

Quick Start

Cloud-Delivered Security with Juniper Secure Edge

IN THIS GUIDE

- Step 1: Begin | 1
- Step 2: Up and Running | 3
- Step 3: Keep Going | 6

Step 1: Begin

IN THIS SECTION

- Set Up Your Service Location | 1

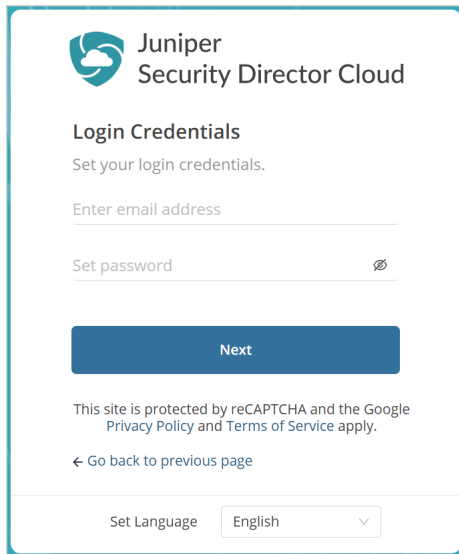
In this guide, we provide a simple, three-step path to quickly get you up and running with Juniper® Secure Edge. You'll set up your service location, also known as point of presence (POP). Use the service location as an access point (AP) to configure and deploy Secure Edge policies for on-premises and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

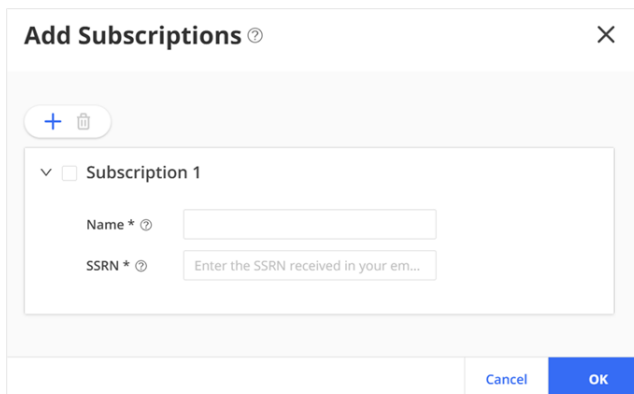
1. Go to <https://sdcloud.juniperclouds.net/> and click **Create an organization account**.

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.



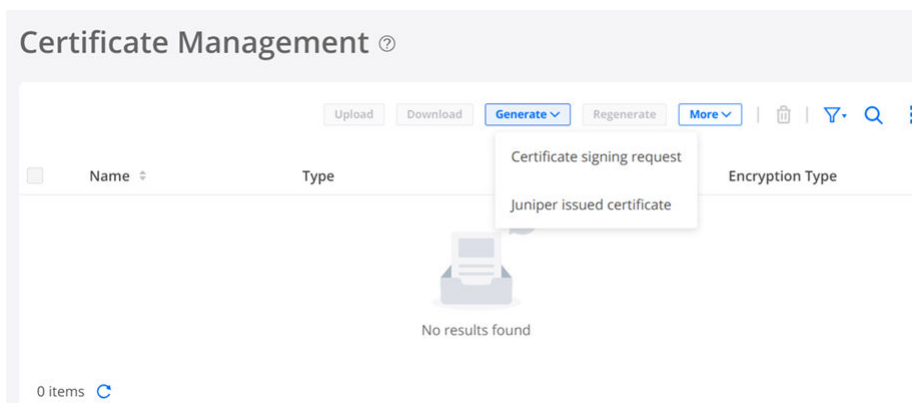
The image shows the 'Login Credentials' page of the Juniper Security Director Cloud interface. At the top is the Juniper logo and the text 'Juniper Security Director Cloud'. Below this is the heading 'Login Credentials' followed by the instruction 'Set your login credentials.' There are two input fields: 'Enter email address' and 'Set password' (with a toggle for visibility). A blue 'Next' button is positioned below the password field. At the bottom, there is a note about reCAPTCHA and Google's Privacy Policy/Terms of Service, a link to 'Go back to previous page', and a language selector set to 'English'.

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



The image shows the 'Add Subscriptions' dialog box. It has a title bar with a close button. Inside, there are icons for adding (+) and deleting (-) subscriptions. A section titled 'Subscription 1' is expanded, showing two required fields: 'Name *' and 'SSRN *'. The SSRN field has a placeholder text 'Enter the SSRN received in your em...'. At the bottom right are 'Cancel' and 'OK' buttons.

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



The image shows the 'Certificate Management' interface. At the top is the title 'Certificate Management'. Below it are buttons for 'Upload', 'Download', 'Generate' (with a dropdown arrow), 'Regenerate', and 'More' (with a dropdown arrow). There are also icons for delete, filter, search, and a menu. Below these buttons is a table with columns: 'Name', 'Type', and 'Encryption Type'. The table is currently empty, showing 'No results found' with a printer icon. At the bottom left, it says '0 items' with a refresh icon. A dropdown menu is open from the 'Generate' button, showing two options: 'Certificate signing request' and 'Juniper issued certificate'.

- 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 the 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 Locations** and click the plus (+) sign.

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

Create Service Locations ⓘ

Name * ⓘ

Locations

Location 1 * ⓘ

Location 2 * ⓘ

Subscriptions

Link subscriptions to the service locations.

Subscriptions * ⓘ

☐ Subscription 1

Total users ⓘ 0

Cancel OK

You must set up at least two service locations. To continue onboarding, proceed to Step 2.

Step 2: Up and Running

IN THIS SECTION

- [Set Up User Profiles | 4](#)
- [Deploy Your Secure Edge Policy | 6](#)

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 Sites** and click the plus (+) sign. Select the service locations, enter the site details, traffic forwarding information (customer premises equipment (CPE) and interfaces), configure CPE routing configuration (optional), and click **Finish**.

Create Site ⓘ Prerequisite: Two active Service Locations

Site Details Traffic Forwarding CPE Configuration Summary

Service Locations

Service location A * ⓘ

Service location B * ⓘ

Number of Users * ⓘ

Available users: 0
Estimated provisioned bandwidth: None

Site Details

Name * ⓘ

Description ⓘ

Country * ⓘ

Postal code ⓘ

Site address ⓘ

Protected networks ⓘ ☒ Add protected networks ☐ Add protected networks using address groups

☐ Protected Networks

2. Expand the site details, go to **Tunnel configurations > View**. The configuration is auto-generated for SRX Series firewall. Click **Copy to Clipboard**. Paste the configuration in the CLI of your CPE device and commit the changes.

Sites ⓘ

Deployed Undeployed

1 selected show selected rows ☐ Refresh Tunnels Export Undeploy More ▾ | + edit delete filter search ⋮

☒	Name ▾	Users	Addresses	Service Location...	Service Location...	Deploy Status	Description
☒	test-site (1 CPE)	10	172.16.0.0/32	North America (Vir...	North America (Vir...	✓ Success	-

1 items Display 25 ▾ < 1 >

For non-SRX Series Firewalls, a generic configuration summary is provided

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

For Roaming Users

1. Go to **Secure Edge > 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**.

End User Authentication ⓘ

SAML ⓘ LDAPS ⓘ Hosted Database ⓘ

SAML Profile * ⓘ ☒

ACS Urls ⓘ [View ACS Urls](#)

Identity Provider (IdP) Configuration

Directory Synchronization ⓘ ☐

IdP Settings ⓘ

☐ Import settings

☐ Enter settings manually

☒ Enter metadata URL

Metadata URL * ⓘ

Service Provider (SP) Configuration

Entity ID * ⓘ

Username attribute * ⓘ

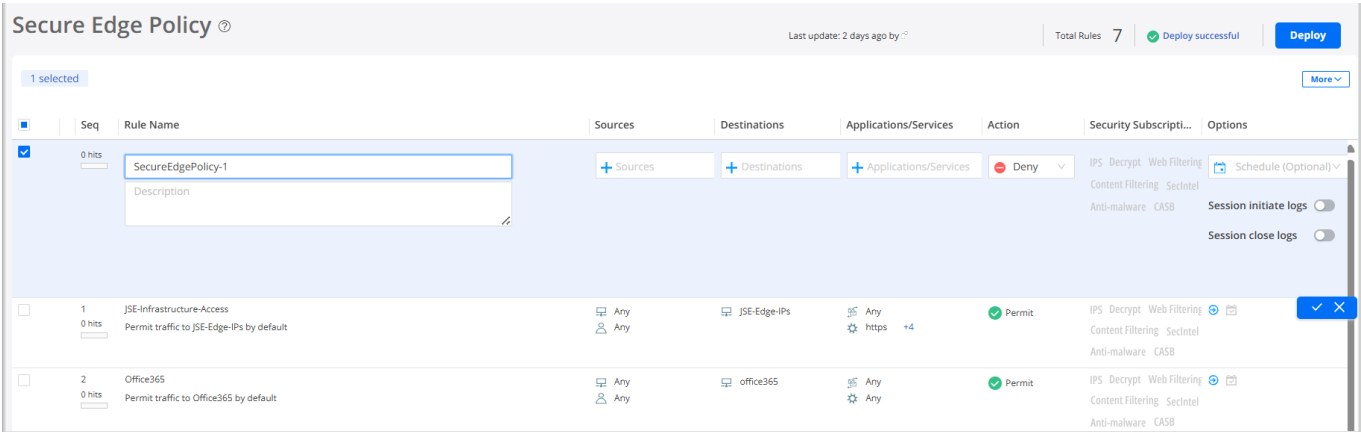
Sign auth requests ⓘ ☐

Group attribute ⓘ

2. Select **Secure Edge > 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**.
3. Select **Secure Edge > PAC Files**. Recommended proxy auto-configuration (PAC) file is auto-generated. Select the PAC file and click **Copy URL**.
4. Go to the browser proxy settings on your device, paste the URL of the PAC file, and click **Save**.

Deploy Your Secure Edge Policy

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



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, after authentication in to the portal, 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? | 6](#)
- [General Information | 7](#)
- [Learn with Videos | 7](#)

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 anti-malware profiles to inspect malware	See Create Anti-malware Profile

(Continued)

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

