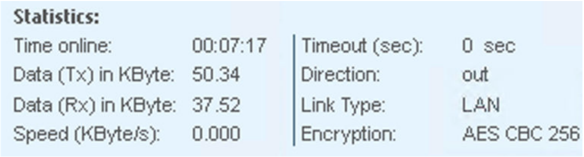
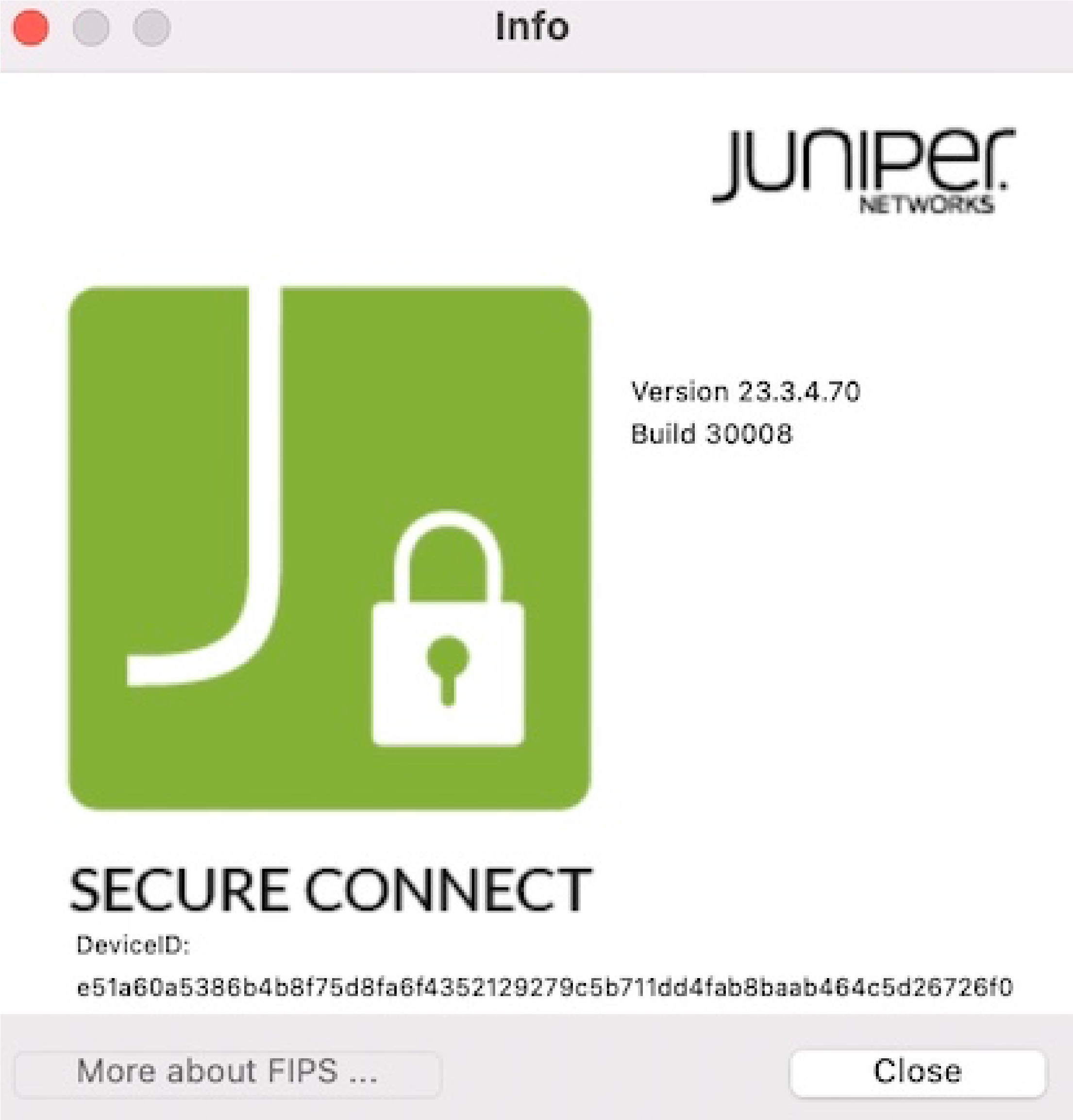
Element	Description
Connection Statistics  Statistics: Time online: 00:07:17 | Timeout (sec): 0 sec Data (Tx) in KByte: 50.34 | Direction: out Data (Rx) in KByte: 37.52 | Link Type: LAN Speed (KByte/s): 0.000 | Encryption: AES CBC 256	Location—Bottom of the Juniper Secure Connect window. Juniper Secure Connect window displays the following connection statistics: • **Time online**—Shows the time a user has been connected with the same connection profile. Restarting the Juniper Secure Connect or changing the connection profile resets this value. • **Data (Tx) in Byte**—Shows the data sent or transmitted over the VPN tunnel into the remote network while being connected to the same connection profile. Restarting the Juniper Secure Connect or changing the connection profile resets this value. • **Data (Rx) in Byte**—Shows the data received over the VPN tunnel into the remote network while being connected to the same connection profile. Restarting the Juniper Secure Connect or changing the connection profile resets this value. • **Speed**—Shows the average speed calculated using the connection time, Data (Tx), and Data (Rx). Restarting the Juniper Secure Connect or changing the connection profile resets this value. • **Timeout**—This value shows `0 sec`, if no timeout for the VPN session is used. If a timeout is used, the timeout shows the amount of seconds. The Juniper Secure Connect starts count down for the timeout as soon as no data is received over the VPN tunnel and resets as soon as data is received of the VPN tunnel. • **Direction**—The Juniper Secure Connect can only establish outgoing connection. The value will show “out”.

Table 30: GUI Elements in Juniper Secure Connect display window *(Continued)*

Element	Description
	• **Link Type**—The Juniper Secure Connect shows "LAN". This means the Juniper Secure Connect does not act as a internet dialer, but only establishes the VPN connection. • **Encryption**—This value shows the encryption used in phase 2.

The Juniper Secure Connect displays Device ID information from May 2023 application release. To know about the Device ID information, navigate to **About Juniper Secure Connect**.

Figure 182: Displays Juniper Secure Connect Device ID Information



Info

Version 23.3.4.70
Build 30008

SECURE CONNECT

DeviceID:
e51a60a5386b4b8f75d8fa6f4352129279c5b711dd4fab8baab464c5d26726f0

WHAT'S NEXT

For more information on Juniper Secure Connect features and how to configure the options on Windows, see "Connection Menu" | 281, "View Menu" | 295, and "Help Menu" | 304.
For more information on Juniper Secure Connect features and how to configure the options on macOS, see "Connection Menu" | 347, "View Menu" | 354, "Log Menu" | 357, and "Help Menu" | 359.

Connection Menu

SUMMARY

Juniper Secure Connect **Connection** menu provides you the options to establish remote access connection and secure the connection with certificates. Use the **Connection** menu for connection related options to view the certificates, enter PIN, reset PIN, or change PIN.

IN THIS SECTION

WHAT'S NEXT

For more information on Juniper Secure Connect GUI elements, see "Juniper Secure Connect GUI Elements" | **274**.
For more information on Juniper Secure Connect features and how to configure the options, see "View Menu" | **354**, "Log Menu" | **357**, and "Help Menu" | **359**.

Connect Menu Option

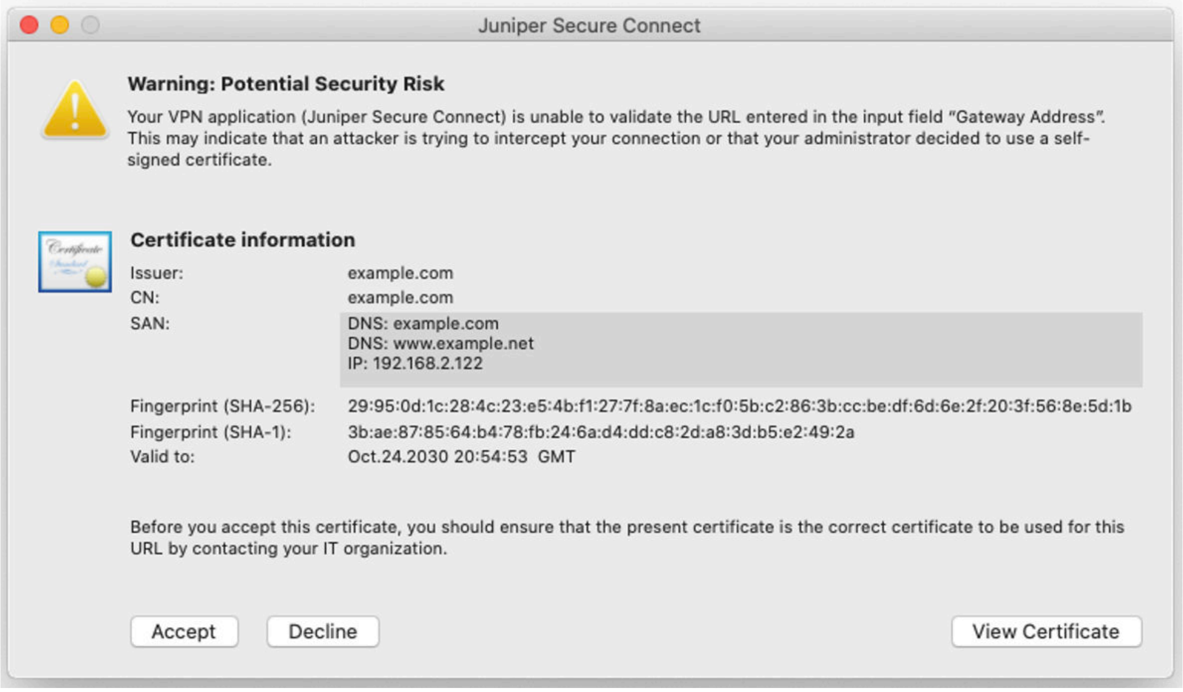
1. You must first define and select a profile to establish a connection for that profile. Click on the **Connection Profile** dropdown list and select a profile for which you want to establish a connection.

2. 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 as shown in Figure 184 on page 348.

   ⚠ **WARNING:** If the following the warning message is displayed, your application is missing the CA certificate from the VPN gateway (SRX Series Firewall). If you are a remote user, contact your IT organization for appropriate action. If you are a system administrator, place the cacerts in the respective location for the platform.

   Figure 183 on page 348 is a sample warning message on macOS platform when CA certificate is not present.

Figure 183: Sample Certificate Warning Message on macOS Platform



Warning: Potential Security Risk

Your VPN application (Juniper Secure Connect) is unable to validate the URL entered in the input field "Gateway Address". This may indicate that an attacker is trying to intercept your connection or that your administrator decided to use a self-signed certificate.

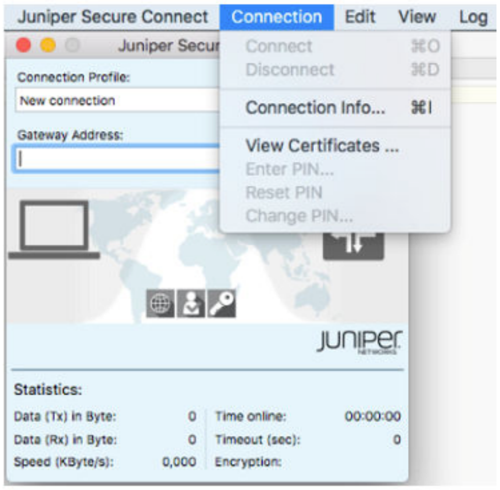
Certificate information

Issuer:	example.com
CN:	example.com
SAN:	DNS: example.com DNS: www.example.net IP: 192.168.2.122
Fingerprint (SHA-256):	29:95:0d:1c:28:4c:23:e5:4b:f1:27:7f:8a:ec:1c:f0:5b:c2:86:3b:cc:be:df:6d:6e:2f:20:3f:56:8e:5d:1b
Fingerprint (SHA-1):	3b:ae:87:85:64:b4:78:fb:24:6a:d4:dd:c8:2d:a8:3d:b5:e2:49:2a
Valid to:	Oct.24.2030 20:54:53 GMT

Before you accept this certificate, you should ensure that the present certificate is the correct certificate to be used for this URL by contacting your IT organization.

3. To disconnect the existing connection, go to **Connection** > **Disconnect**, or use the **Connection** toggle button.

Figure 184: Connection Menu



Connection Profile: New connection

Gateway Address:

Statistics:

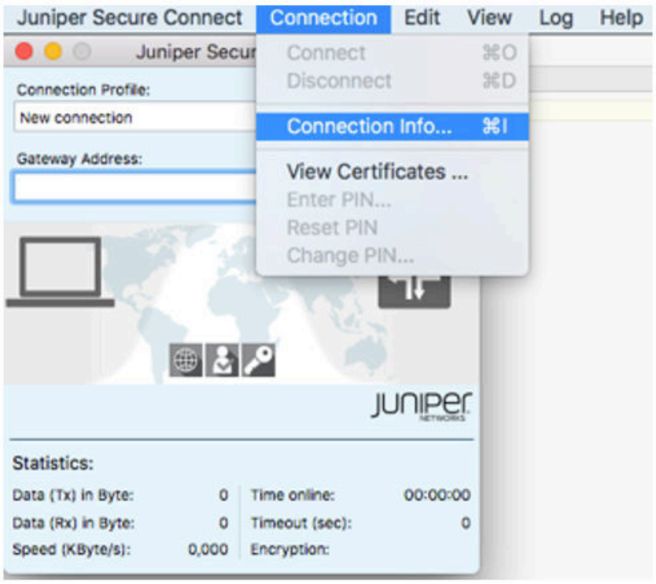
Data (Tx) in Byte:	0	Time online:	00:00:00
Data (Rx) in Byte:	0	Timeout (sec):	0
Speed (KByte/s):	0,000	Encryption:	

Connection Info Menu Option

In the menu bar, navigate to **Connect** > **Connection Info** to get the following information on your connection as shown in Figure 185 on page 349:

- Name of the currently selected profile
- Statistics information (for example, time online, and value of timeout)
- IP addresses (VPN IP address, DNS server, and VPN Endpoint)
- Security mode
- Security keys used

Figure 185: Connection Info Option



Connection Profile:
New connection

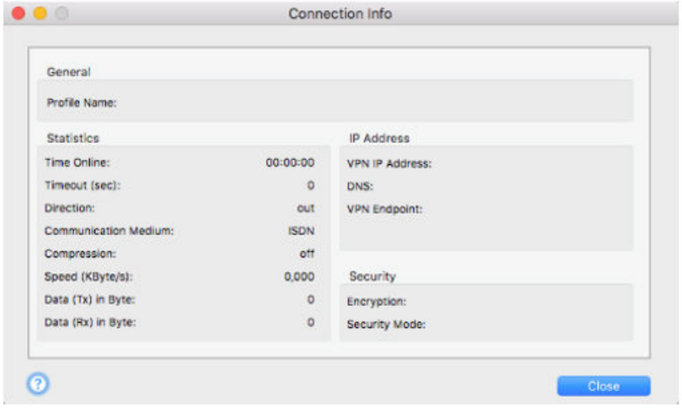
Gateway Address:

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:

Figure 186 on page 350 shows an example of connection information for a VPN connection.

Figure 186: Connection Information



General

Profile Name:

Statistics

Time Online: 00:00:00
Timeout (sec): 0
Direction: out
Communication Medium: ISDN
Compression: off
Speed (KByte/s): 0,000
Data (Tx) in Byte: 0
Data (Rx) in Byte: 0

IP Address

VPN IP Address:
DNS:
VPN Endpoint:

Security

Encryption:
Security Mode:

View Certificates Menu Option

Certification Authority (CA) (also referred as the Issuer) creates and issues certificates using a PKI manager (software) and stores as a soft certificate.

User and CA certificates are stored in the following directory locations:

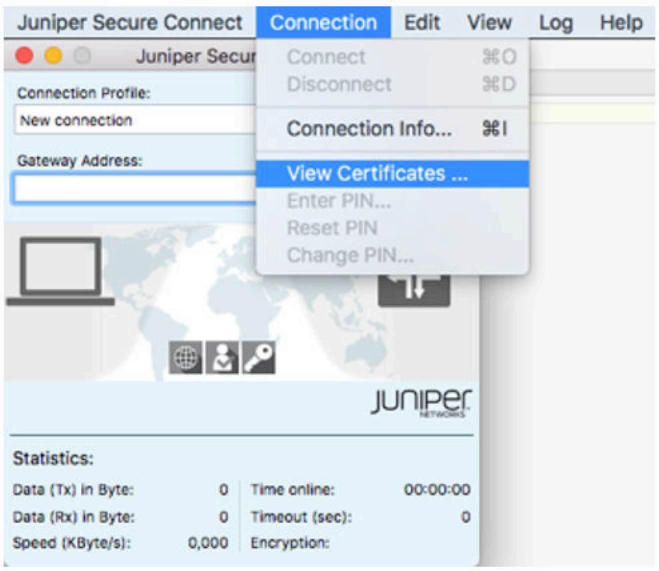
- User certificates are stored as a **PKCS#12** file in **/Library/Application Support/Juniper/SecureConnect/certs** folder location, like **/Library/Application Support/Juniper/SecureConnect/certs/user.p12**.

- CA or issuer certificates are stored in **/Library/Application Support/Juniper/SecureConnect/cacerts** folder location.

Juniper Secure Connect supports ***.pem** and ***.crt** formats for CA certificates.

Navigate to **Connection** > **Certificates** and select **View Certificates** as shown in Figure 187 on page 351 to view certificates related menu options.

Figure 187: Certificates Menu Option



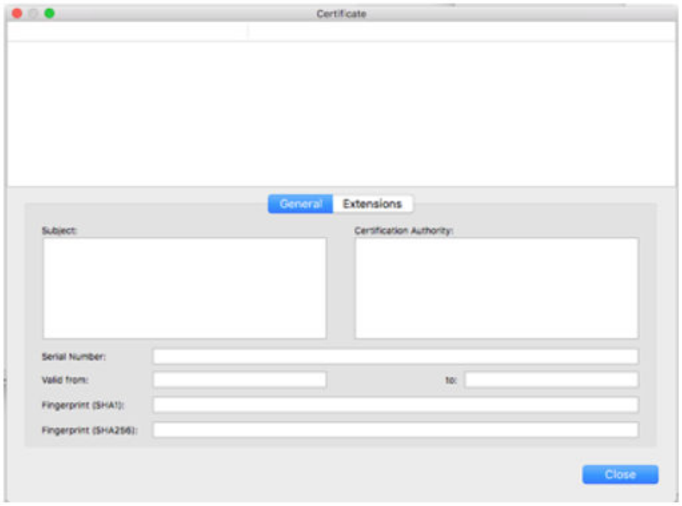
Connection Profile: New connection

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:

Figure 188 on page 351 shows an example of **CA certificates** window, after selecting **Display CA Certificates** option from the **Certificates** menu.

Figure 188: View Certificates



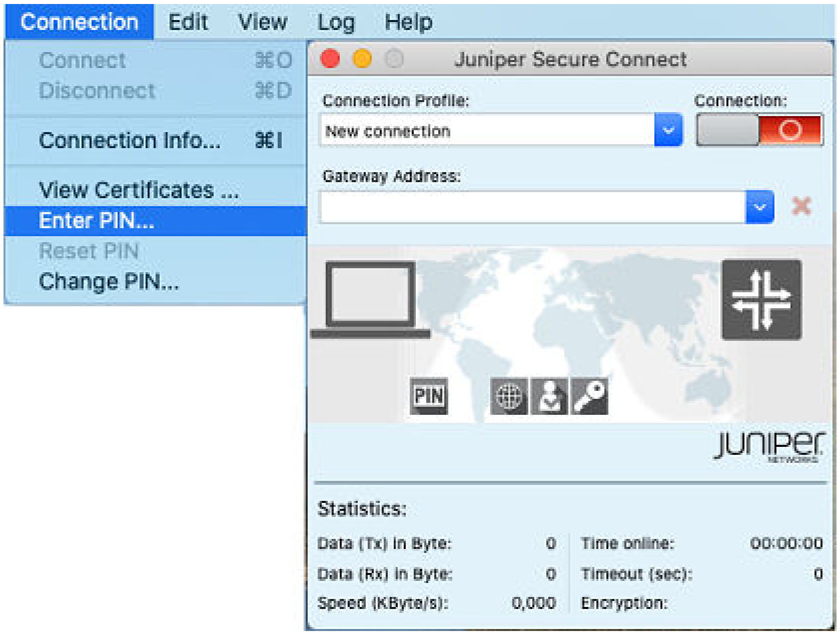
Enter PIN Menu Option

You can enter the PIN after starting the Juniper Secure Connect and before establishing a connection. If you want to establish a connection using a certificate at a later time, then you can skip the PIN entry unless the certificate configuration requires it.

To enter your PIN:

1. Navigate to **Connection** > **Enter PIN** from the menu. See Figure 189 on page 352.

Figure 189: Enter PIN 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:	

2. Enter the PIN. Your PIN must be minimum of six digits in length.
3. Click **OK**.

You need a PIN to establish the connection with certificates successfully. At the first time of establishing a connection manually, you must enter the PIN. For subsequent manual connections, you can skip entering the PIN again. A correct PIN entry is indicated by a green PIN symbol.

Change PIN Menu Option

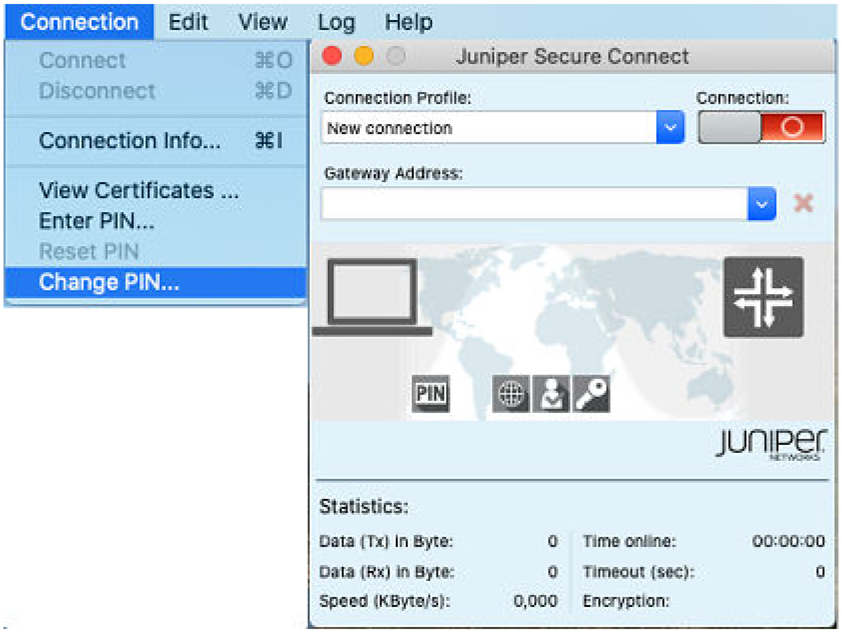
In Juniper Secure Connect, if you want to enter the PIN only before establishing the connection, your administrator needs to enable **PIN request at each connection** option for **Certificate Based** Authentication method. Administrator can enable **PIN request at each connection** option to prevent an unauthorized user from setting up an unauthorized connection when the PIN has already been entered. When **PIN request at each connection** option is enabled, whenever you establish a connection, you are prompted to enter the PIN.

If you select **Connection** > **Change PIN**, the PIN that has already been requested in connection with other functions is no longer used, that is, when setting up a connection, or in the **Enter PIN** connection menu. Instead you can always select the **Connection** > **Change PIN** and the new PIN will be automatically reset immediately after the change. This ensures that when configuring **PIN request at each connection** (by your administrator) on an unauthorized Juniper Secure Client, an unauthorized user's PIN cannot be used at anytime to establish a connection.

To change your PIN for a smartcard or token or soft certificate:

1. Navigate to **Connection** > **Change PIN** in the menu bar. See Figure 190 on page 353.

Figure 190: Change PIN 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:	

2. Enter the correct PIN number has been entered previously.
3. Enter your new PIN and confirm it by repeating it.
4. Click **OK**. You have now changed your PIN.

Reset PIN Menu Option

To reset your PIN:

1. You can select **Connection** > **Reset PIN** to reset the PIN.
2. You must enter the correct PIN to reset the PIN, because, the certificate is used to establish the connection.
3. If the PIN is reset, you cannot use this certificate to establish a connection, until the correct PIN is entered again.

View Menu

SUMMARY

Juniper Secure Connect **View** menu provides you options to change the appearance or display of Juniper Secure Connect application.

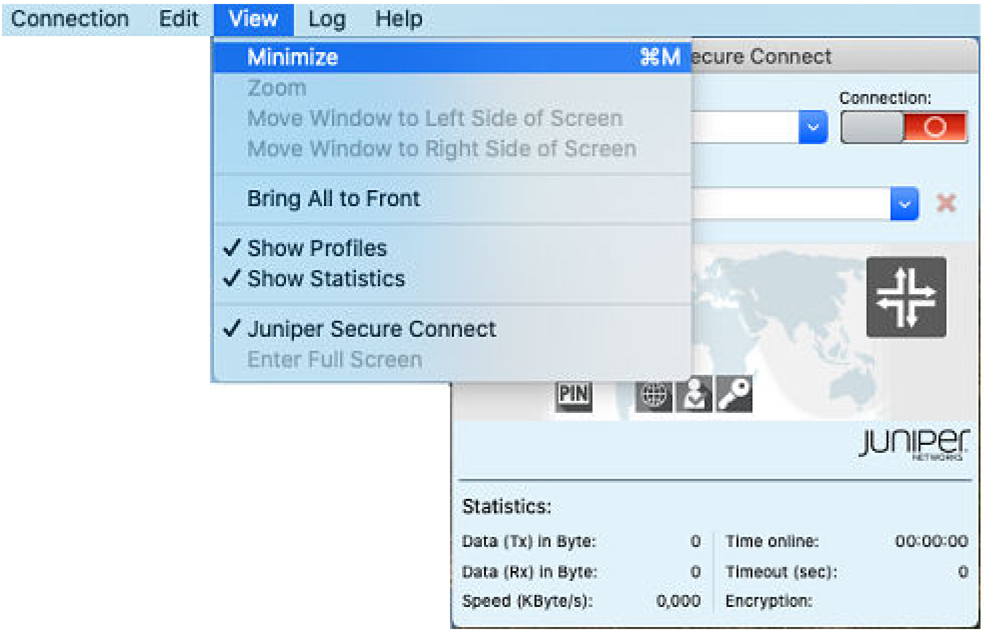
IN THIS SECTION

You can use the **View** menu options to show or hide various information and statistics fields.

- Navigate to **View** > **Zoom** and select **Zoom** option to increase the size of the Juniper Secure Connect window on the display with information fields (if needed), or reduce to its smallest possible size by switching off all information fields.

- Navigate to **View** > **Minimize** and select **Minimize** option as shown in Figure 191 on page 355 to minimize the Juniper Secure Connect as an icon that is displayed in the menu bar.

Figure 191: Minimize Menu Option

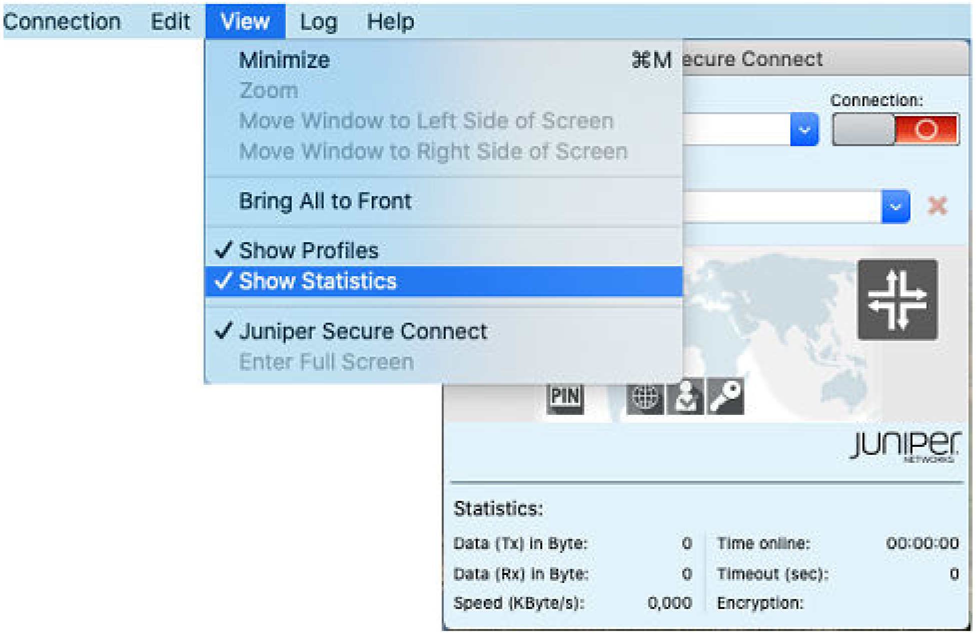


Statistics:

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

- Navigate to **View > Show Statistics** and select **Show Statistics** as shown in Figure 192 on page 355 to view or hide the statistics in the Juniper Secure Connect window.

Figure 192: Show Statistics Menu Option

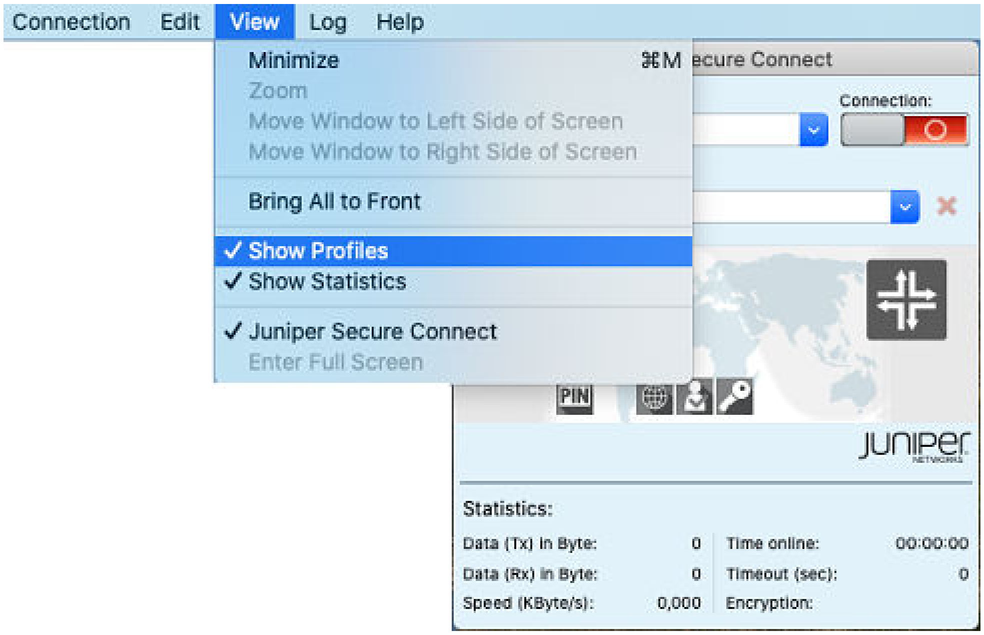


Statistics:

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

- Navigate to **View > Show Profiles** and select **Show Profiles** as shown in Figure 193 on page 356 to view or hide the profiles section in the Juniper Secure Connect window.

Figure 193: Show Profiles Menu Option



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:

Administrator can set parameter locks. Following are the purposes of parameter locks:

- Reduces the complexity of many configurations and provides simple appearance to the Juniper Secure Connect user interface. Parameter locks allows you to hide the features that are not used, so that you can view only the settings that are relevant to your working environment.

- Allows you to configure pre-settings. This avoids misconfigurations and undesired connection setups. In this case, after installation, you need to enter only the personal passwords to a establish connection.

You can unlock the parameter locks from the **Connection** menu. To do this, you must enter your user ID and password.

WHAT'S NEXT

For more information on Juniper Secure Connect GUI elements, see "Juniper Secure Connect GUI Elements" | 274.
For more information on Juniper Secure Connect features and how to configure the options, see "Connection Menu" | 347, "Log Menu" | 357, and "Help Menu" | 359.

Log Menu

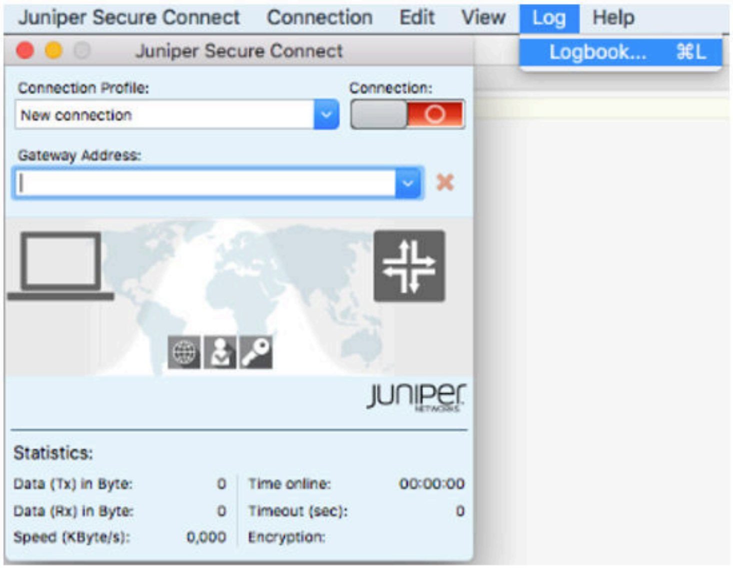
SUMMARY

Juniper Secure Connect **Log** menu provides option to log all the communication process.

IN THIS SECTION

Use the **Logbook** menu option to view the current log file or create a logbook. See Figure 194 on page 357.

Figure 194: Logbook Menu Option



Connection Profile: New connection

Connection:

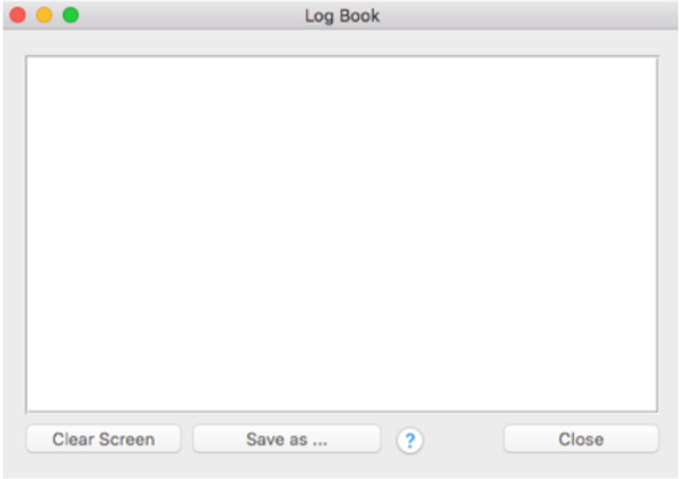
Gateway Address:

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:	

Figure 195 on page 358 shows an example of log messages for a VPN connection when **Logbook** option is selected from the **Log** menu.

Figure 195: Displays Log Messages



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 **Log** folder when the communication process is completed. The log file is named in **NCPyymmdd.LOG** format, where yy=year, mm=month, dd=date. You can change the storage time for log files in **Extended Log Settings** option. You can open and analyze the log files using a text editor.

Open the **Log** windows to view and follow the current log messages. In the log window, you can manually save or search for specific events.

Table 31 on page 358 lists options in the **Logbook** window.

Table 31: Logbook Options and Description

Logbook Option	Action
Clear Screen	Click this button to clear the log entries in the log window.
Save As	Click on this button to save the logs in a file. The default log file name is **ncpmon.log**. All transaction with the Juniper Secure Connect, such as dialing and reception, including the numbers, are written in this file until the file is closed. When you add log entries in a log file, you can follow the transactions with the Juniper Secure Connect for a longer period.
Close	Click this button to save the log entries in a file (any file name) and close the log window. You can use this file to analyze the transactions with Juniper Secure Connect or search for errors.

WHAT'S NEXT

For more information on Juniper Secure Connect GUI elements, see "Juniper Secure Connect GUI Elements" | 274.
For more information on Juniper Secure Connect features and how to configure the options, see "Connection Menu" | 347, "View Menu" | 354, and "Help Menu" | 359.

Help Menu

SUMMARY

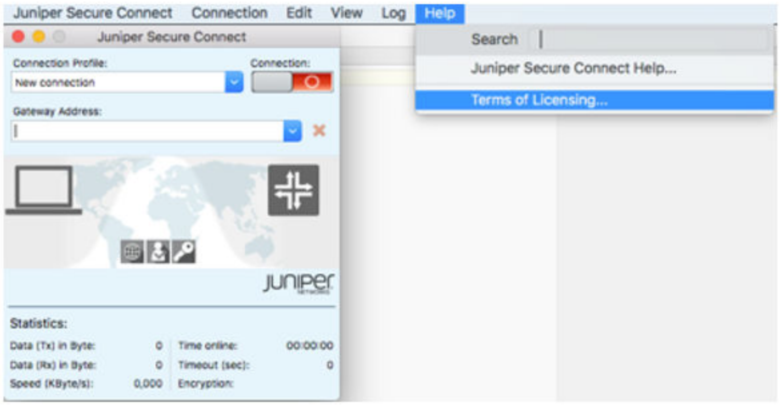
Juniper Secure Connect **Help** menu provides you the configuration tips to use the Juniper Secure Connect effectively.

IN THIS SECTION

The Juniper Secure Connect help provides you the help information for the menu options with configuration tips. If you need help while working with any particular configuration field during profile settings, press help button. The help page displays the functional descriptions for the configuration parameters.

If you want to see the license terms for the Juniper Secure Connect, navigate to **Help** > **Terms of Licensing** shown in Figure 196 on page 359.

Figure 196: Terms of Licensing 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:	

WHAT'S NEXT

For more information on Juniper Secure Connect GUI elements, see "Juniper Secure Connect GUI Elements" | **274**.

For more information on Juniper Secure Connect features and how to configure the options, see "Connection Menu" | **347**, "View Menu" | **354**, and "Log Menu" | **357**.

9

CHAPTER

Juniper Secure Connect for Android

SUMMARY

Learn about Juniper Secure Connect application for Android.

IN THIS CHAPTER

Juniper Secure Connect application is a client-based SSL VPN software that can run on Android device. It ensures that you securely access resources in your corporate network. To complete the setup of Juniper Secure Connect application, your system administrator must first configure remote access on the SRX Series Firewall. After the remote access is configured, you can connect to your secured corporate resources using the Juniper Secure Connect application.

Read the following topics to install and use Juniper Secure Connect application for Android:

- "Install Juniper Secure Connect on Android" on page 362
- "Connect Menu" on page 364
- "Statistics Menu" on page 366
- "Logbook Menu" on page 368
- "Import/Export Menu" on page 369
- "Reset PIN Menu" on page 373
- "General Settings Menu" on page 374
- "About Menu" on page 376

RELATED DOCUMENTATION

Get Started with Juniper Secure Connect | 10

Install Juniper Secure Connect on Android

SUMMARY

Learn about step-by-step procedures on how to install Juniper Secure Connect on Android platform.

IN THIS SECTION

- Manual Installation of Juniper Secure Connect | 363

What's Next

Download the Juniper Secure Connect application software from here. See release notes for more details.

For more information on Juniper Secure Connect features and how to configure the options, see "Connect Menu" on page 364, "Statistics Menu" on page 366, "Logbook Menu" on page 368, "Import/ Export Menu" on page 369, "Reset PIN Menu" on page 373, "General Settings Menu" on page 374, and "About Menu" on page 376.

Manual Installation of Juniper Secure Connect

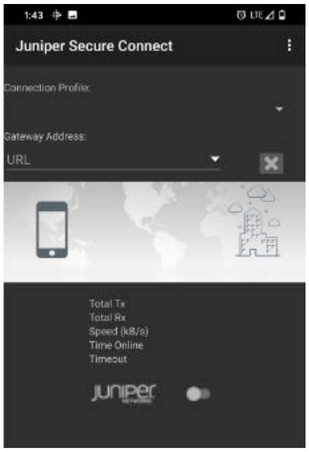
You can install Juniper Secure Connect only from **Google Play Store**. Install the Juniper Secure Connect application on your android device from Google Play Store.

Launch the Juniper Secure Connect and enter the **Gateway Address** URL to connect with the SRX Series Firewall. Figure 197 on page 363 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.example.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 197: Connect to SRX Series Firewalls using Gateway Address



To import user or CA certificates, see "Import/Export Menu" on page 369.

Connect Menu

SUMMARY

Juniper Secure Connect **Connect** menu allows you to establish remote access connection.

IN THIS SECTION

Following are the steps to establish a secure VPN connection with Juniper Secure Connect:

1. You must first define and select a profile to establish a connection for that profile. To do so, click on **Connection Profile** drop down and select the profile from the list of connections.

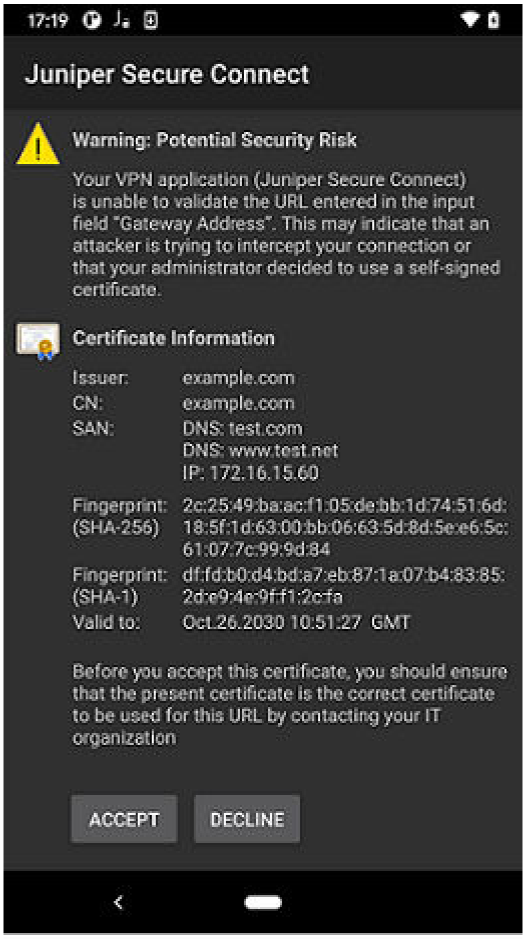
2. Enter the URL or select the URL from the drop down list for the SRX Series Firewalls in the **Gateway Address**.

3. Click on the three vertical dots at the top right corner and select **Connection** as shown in Figure 199 on page 366 to establish connection manually to the destination system.

   > **WARNING**: If the following the warning message is displayed, your application is missing the CA certificate from the VPN gateway (SRX Series Firewall). If you are a remote user, contact your IT organization for appropriate action. If you are a system administrator, place the cacerts in the respective location for the platform.

   Figure 198 on page 365 is a sample warning message on Android platform that is displayed when CA certificate is not present.

Figure 198: Sample Certificate Warning Message on Android Platform



Warning: Potential Security Risk

Your VPN application (Juniper Secure Connect) is unable to validate the URL entered in the input field "Gateway Address". This may indicate that an attacker is trying to intercept your connection or that your administrator decided to use a self-signed certificate.

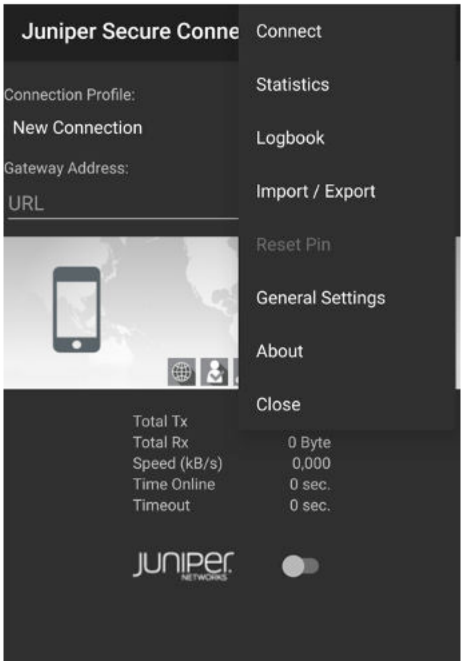
Certificate Information

Issuer:	example.com
CN:	example.com
SAN:	DNS: test.com DNS: www.test.net IP: 172.16.15.60
Fingerprint: (SHA-256)	2c:25:49:ba:ac:f1:05:de:bb:1d:74:51:6d:18:5f:1d:63:00:bb:06:63:5d:8d:5e:e6:5c:61:07:7c:99:9d:84
Fingerprint: (SHA-1)	df:fd:b0:d4:bd:a7:eb:87:1a:07:b4:83:85:2d:e9:4e:9f:f1:2c:fa
Valid to:	Oct.26.2030 10:51:27 GMT

Before you accept this certificate, you should ensure that the present certificate is the correct certificate to be used for this URL by contacting your IT organization

4. To disconnect the existing connection, navigate to **Connection > Disconnect**, or use the **Connection** toggle button.

Figure 199: Juniper Secure Connect Menu Options



Connection Profile:
New Connection

Gateway Address:
URL

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

WHAT'S NEXT

For more information on Juniper Secure Connect features and how to configure the options, see "Statistics Menu" | 366, "Logbook Menu" | 368, "Import/Export Menu" | 369, "Reset PIN Menu" | 373, "General Settings Menu" | 374, and "About Menu" | 376.

Statistics Menu

SUMMARY

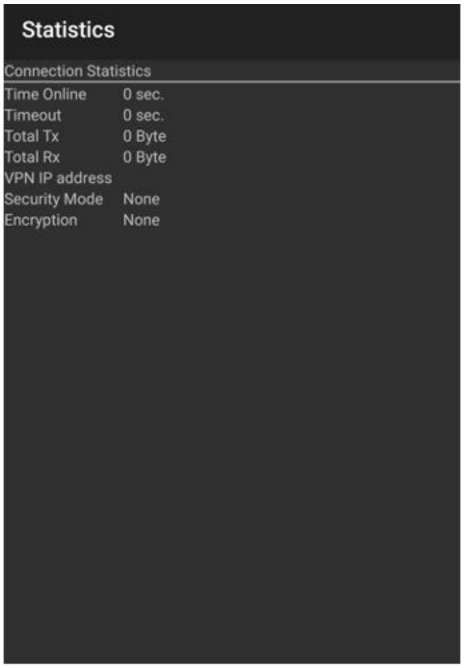
Juniper Secure Connect **Statistics** menu allows you to view the connection statistics information.

IN THIS SECTION

Click on the three vertical dots at the top right corner and select **Statistics** to view the following statistics information:

Figure 200 on page 367 shows a example for connection statistics details for a VPN connection.

Figure 200: Connection Statistics Details



Statistics

Connection Statistics

Time Online	0 sec.
Timeout	0 sec.
Total Tx	0 Byte
Total Rx	0 Byte
VPN IP address	
Security Mode	None
Encryption	None

Table 32 on page 367 summarizes the fields in connections statistics.

Table 32: Connection Statistics

Statistics	Description
Time online	Shows the time a user has been connected with the same connection profile. Restarting the Juniper Secure Connect or changing the connection profile resets this value.
Total Tx	Shows the data sent or transmitted over the VPN tunnel into the remote network while being connected to the same connection profile. Restarting the Juniper Secure Connect or changing the connection profile resets this value.
Total Rx	Shows the data received over the VPN tunnel into the remote network while being connected to the same connection profile. Restarting the Juniper Secure Connect or changing the connection profile resets this value.
Timeout	This value shows `0 sec`, if no timeout for the VPN session is used. If a timeout is used, the timeout shows the amount of seconds. The Juniper Secure Connect starts count down for the timeout as soon as no data is received over the VPN tunnel and resets as soon as data is received of the VPN tunnel.

Table 32: Connection Statistics *(Continued)*

Statistics	Description
VPN IP address	Shows the private IP address of Juniper Secure Connect.
Security Mode	Shows IPsec information.

WHAT'S NEXT

For more information on Juniper Secure Connect features and how to configure the options, see "Connect Menu" | 364, "Logbook Menu" | 368, "Import/Export Menu" | 369, "Reset PIN Menu" | 373, "General Settings Menu" | 374, and "About Menu" | 376.

Logbook Menu

SUMMARY

Juniper Secure Connect **Logbook** menu provides option to log all the communication process.

IN THIS SECTION

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. Navigate to **Import/Export > Export Data > Export Log Files** to export the log file that is generated automatically. The logs are stored exported to **/Juniper/Export** directory location. The name of the log is displayed during the export process. You can open the log files and analyze with a text editor.

WHAT'S NEXT

For more information on Juniper Secure Connect features and how to configure the options, see "Connect Menu" | 364, "Statistics Menu" | 366, "Import/Export Menu" | 369, "Reset PIN Menu" | 373, "General Settings Menu" | 374, and "About Menu" | 376.

Import/Export Menu

SUMMARY

Juniper Secure Connect **Import/Export** menu allows you to import certificate files and export logs and configuration files.

IN THIS SECTION

WHAT'S NEXT

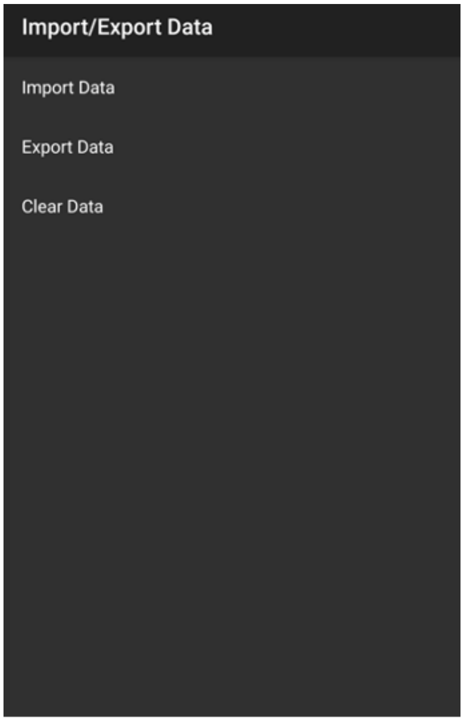
For more information on Juniper Secure Connect features and how to configure the options, see "Connect Menu" | **364**, "Statistics Menu" | **366**, "Logbook Menu" | **368**, "Reset PIN Menu" | **373**, "General Settings Menu" | **374**, and "About Menu" | **376**.

Import Data Menu Option

Certification Authority (CA) (also referred as the Issuer) creates and issues certificates using a PKI manager (software) and stores as a soft certificate. User certificates are stored as a **PKCS#12** file in the installation path.

The **Import/Export Data** window enables you to import or export data. See Figure 201 on page 370.

Figure 201: Import/Export Data Options



Import/Export Data

Import Data

Export Data

Clear Data

Table 33 on page 370 summarizes the import options in Juniper Secure Connect.

Table 33: Import User or CA Certificates

Import/Delete Certificates	Action
Import User Certificates	Follow these steps to import the user certificates: 1. Click on the three vertical dots at the top right corner and select **Import/Export Data > Import Data > Import User Certificates** to import the user certificates to Juniper Secure Connect application. 2. Rename the file as **user.p12** and save the file in **/Juniper/Import/** directory. Based on the Android version and Juniper Secure Connect Application, the absolute path for the import might change. For example, in Android 11 and later, the import directory is **/storage/emulated/0/Android/data/de.juniper.vpn.secureconnect/files/Juniper/Import**

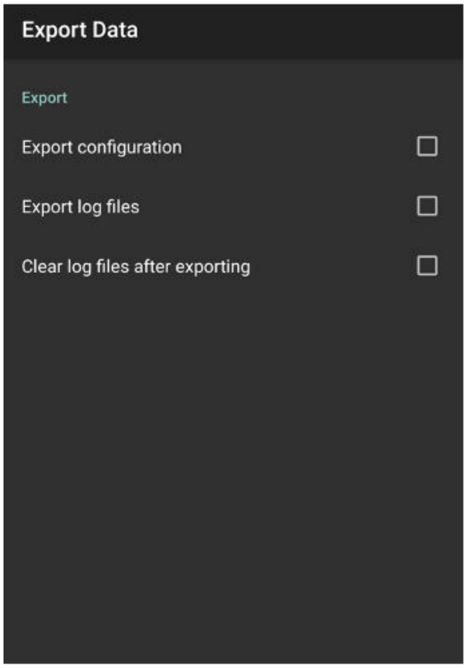
Table 33: Import User or CA Certificates *(Continued)*

Import/Delete Certificates	Action
Import CA Certificates	Follow these steps to import the CA certificates: 1. Click on the three vertical dots at the top right corner and select **Import/Export Data > Import Data > Import CA Certificates** to import CA certificates to the Juniper Secure Connect application. 2. You must save the CA certificates in **/Juniper/Import/** path. Juniper Secure Connect supports ***.pem** and ***.crt** formats for CA certificates. Based on the Android version and Juniper Secure Connect Application, the absolute path for the import might change. For example, in Android 11 and later, the import directory is **/storage/emulated/0/Android/data/de.juniper.vpn.secureconnect/files/Juniper/Import**
Delete after import	Select the toggle button to remove the files from the file system after the files have been imported.

Export Data Menu Option

The **Import/Export Data** window enables you to export data. Figure 202 on page 372 shows an example of the list of files that you can select to import.

Figure 202: Export Data Options



Export Data

Export

Export configuration □

Export log files □

Clear log files after exporting □

Table 34 on page 372 summarizes the export options in Juniper Secure Connect.

Table 34: Export Data

Export Certificates and Log Files	Action
Export configuration	Select the check box to export the configuration file to the file system. The configuration file is exported to **/Juniper/Export/** directory. The name of the file is displayed during the export process. Based on the Android version and Juniper Secure Connect Application, the absolute path for the export might change. For example, in Android 11 and later, the export directory is **/storage/emulated/0/Android/data/de.juniper.vpn.secureconnect/files/Juniper/Export**

Table 34: Export Data *(Continued)*

Export Certificates and Log Files	Action
Export log files	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. Follow these steps to export the log files: 1. Click on the three vertical dots at the top right corner and select **Import/Export Data** > **Export Data**. Select the **Export log files** check box to export the logs to the file system. 2. The logs are exported to **/Juniper/Export** directory. The name of the log file is displayed during the export process. Based on the Android version and Juniper Secure Connect Application, the absolute path for the export might change. For example, in Android 11 and later, the export directory is **/storage/emulated/0/Android/data/de.juniper.vpn.secureconnect/files/Juniper/Export**
Clear logs after exporting	Select the check box to remove the files from the file system after the files have been imported.

Reset PIN Menu

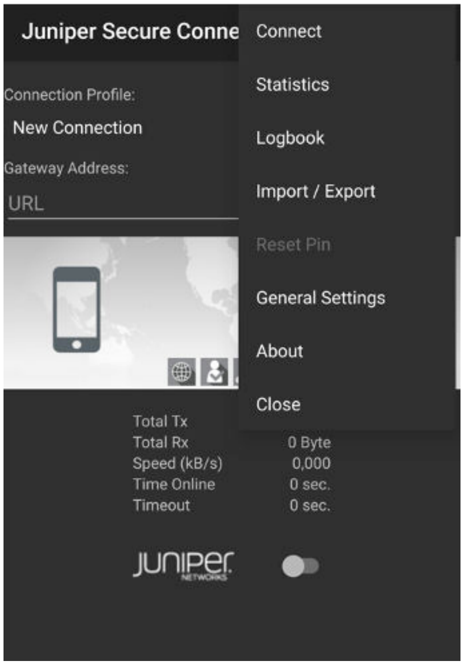
SUMMARY

Juniper Secure Connect **Reset PIN** menu allows you to reset your PIN.

IN THIS SECTION

Click on the three vertical dots at the top right corner and select **Reset PIN** to reset your PIN. This menu item is active only when the PIN has been entered correctly, that is, the certificate is used for the connection to be established. See Figure 203 on page 374. If the PIN is reset, this certificate can no longer be used to establish a connection, until the correct PIN is entered again.

Figure 203: Juniper Secure Connect Menu Options



WHAT'S NEXT

For more information on Juniper Secure Connect features and how to configure the options, see "Connect Menu" | 364, "Statistics Menu" | 366, "Logbook Menu" | 368, "Import/Export Menu" | 369, "General Settings Menu" | 374, and "About Menu" | 376.

General Settings Menu

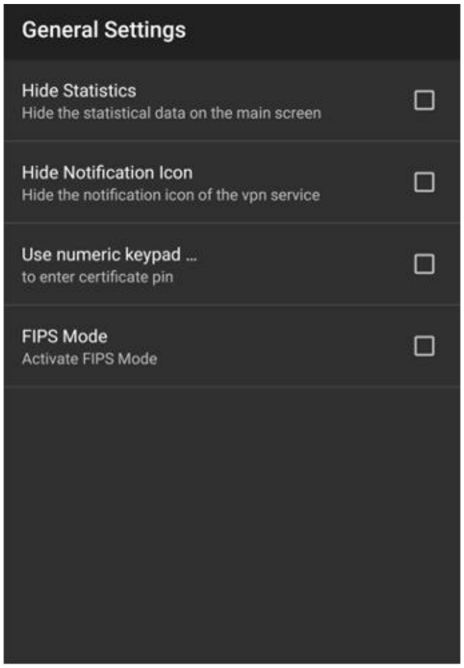
SUMMARY

Juniper Secure Connect **General Settings** menu allows you to configure general settings for the application.

IN THIS SECTION

Click on the three vertical dots at the top right corner and select **General Settings** to configure some general settings options in Juniper Secure Connect. See Figure 204 on page 375.

Figure 204: General Settings Options



General Settings

Hide Statistics □
Hide the statistical data on the main screen

Hide Notification Icon □
Hide the notification icon of the vpn service

Use numeric keypad ... □
to enter certificate pin

FIPS Mode □
Activate FIPS Mode

Table 35 on page 375 summarizes the general settings options in Juniper Secure Connect.

Table 35: General Settings Options

General Settings	Action
Hide Statistic	Select the check box to hide the statistical data on the main screen.
Hide Notification Icon	Select the check box to hide the notification icon of the Juniper Secure Connect.
Use numeric keypad	Select the check box to use a numeric keypad by default to enter the PIN for the user certificate.

Table 35: General Settings Options *(Continued)*

General Settings	Action
FIPS Mode	Select the check box to use FIPS certified encryption libraries. The IPsec Client incorporates cryptographic algorithms conformance to the FIPS standard 140-2. The embedded cryptographic algorithms has been validated with certificate #1747. FIPS conformance are maintained when the following algorithms are used for establishment and encryption of the IPsec connection: • Diffie Hellman Group: Group 2 to 14 (DH length of 1024 bits up to 2048 bits) • Hash Algorithms: SHA1, SHA 256, SHA 384, or SHA 512 Bit • Encryption Algorithms: AES with 128, 192 or 256 Bit or Triple DES You can configure the **IPsec settings** in SRX Series Firewalls. **NOTE**: The SRX Series Firewall and the Juniper Secure Connect application are independent FIPS compliant products. For remote access VPN solution on FIPS evaluated SRX Series Firewall, see Juniper Secure Connect.

WHAT'S NEXT

For more information on Juniper Secure Connect features and how to configure the options, see "Connect Menu" | **364**, "Statistics Menu" | **366**, "Logbook Menu" | **368**, "Import/Export Menu" | **369**, "Reset PIN Menu" | **373**, and "About Menu" | **376**.

About Menu

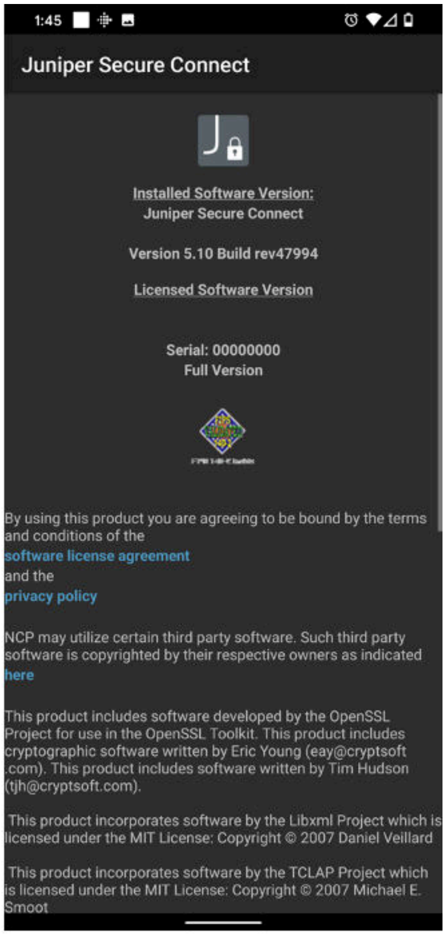
SUMMARY

Juniper Secure Connect **About** menu provides the version and license information for the application.

IN THIS SECTION

Click on the three vertical dots at the top right corner and select **About** to know the Juniper Secure Connect product label and version number details as shown in Figure 205 on page 377.

Figure 205: Displays Juniper Secure Connect Version Information



Installed Software Version:
Juniper Secure Connect

Version 5.10 Build rev47994

Licensed Software Version

Serial: 00000000
Full Version

By using this product you are agreeing to be bound by the terms and conditions of the
software license agreement
and the
privacy policy

NCP may utilize certain third party software. Such third party software is copyrighted by their respective owners as indicated
here

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product incorporates software by the Libxml Project which is licensed under the MIT License: Copyright © 2007 Daniel Veillard

This product incorporates software by the TCLAP Project which is licensed under the MIT License: Copyright © 2007 Michael E. Smoot

WHAT'S NEXT

For more information on Juniper Secure Connect features and how to configure the options, see "Connect Menu" | 364, "Statistics Menu" | 366, "Logbook Menu" | 368, "Import/Export Menu" | 369, "Reset PIN Menu" | 373, and "General Settings Menu" | 374.

10

CHAPTER

Juniper Secure Connect for iOS

SUMMARY

Learn about Juniper Secure Connect application for iOS.

IN THIS CHAPTER

Juniper Secure Connect application is a client-based SSL VPN software that can run on macOS. It ensures that you securely access resources in your corporate network. To complete the setup of Juniper Secure Connect application, your system administrator must first configure remote access on the SRX Series Firewall. After the remote access is configured, you can connect to your secured corporate resources using the Juniper Secure Connect application.

Read the following topics to install and use Juniper Secure Connect application for macOS:

- "Install Juniper Secure Connect on iOS" on page 379
- "Diagnostics Menu" on page 387
- "Info Menu" on page 399

RELATED DOCUMENTATION

Get Started with Juniper Secure Connect | 10

Install Juniper Secure Connect on iOS

SUMMARY

Learn about step-by-step procedures on how to install Juniper Secure Connect on iOS platform.

IN THIS SECTION

What's Next

Download the Juniper Secure Connect application software from here. See release notes for more details.

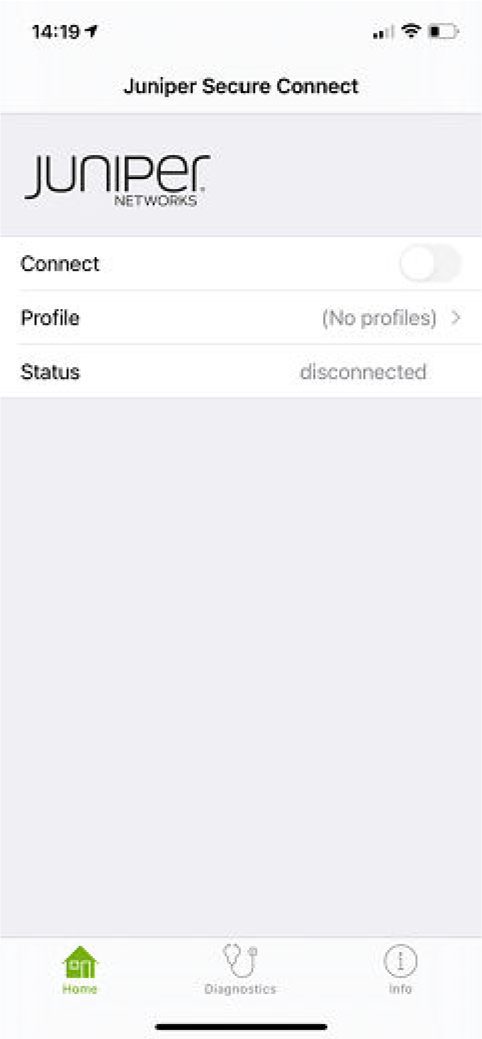
For more information on Juniper Secure Connect features and how to configure the options, see "Diagnostics Menu" on page 387 and "Info Menu" on page 399.

Manual Installation of Juniper Secure Connect

Install the Juniper Secure Connect application from **App Store**.

1. Install the Juniper Secure Connect application on your iPhone device from **App Store**. Figure 206 on page 380 shows the Juniper Secure Connect home screen.

   Figure 206: Juniper Secure Connect Home Screen

   14:19

   Juniper Secure Connect

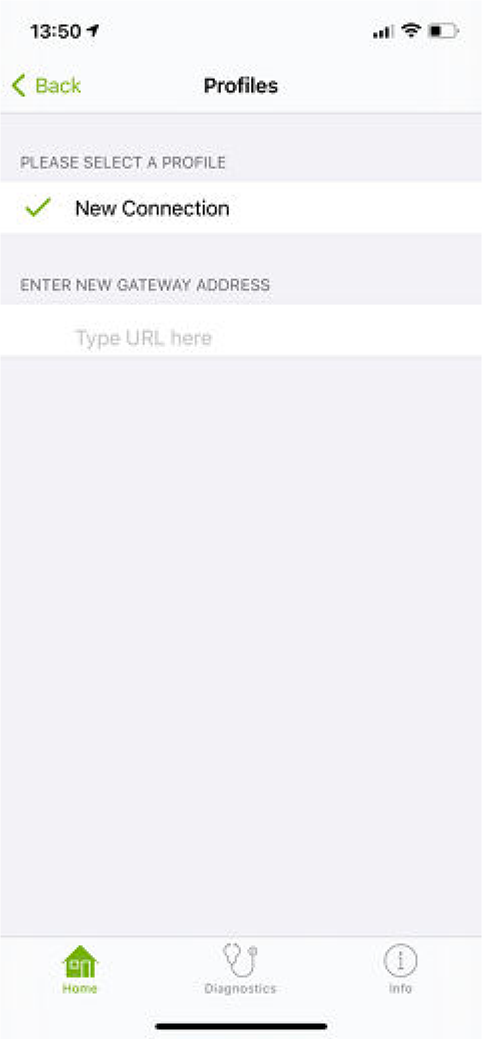
   Connect

   Profile (No profiles)

   Status disconnected

2. Launch the Juniper Secure Connect Application and select **Profile** from the application home screen as shown in Figure 207 on page 381.

Figure 207: Profiles Page



13:50

Back

Profiles

PLEASE SELECT A PROFILE

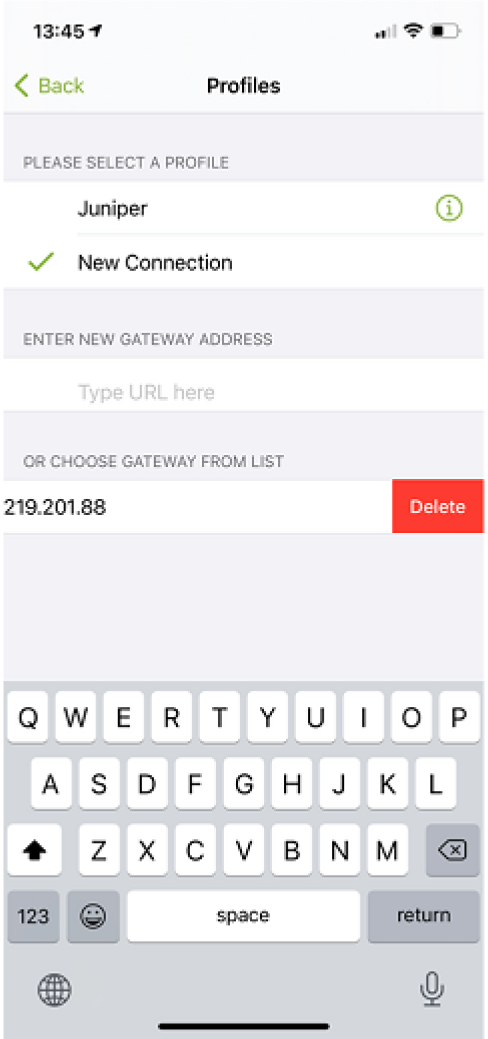
✓ New Connection

ENTER NEW GATEWAY ADDRESS

Type URL here

Figure 208 on page 382, Figure 209 on page 383, and Figure 210 on page 384 shows an example for selecting, adding, or deleting a gateway address for the new connection.

Figure 208: Select Gateway Address from the List



13:45

Back

Profiles

PLEASE SELECT A PROFILE

Juniper

✓ New Connection

ENTER NEW GATEWAY ADDRESS

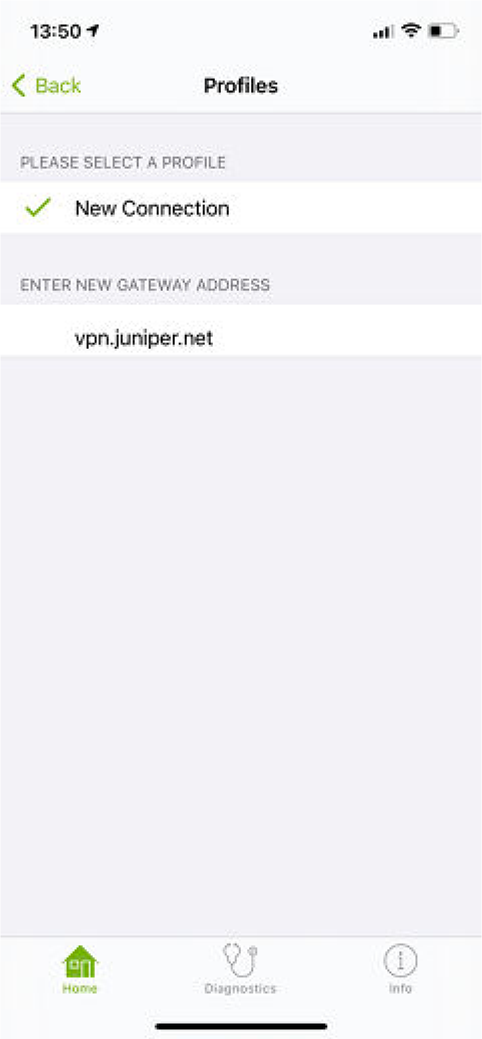
Type URL here

OR CHOOSE GATEWAY FROM LIST

219.201.88

Click on **New Connection** to enter the gateway IP address or URL to connect with the SRX Series Firewall. Figure 209 on page 383 shows an example to enter the gateway address to the SRX Series Firewall.

Figure 209: Enter New Gateway Address



PLEASE SELECT A PROFILE

✓ New Connection

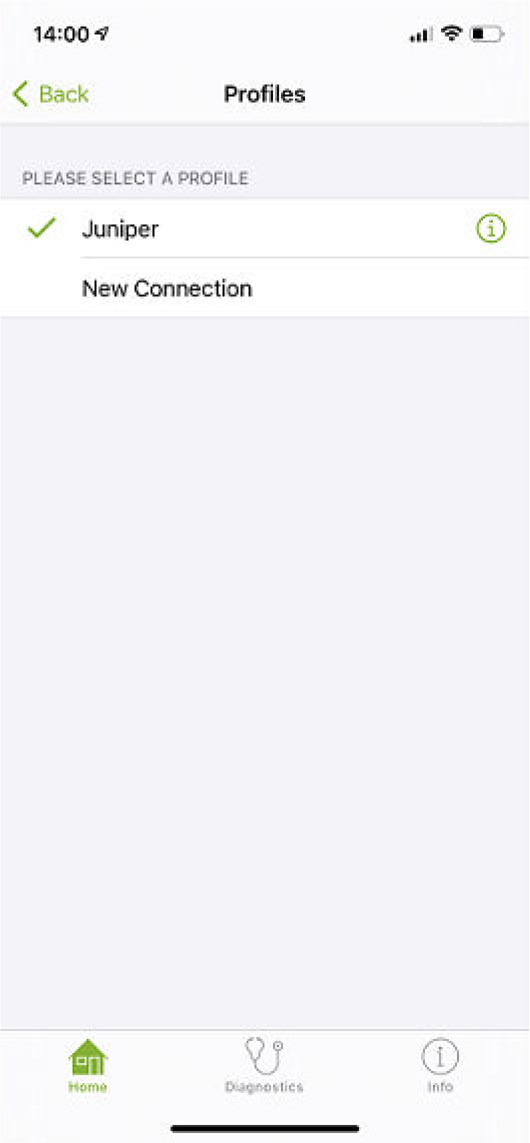
ENTER NEW GATEWAY ADDRESS

vpn.juniper.net

After entering the gateway address, click the **Back** button at the bottom.

NOTE: In the **Profiles** page, you can remove the profile name if you want. For example, if you want to remove the profile name 'Juniper' in the **Profile** page as shown in Figure 210 on page 384, navigate to iOS **Settings** > **General** > **VPN**.

Figure 210: Remove 'Juniper' Profile Name



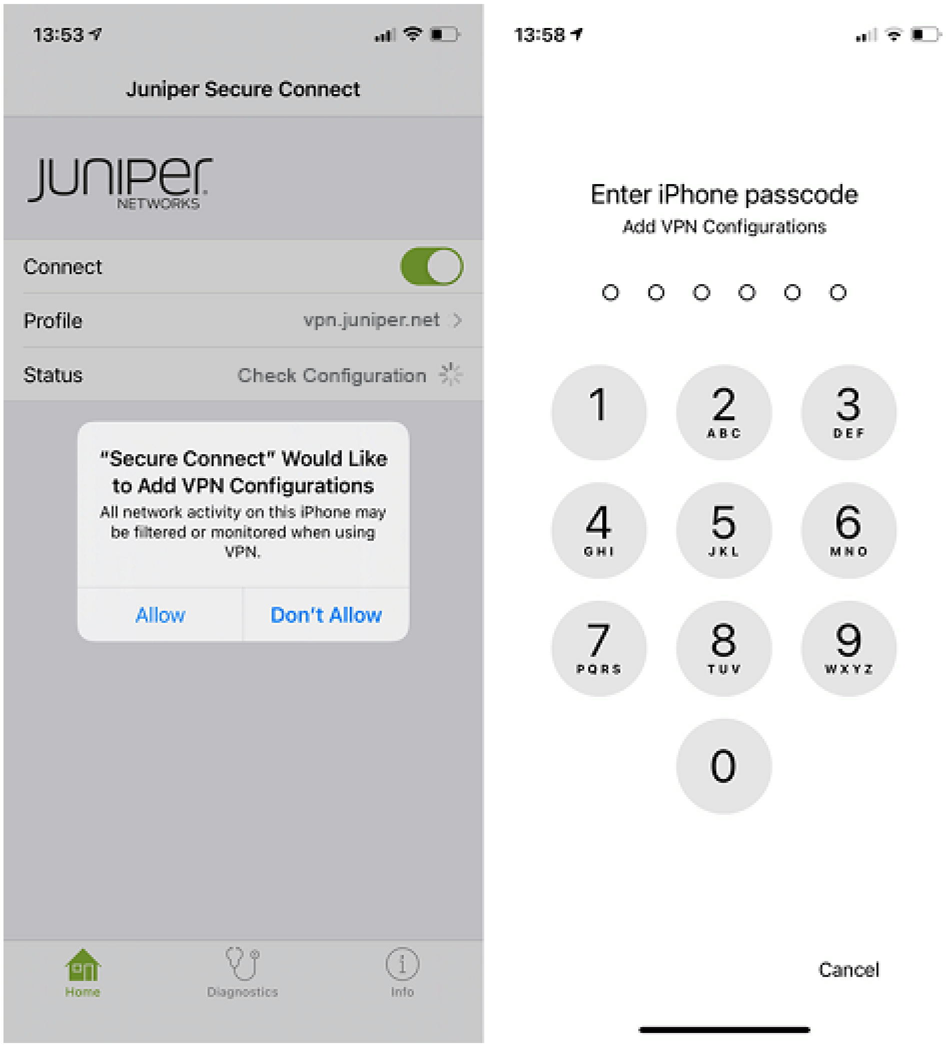
PLEASE SELECT A PROFILE

✓ Juniper

New Connection

3. Toggle the **Connect** button to establish connection as shown in Figure 211 on page 385. When you connect for the first time to a new gateway or profile, you need to allow the addition of the downloaded VPN configuration. If your device is password protected, you must enter the password.

Figure 211: Enable Connect to Establish VPN Connection



13:53

Juniper Secure Connect

Connect

Profile vpn.juniper.net

Status Check Configuration

"Secure Connect" Would Like to Add VPN Configurations

All network activity on this iPhone may be filtered or monitored when using VPN.

13:58

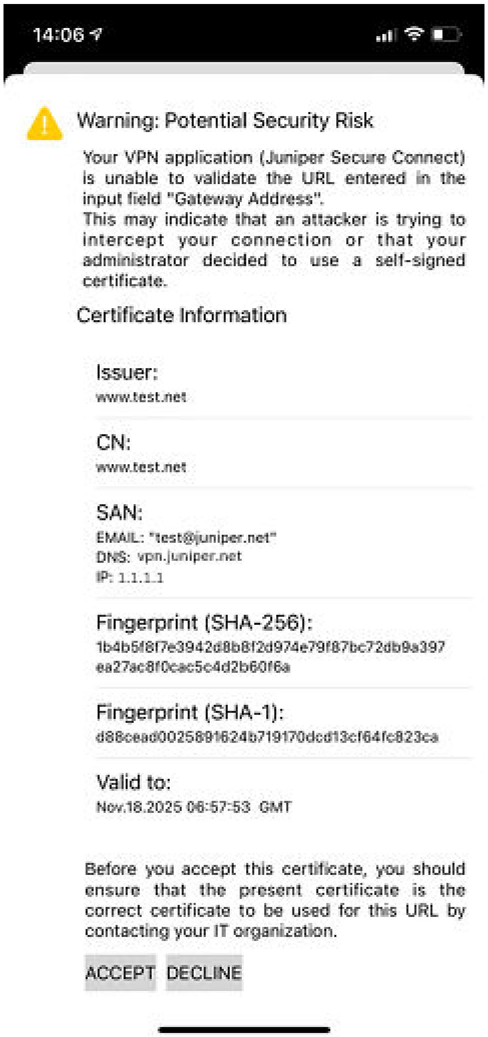
Enter iPhone passcode

Add VPN Configurations

If your device is missing a CA certificate for the SRX Series Firewall, a warning message is displayed. You can prevent this, if you install a CA certificate into the Juniper Secure Connect directory location of the device. To import user or CA certificates, see "Certificates Import Menu Option" on page 397.

WARNING: If the following warning message as shown in Figure 212 on page 386 is displayed, your application is missing the CA certificate from the VPN gateway (SRX Series Firewall). If you are a remote user, contact your IT organization for appropriate action.

Figure 212: Sample Certificate Warning Message on iOS Platform



Warning: Potential Security Risk

Your VPN application (Juniper Secure Connect) is unable to validate the URL entered in the input field "Gateway Address".
This may indicate that an attacker is trying to intercept your connection or that your administrator decided to use a self-signed certificate.

Certificate Information

Issuer:
www.test.net

CN:
www.test.net

SAN:
EMAIL: "test@juniper.net"
DNS: vpn.juniper.net
IP: 1.1.1.1

Fingerprint (SHA-256):
1b4b5f8f7e3942d8b8f2d974e79f87bc72db9a397
ea27ac8f0cac5c4d2b60f6a

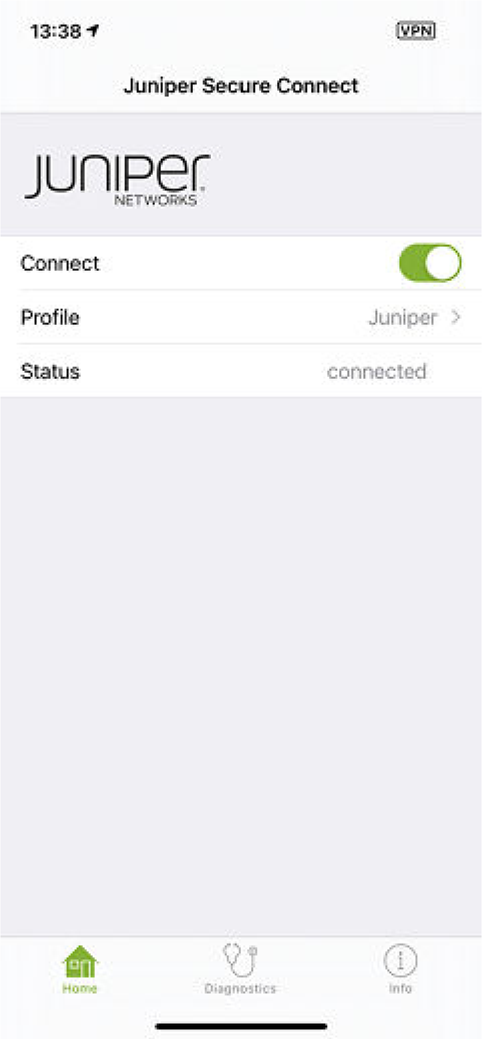
Fingerprint (SHA-1):
d88cead0025891624b719170dcd13cf64fc823ca

Valid to:
Nov.18.2025 06:57:53 GMT

Before you accept this certificate, you should ensure that the present certificate is the correct certificate to be used for this URL by contacting your IT organization.

When the connection is established successfully, the **Status** of the connection changes to **connected** as shown in Figure 213 on page 387.

Figure 213: VPN Connection Established Successfully



Connect

Profile Juniper >

Status connected

Diagnostics Menu

SUMMARY

Juniper Secure Connect Diagnostics menu provides you various options to troubleshoot your VPN connection.

IN THIS SECTION

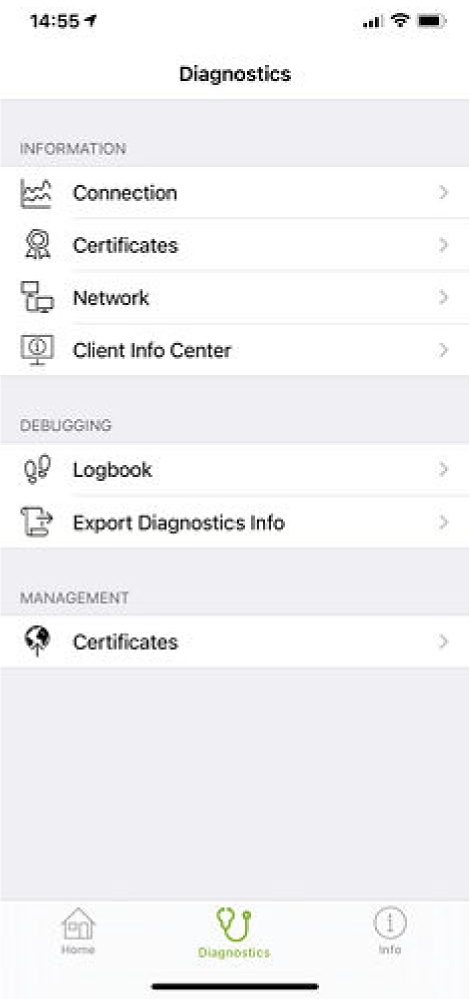
WHAT'S NEXT

For more information about Juniper Secure Connect features and how to configure the options, see "Info Menu" | 399.

Diagnostics Menu Page

The **Diagnostics** page contains options related to troubleshooting as shown in Figure 214 on page 389.

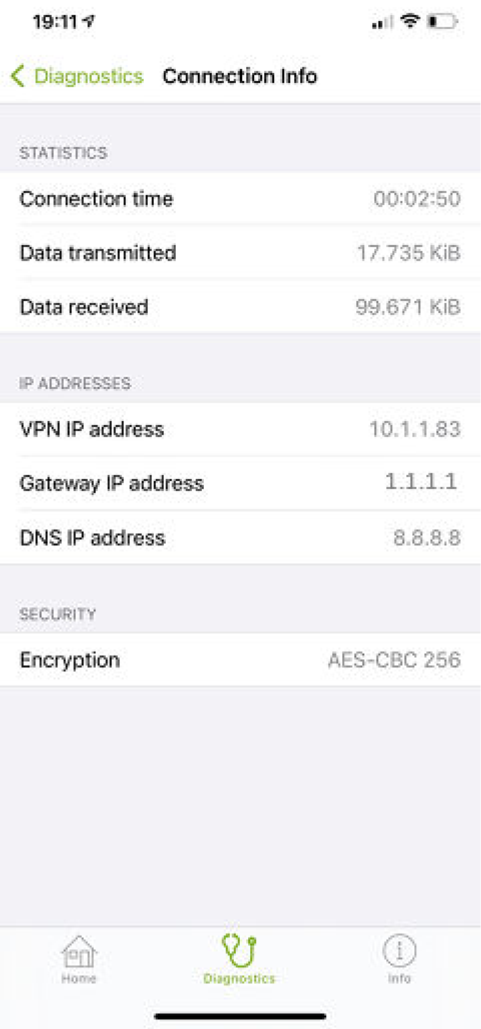
Figure 214: Diagnostics Page



Connection Menu Option

To get the information related to current connection, choose **Diagnostics** > **Information** > **Connection** menu option. Figure 215 on page 390 shows an example of connection related information for a VPN connection.

Figure 215: Current VPN Connection Information



19:11

Diagnostics Connection Info

STATISTICS

Connection time 00:02:50

Data transmitted 17.735 KiB

Data received 99.671 KiB

IP ADDRESSES

VPN IP address 10.1.1.83

Gateway IP address 1.1.1.1

DNS IP address 8.8.8.8

SECURITY

Encryption AES-CBC 256

Table 36 on page 390 shows the statistics, IP address, and security related information that Juniper Secure Connect displays about the current connection.

Table 36: Connection Related information

Connection Information	Description
Statistics	
Connection time	Shows the time duration for which a user is connected with the same connection profile. Restarting the Juniper Secure Connect or changing the connection profile resets this value.

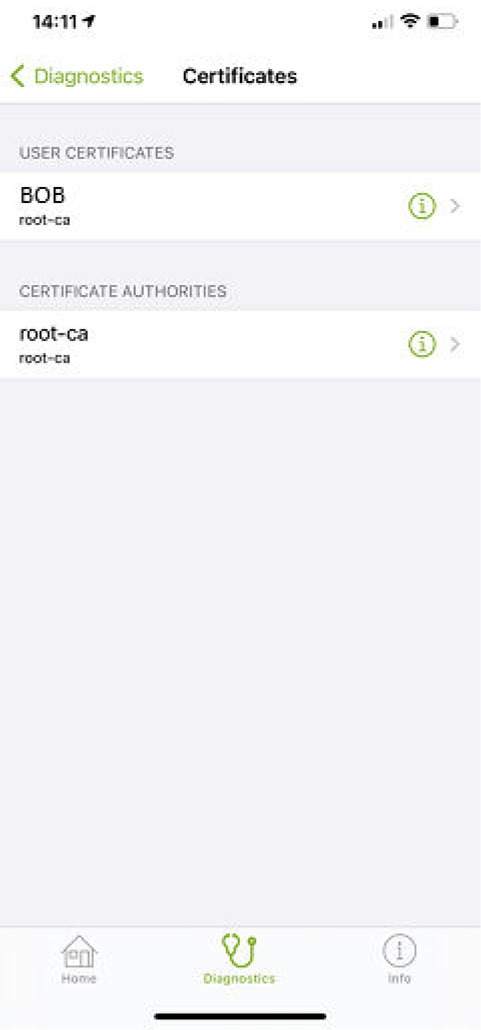
Table 36: Connection Related information *(Continued)*

Connection Information	Description
Data transmitted	Shows the data sent or transmitted over the VPN tunnel into the remote network while being connected to the same connection profile. Restarting the Juniper Secure Connect or changing the connection profile resets this value.
Data received	Shows the data received over the VPN tunnel into the remote network while being connected to the same connection profile. Restarting the Juniper Secure Connect or changing the connection profile resets this value.
IP addresses	
VPN IP address	Shows the private IP address of Juniper Secure Connect application.
Gateway IP address	Shows the gateway IP address of Juniper SRX Series Firewall.
DNS IP address	Shows the DNS IP address for Juniper Secure Connect application.
Security	
Encryption	Shows the encryption algorithm.

Certificates Menu Option

To get the information related to the certificates for the current connection, choose **Diagnostics > Information > Certificates** menu option. Figure 216 on page 392 shows a sample imported certificate profile. Click on each certificate for more details of the certificate.

Figure 216: Sample Page for Imported Certificate Profiles



USER CERTIFICATES

BOB
root-ca

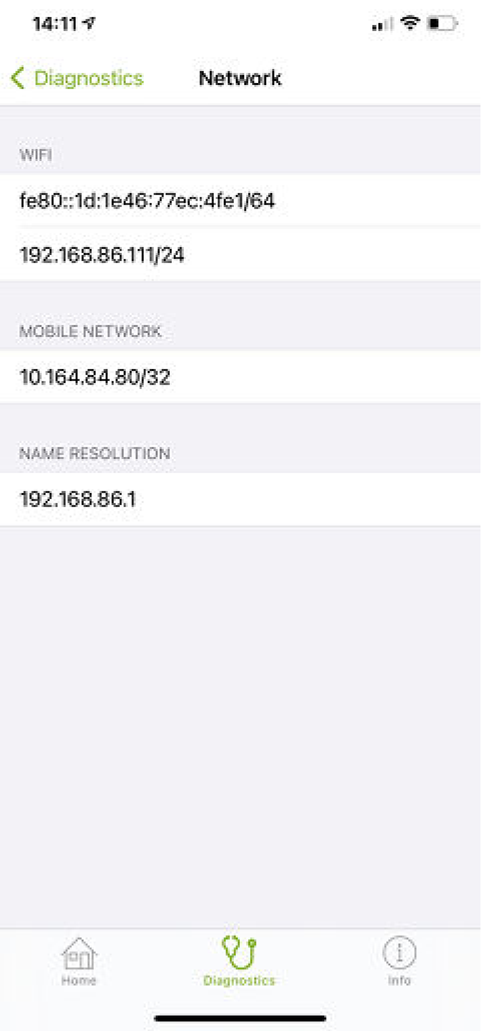
CERTIFICATE AUTHORITIES

root-ca
root-ca

Network Menu Option

To get the network parameters for the network your iOS device is connected with, choose **Diagnostics > Information > Network** menu option. Figure 217 on page 393 shows a sample network information of an iOS device.

Figure 217: Network Information



WIFI

fe80::1d:1e46:77ec:4fe1/64

192.168.86.111/24

MOBILE NETWORK

10.164.84.80/32

NAME RESOLUTION

192.168.86.1

Table 37 on page 393 shows the list of network parameters for an iOS device.

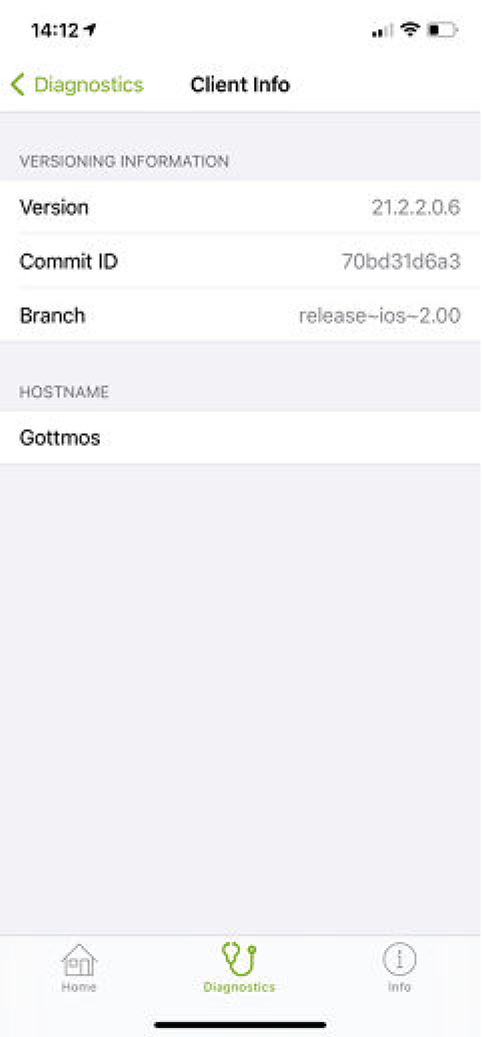
Table 37: Network Parameters

Network Parameter	Description
WiFi	Shows the IP addresses assigned in the current connected WiFi network.
Mobile network	Shows the IP addresses assigned in the current connected mobile network.
Name resolution	Shows the DNS servers assigned in the current connected network.

Client Info Center Menu Option

To get the information related to version information and hostname of your iOS device, choose **Diagnostics > Information > Client Info Center** menu option. Figure 218 on page 394 shows a sample device information of an iOS device.

Figure 218: Device Related Information



14:12

< Diagnostics Client Info

VERSIONING INFORMATION

Version 21.2.2.0.6

Commit ID 70bd31d6a3

Branch release-ios-2.00

HOSTNAME

Gottmos

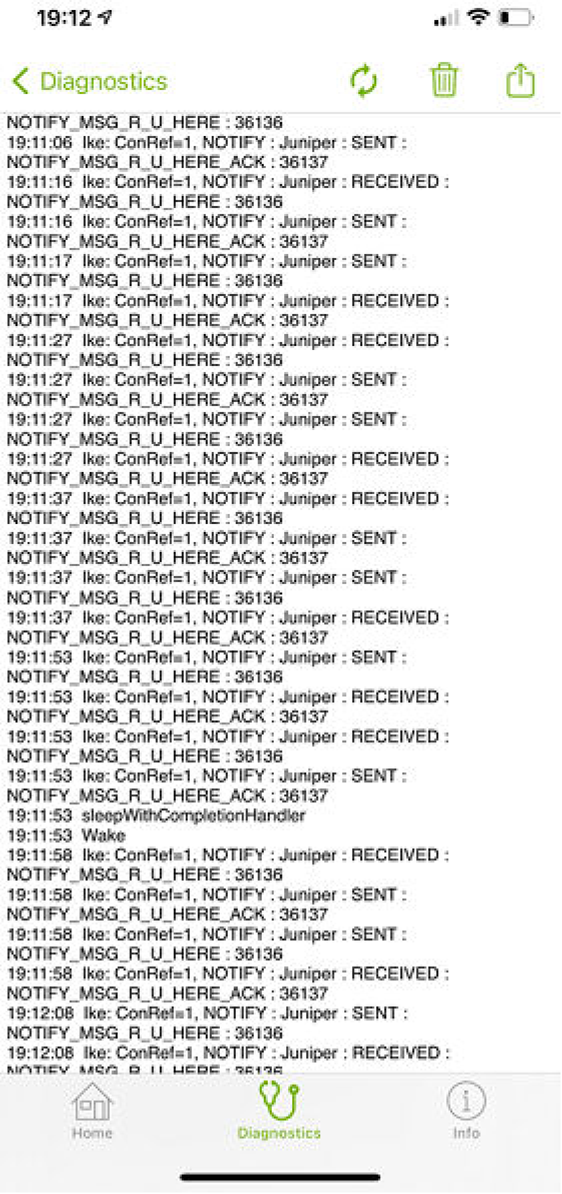
Error Log Menu Option

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 219 on page 395 shows a sample log message for an active VPN connection.

Figure 219: Log Messages



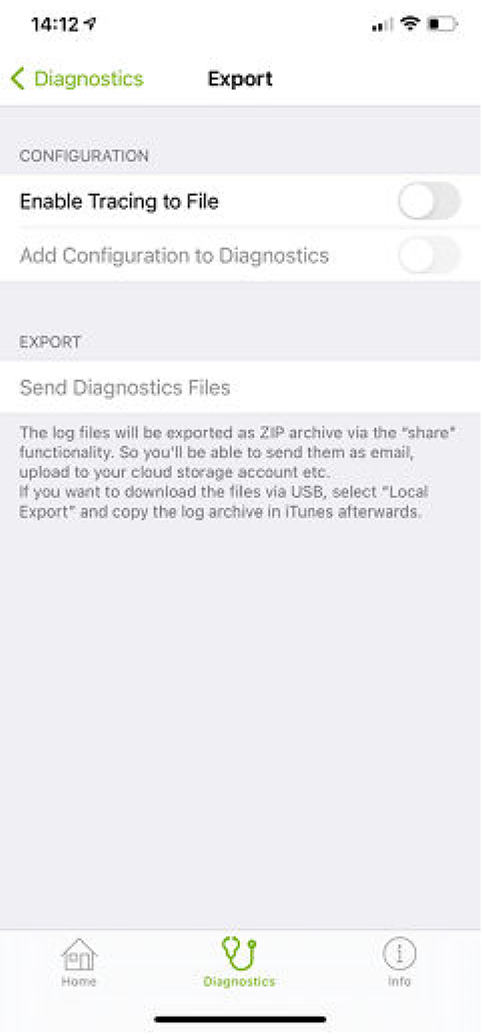
```
NOTIFY_MSG_R_U_HERE : 36136
19:11:06  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:11:16  Ike: ConRef=1, NOTIFY : Juniper : RECEIVED :
NOTIFY_MSG_R_U_HERE : 36136
19:11:16  Ike: ConRef=1, NOTIFY : Juniper : SENT :
NOTIFY_MSG_R_U_HERE_ACK : 36137
19:11:17  Ike: ConRef=1, 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
```

Export Diagnostics Info Menu Option

Navigate to **Diagnostics** > **Debugging** > **Export Diagnostics Info** menu option to archive and send the log file to the administrator through an e-mail or upload to your cloud storage, and so on. Optionally you can also add the configuration file generated on the device to your administrator along with the log file.

Figure 220 on page 396 shows a sample Export page.

Figure 220: Export Diagnostics Information



Enable Tracing to File ○

Add Configuration to Diagnostics ○

The log files will be exported as ZIP archive via the "share" functionality. So you'll be able to send them as email, upload to your cloud storage account etc.
If you want to download the files via USB, select "Local Export" and copy the log archive in iTunes afterwards.

Certificates Import Menu Option

Certification Authority (CA) (also referred as the Issuer) creates and issues certificates using a PKI manager (software) and stores as a soft certificate. User certificates are stored as a **PKCS#12** file (**user.p12**) in the installation path. CA Root certificates must have a **.cer** file extension and must be in DER format.

Execute the following command to export the certificate from the SRX Series Firewall:

```
request security pki local-certificate export certificate-id xxx type der filename /var/tmp/
filename.cer
```

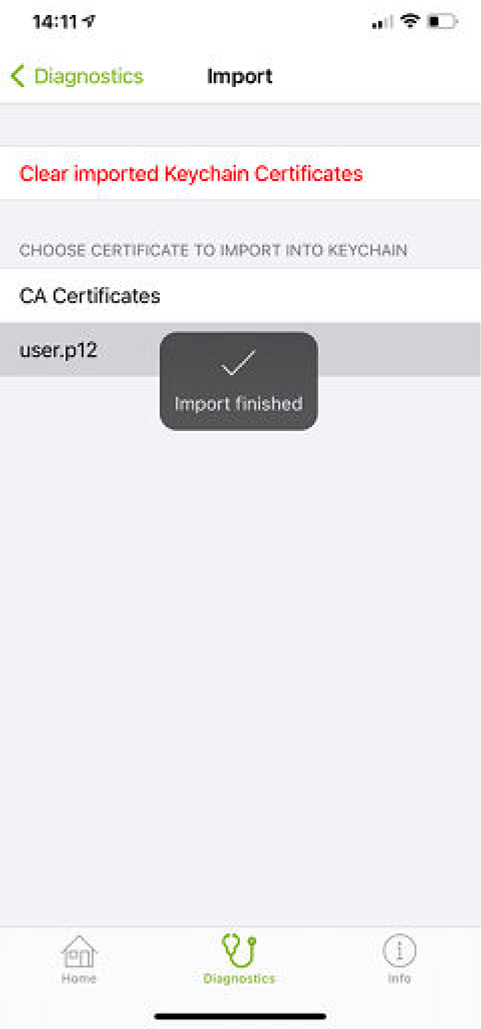
Following is an example of converting a PEM formated/Base-64 certificate using OpenSSL.

```
openssl x509 -in /…/RootCA.pem -outform DER -out /…/RootCA.cer
```

Save the certificates in the application directory using files. On iOS email client, click and hold the certificate file until you see the **Save to Files** option. Now select **Save to Files** under Secure Connect folder location.

1. Open the Juniper Secure Connect application and navigate to **Diagnostics** > **Management** > **Certificates** menu opton.
2. Click the certificate of your choice to add to the iOS keychain. Figure 221 on page 398 shows an example for successful importing of the certificates.

Figure 221: Certificate Import Completed



Clear imported Keychain Certificates

CHOOSE CERTIFICATE TO IMPORT INTO KEYCHAIN

CA Certificates

user.p12

✓ Import finished

When the certificates have been imported into keychain, you can optionally view them under **Diagnostics** > **Information** > **Certificates**. At this page, you can also delete all imported certificates from the keychain by click on **Delete Certificate Profiles**.

We also recommend you to remove your user certificate from the local directory to secure the certificate.

3. After import, you can view the imported certificates (in keychain) by choosing **Diagnostics** > **Information** > **Certificates** menu option.

Info Menu

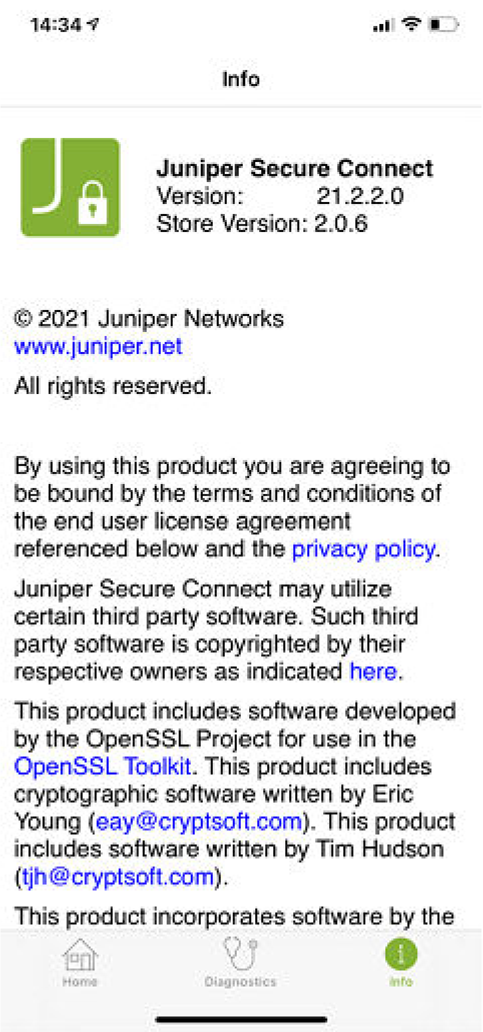
SUMMARY

Juniper Secure Connect **Info** menu provides the version and license information of the application.

IN THIS SECTION

Click on the **Info** button at the bottom right corner of the application to know the Juniper Secure Connect product label and version number details as shown in Figure 222 on page 399.

Figure 222: Displays Juniper Secure Connect Version Information



14:34

Info

Juniper Secure Connect
Version: 21.2.2.0
Store Version: 2.0.6

© 2021 Juniper Networks
www.juniper.net
All rights reserved.

By using this product you are agreeing to be bound by the terms and conditions of the end user license agreement referenced below and the privacy policy.

Juniper Secure Connect may utilize certain third party software. Such third party software is copyrighted by their respective owners as indicated here.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product incorporates software by the

WHAT'S NEXT

For more information on Juniper Secure Connect features and how to configure the options, see "Diagnostics Menu" | **387**.