

Quick Start

Cloud-Delivered Security with Juniper Secure Edge

IN THIS GUIDE

- Step 1: Begin | 1
- Step 2: Up and Running | 4
- Step 3: Keep Going | 8

Step 1: Begin

IN THIS SECTION

- Set Up Your Service Location | 1

In this guide, we provide a simple, three-step path to quickly get you up and running with Juniper® Secure Edge. You'll set up your service location, also known as point of presence (POP). Use the service location as an access point to configure and deploy secure edge policies for on-premises and roaming users.

Set Up Your Service Location

Decide the [Juniper Secure Edge Subscriptions](#) you need and reach out to your sales representative or account manager to purchase the selected subscriptions.

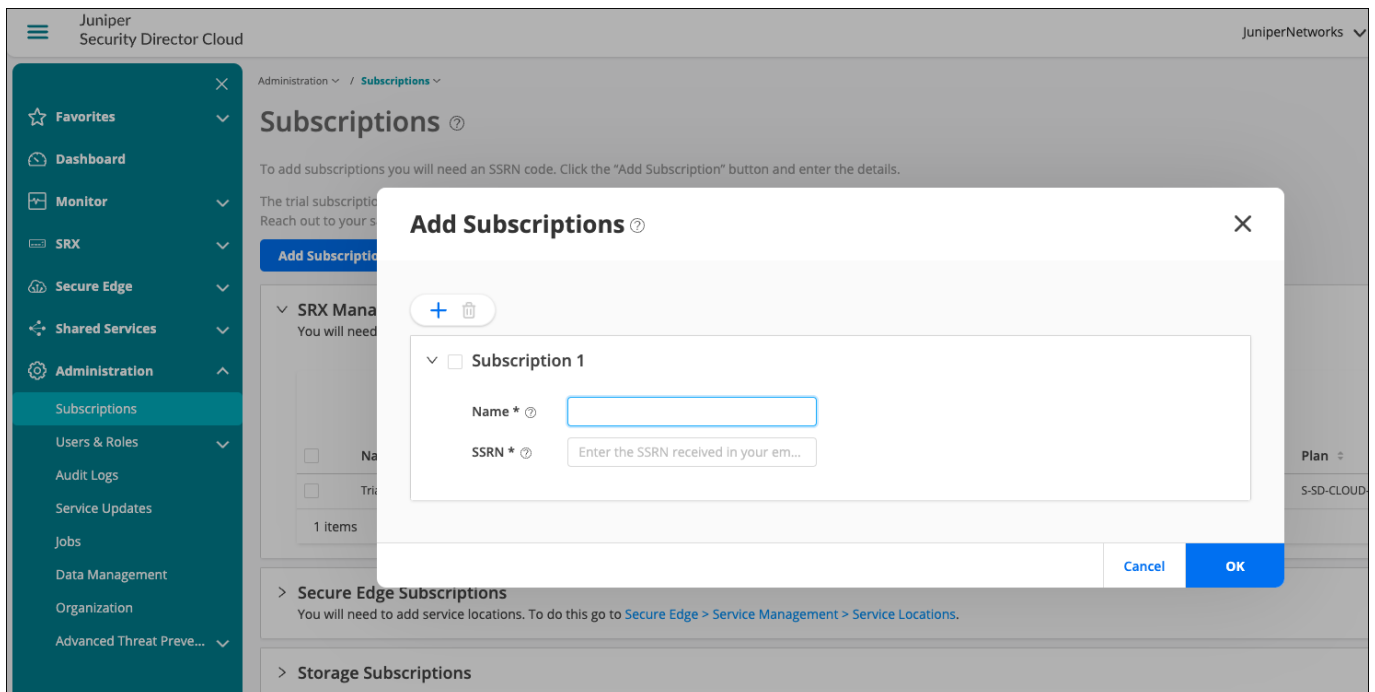
1. Go to <https://sdcloud.juniperclouds.net/> and click **Create an organization account**.

Follow the on-screen instructions to activate your account. You'll receive an e-mail about the status of your organization account activation within 7 working days. If you already have an organization account with Juniper Security Director Cloud, skip to Step 2.



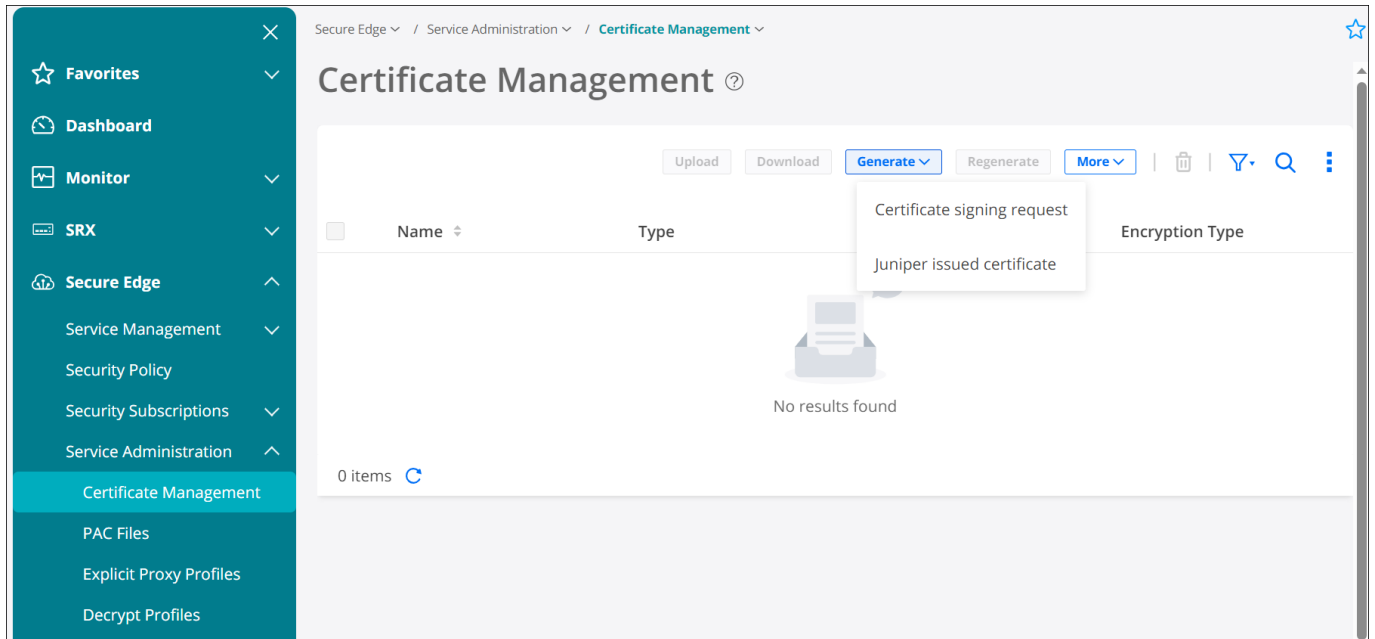
The image shows the Juniper Security Director Cloud login page. It features the Juniper logo and the text "Juniper Security Director Cloud". Below this, there are input fields for "E-mail" and "Password". A link "Forgot your password?" is located below the password field. A blue "Log In" button is positioned below the input fields. At the bottom, there is a link "New to Security Director Cloud? Create an organization account."

2. Log in to the Juniper Security Director Cloud portal, click **Add Subscriptions**, enter details, and click **OK**.



The image shows the Juniper Security Director Cloud portal interface. The left sidebar contains a navigation menu with items like Favorites, Dashboard, Monitor, SRX, Secure Edge, Shared Services, Administration, Subscriptions, Users & Roles, Audit Logs, Service Updates, Jobs, Data Management, Organization, and Advanced Threat Preve... The main content area is titled "Subscriptions" and includes instructions: "To add subscriptions you will need an SSRN code. Click the 'Add Subscription' button and enter the details." A modal dialog titled "Add Subscriptions" is open, showing a list of subscriptions. The first subscription is "Subscription 1" with a checkbox. It has two fields: "Name" and "SSRN". The "SSRN" field has a placeholder text "Enter the SSRN received in your em...". At the bottom of the dialog are "Cancel" and "OK" buttons.

3. Go to **Secure Edge > Service Administration > Certificate Management**, and click **Generate**.



- a. If your company maintains a Private Key Infrastructure (PKI) and Certificate Authority (CA), select **Certificate Signing Request (CSR)**. Enter the details, click **OK**, and download the CSR file. Get your CA's signature on the certificate and upload the signed certificate.
- b. If your company does not have a CA, select **Juniper Issued Certificate**, enter details, and click **OK**. Download and distribute the certificate among your managed devices.

You must install the certificate in your browser's trusted root store. Only one certificate is supported at a time.

4. Go to **Secure Edge > Service Management > Service Locations** and click the plus (+) sign.

Provide the service location details, link the Secure Edge subscriptions, and click **OK**.

Juniper Security Director Cloud

Secure Edge / Service Management / Service Locations

Create Service Locations

Name * ?

Locations

Location 1 * ?

Location 2 * ?

Subscriptions

Link subscriptions to the service locations.

Subscriptions * ?

Subscription 1

Total users ? 0

To continue onboarding, proceed to Step 2.

Step 2: Up and Running

IN THIS SECTION

- Set Up User Profiles | 5
- Deploy Your Secure Edge Policy | 8

Now that you've set up your service location, you're now ready to configure and deploy Juniper Secure Edge policies for on-premises and roaming users.

Set Up User Profiles

For On-Premises Users

1. Select **Secure Edge > Service Management > Sites** and click the plus (+) sign. Enter the site details, traffic forwarding information, site configuration and click **Finish**.

Juniper Security Director Cloud

Secure Edge / Service Management / Sites

Create Site

Prerequisite: Two active Service Locations

Site Details Traffic Forwarding Site Configuration Summary

Service Locations

Primary service location * ?

Secondary service location * ?

Number of Users * ?

Estimated provisioned bandwidth: None

Site Details

Name * ?

Description ?

Country * ?

Postal code ?

Site address ?

Protected networks * ?

- From the **Deploy Status > Tunnel configuration**, click **Copy to Clipboard**. Paste the configuration in the CLI of your customer premises equipment (CPE) device and commit the changes.

Secure Edge ▾ / Service Management ▾ / Sites ▾

Sites ?

Deployed Undeployed

Export More ▾ + ✎ 🗑️ 🔍 ⋮

<input type="checkbox"/>	Name ↕	Provisioned Users	Tunnel Type	Primary Servi...	Secondary Se...	Deploy Status	Description
<input checked="" type="checkbox"/>	A_IPSEC_QS...	1	IPSec Profile Name: PSK_G14	North America (Oreg Tunnel Status	North America (Cana Tunnel Status	Deployed Tunnel Configurations	
<input type="checkbox"/>	CTC00_000...	1	IPSec Profile Name: PSK_G14	North America (Oreg Tunnel Status	North America (Cana Tunnel Status	Deployed Tunnel Configurations	IPSEC_DYNAMIC ...
<input type="checkbox"/>	CTC00_000...	1	IPSec Profile Name: PSK_G14	North America (Oreg Tunnel Status	North America (Cana Tunnel Status	Deployed Tunnel Configurations	IPSEC_DYNAMIC ...
<input type="checkbox"/>	CTC00_000...	1	IPSec Profile Name: PSK_G14	North America (Oreg Tunnel Status	North America (Cana Tunnel Status	Deployed Tunnel Configurations	IPSEC_DYNAMIC ...
<input type="checkbox"/>	CTC00_000...	1	IPSec Profile Name: PSK_G14	North America (Oreg Tunnel Status	North America (Cana Tunnel Status	Deployed Tunnel Configurations	IPSEC_DYNAMIC ...
<input type="checkbox"/>	CTC00_000...	1	IPSec Profile Name: PSK_G14	North America (Oreg Tunnel Status	North America (Cana Tunnel Status	Deployed Tunnel Configurations	IPSEC_DYNAMIC ...

2001 items ↻

Display 25 ▾ < 1 2 3 4 5 ... 81 > Go to

- Select **Secure Edge > Service Management > IPsec Profiles**, click the plus (+) sign, enter the required information, and click **OK**.

For Roaming Users

- Go to **Secure Edge > Identity > User Authentication**, select an authentication method (Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), or Hosted Database), enter the required

configuration, and click **Save**.

Juniper Security Director Cloud

Secure Edge ▾ / Identity ▾ / User Authentication ▾

End User Authentication ?

[SAML Profile ?](#) [LDAP Profile ?](#) [Hosted Database ?](#)

SAML Profile

SAML Profile * ? ☒

ACS Urls [View ACS Urls](#)

Identity Provider (IdP)

IdP settings ?

☐ Import settings

☐ Enter settings manually

☐ Enter metadata URL

Service Provider (SP)

Entity ID * ?

Username attribute * ?

Sign auth requests ? ☒

Group attribute ?

2. Select **Secure Edge** > **Service Administration** > **PAC Files**. Select the proxy auto-configuration (PAC) file and click **Copy URL**.
3. Go to your browser proxy settings, paste the URL of the PAC file, and click **Save**.
4. Select **Secure Edge** > **Service Administration** > **Explicit Proxy Profiles**. Enter the port number of the proxy server and select the decrypt profile from the list. If you do not have a decrypt profile, click **Create Decrypt Profile**, enter the required information, and click **Save**.

Deploy Your Secure Edge Policy

1. Select **Secure Edge > Security Policies** and click plus (+) sign to create a new rule.

Juniper Security Director Cloud

Secure Edge Policy

Last update: 10 days ago by [user]@juniper.net | Total Rules 6 | ✖ Deploy failed

1 selected

Seq	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options
0 hits	SecureEdgePolicy-1	+ Sources	+ Destinations	+ Applications/Services	Deny	IPS, Decrypt, Web Filtering, Content Filtering, Secintel, Anti-malware, CASB	Schedule (On)
1	JSE-Infrastructure-Access	Any	JSE-Edge-IPs	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, Secintel, Anti-malware, CASB	Schedule (On)
2	Office365	Any	office365	Any	Permit	IPS, Decrypt, Web Filtering, Content Filtering, Secintel, Anti-malware, CASB	Schedule (On)
3	Core-Network-Services	Any	Any	DNS defaults	Permit	IPS, Decrypt, Web Filtering, Content Filtering, Secintel, Anti-malware, CASB	Schedule (On)

2. Enter the required information, click ✓ to save the policy, and click **Deploy**.

For on-premise users, the site tunnel status displays as



Up

in the portal. For roaming users, the end user authentication status displays as **Success**.

Congratulations! You have successfully onboarded Juniper Secure Edge for on-premises and roaming users!

Step 3: Keep Going

IN THIS SECTION

- What's Next? | 9
- General Information | 9
- Learn with Videos | 9

What's Next?

Use the Juniper Security Director Cloud portal to configure and monitor Secure Edge services for your network. Here are some things you can do next:

If You Want To	Then
Configure allowlists and blocklists to filter trusted and untrusted resources	See Create Allowlists and Blocklists
Configure anti-malware profiles to inspect malware	See Create Anti-malware Profile
Configure content filtering policies to prevent access to malicious content	See Create a Content Filtering Policy
Configure Secure Edge policy rule to specify actions for a transit traffic	See Add a Secure Edge Policy Rule

General Information

If You Want To	Then
See all the available documentation for Juniper Secure Edge	Visit Juniper Secure Edge
See all the available documentation for Juniper Security Director Cloud	Visit Juniper Security Director Cloud

Learn with Videos

If You Want To	Then
Understand what is Secure Access Service Edge (SASE)	Watch What is SASE?
Understand what is Juniper Secure Edge	Watch What is Juniper Secure Edge?
See a demonstration of how to get started with Juniper Secure Edge	Watch Getting Started with Juniper Secure Edge

(Continued)

If You Want To	Then
Deploy Juniper Security Service Edge	See Juniper Secure Edge Training Course
Learn how to manage security with Security Director Cloud and Juniper Secure Edge	Watch Manage Security Anywhere With Security Director Cloud and Juniper Secure Edge