Juniper Networks | Engineering Simplicity

Juniper Cloud

Administration Guide

Published
2023-10-16

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

Juniper Cloud Administration 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 | v

1 Introduction

Administration Overview | 2

User Activation and Login | 4

Administration Workflow | 6

2 Organization Management

Organization and Sites Overview | 9

Add an Organization | 9

Delete an Organization | 10

Manage Organization Settings | 11

Authentication Methods Overview | 15

Manage Identity Providers | 16

- Add an Identity Provider | 17
- Edit an Identity Provider | 18
- Delete an Identity Provider | 18

Manage Roles | 18

- Add a User-Defined Role | 19
- Edit a User-Defined Role | 20
- Delete a User-Defined Role | 20

Manage API Tokens | 21

- Add an API Token | 21
- Edit an API Token | 22
- Delete an API Token | 22

Configure Webhooks to Receive Event Notifications in Slack Channels | 23

Link Your Juniper Networks Account to Your Organization | 26

3 Site Management

About the Sites Page | 28

Manage Sites | 29

4 User Management

About the Users Page | 33

Predefined User Roles Overview | 34

Add Users to an Organization | 36

Invite Users | 38

Manage Users and Invites | 39

- Edit User Role | 40
- Reinvite a User | 40
- Cancel an Invitation | 41
- Revoke a User | 42

Manage Your Juniper Cloud Account | 42

5 Inventory Management

About the Inventory Page | 46

Adopt a Device | 58

- Adopt a Device to Juniper Cloud-hosted Application | 58
- Adopt a Device to JSI Service | 60

Assign a Device to a Site | 61

6 Audit Logs

Audit Logs Overview | 63

About the Audit Logs Page | 64

About This Guide

Use this guide to understand the various features that Juniper Cloud provides to the applications running on Juniper Cloud. This guide provides overviews, workflows, and procedures that help you understand and manage the organizations, users, and the sites configured in the applications running on Juniper Cloud.

1

CHAPTER

Introduction

Administration Overview | 2

User Activation and Login | 4

Administration Workflow | 6

Administration Overview

IN THIS SECTION

- Manage Organizations | 2
- Manage Sites | 3
- Manage Users | 3
- Manage Inventory | 3
- Monitor Audit Logs | 4

Juniper Cloud is Juniper's software as a service solution that hosts applications in the cloud and enables these applications to interact with the devices in the network. Juniper Cloud is based on a modern microservices-based architecture that ensures scalability, flexibility, and maintainability. Juniper Cloud provides the hosted applications, an easy to use user and organization management system that supports multi-tenancy. The user management module in Juniper Cloud enables administrators to add users and assign the required roles. An administrator with the Super User role can manage organizations, sites, and the users in the organization. The user who creates the organization is assigned the superuser role in the organization, by default. After the organization is created, the Super User needs to configure organization settings, add sites, and then add users to predefined roles according to the tasks the users need to perform in the organization. This topic provides an overview of the tasks a superuser performs in an organization.

Manage Organizations

After you create an account in Juniper Cloud, you need to create an organization in the hosted application. An organization in Juniper Cloud represents a customer (for a service provider) or a branch (for an enterprise). To manage an organization, you must log in to Juniper Cloud and then access the organization. An organization may have multiple sites that represent the locations where routers, switches, and firewalls are installed. After creating an organization, the superuser needs to configure the following features from the Settings page to efficiently manage the organization:

- Authentication methods to manage access to the organization
- Identity providers (IdP) to enable single sign-on (SSO)
- Roles for users at the organization-level, mapping to the predefined roles

- Session policy to time out sessions following a period of inactivity
- API tokens to enable users to retrieve information through REST APIs
- Password policy to secure users' access to the applications hosted on Juniper Cloud
- Webhooks to view alerts and events notifications in real-time
- Juniper Networks account to view details of the devices associated with the account

For more information, see "Organization and Sites Overview" on page 9.

Manage Sites

After you create an organization, you need to create sites, which are the physical locations within the organization. Sites house the devices in a network, such as routers, switches, and firewalls. After sites are created, a superuser can assign devices to those sites. The Sites page provides information about sites, their location and timezone, and the site group to which the sites belong. A Super User can edit site information or delete sites that are not in use.

For more information, see "About the Sites Page" on page 28.

Manage Users

To perform the various tasks in an organization, the superuser needs to add users to various predefined roles according to the tasks the users with those roles need to perform in the organization. Adding a user to the organization is as easy as sending an e-mail invite to a user, and assigning a predefined role in the organization. Based on the tasks that a user needs to perform, superuser can assign the roles, such as Super User, Network Admin, Observer, and Installer, providing role-based access to resources. A superuser can add, modify, and delete users. An invite expires if the user doesn't accept the invite within seven days of receiving the invite. For more information, see "About the Users Page" on page 33.

Manage Inventory

Inventory consists of the devices in the organization. The devices can be physical or virtual and are grouped by type, such as routers, switches, and firewalls. Users with Super User and Network Admin roles can onboard a device by using the **Adopt Device** option and remove a device from Juniper Cloud by using the **Release Device** option. Adopting a device is the process of adding a device to Juniper Cloud

by a superuser or a network administrator to manage it in a brownfield deployment. By releasing a device, you remove the device from Juniper Cloud due to reasons such as a device reaching its end of life. For more information, see "About the Inventory Page" on page 46.

Monitor Audit Logs

An audit log is a record of a sequence of user-initiated activities such as accessing an organization, or adding or deleting a user or a site. Audit logs are stored for 30 days. Audit logs are useful in tracking and maintaining a history of users' activities on the network. For more information, see "About the Audit Logs Page" on page 64.

User Activation and Login

To access an application in Juniper Cloud, you must create an account in Juniper Cloud and then, activate the account. After you activate your account, you either create an organization or join an organization through an invite.

Juniper Cloud initiates user activation when:

- The first user accesses the Web GUI without an invite.
- The superuser invites you to an organization. Click the link in the invite and complete the login tasks. Your login procedure depends on whether you are an existing user with a Juniper Cloud account or a new user without a Juniper Cloud account.

1. To log in as the first admin user without an invite:
   a. Access the GUI directly at https://manage.cloud.juniper.net.

      NOTE: Juniper Networks recommends that you use Chrome 10.8, Firefox 107.0.1, or Safari 16.1 browsers to access Juniper Cloud.

   b. Click **Create Account** on the Juniper Cloud page.

   c. Type your first name, last name, e-mail address, and password on the My Account page.
      The password is case sensitive.

   d. Click **Create Account**.
      Juniper Cloud sends a verification e-mail to activate your account.

e. Click **Validate Me** in the e-mail body.

   The New Account page appears.

f. (Optional) Click **View Account** to check your name and e-mail address.

g. Click **Create Organization**.

h. Type a unique name for your organization and click **Create**.

   The New Account page appears.

i. Click the organization on the New Account page.

2. To log in as a new user with an invite:

   a. Click **Go to *organization-name*** in the e-mail body.

      The Invite to Organization page opens in your default browser.

   b. Click **Register to Accept**.

      The My Account page appears.

   c. Enter your first name, last name, e-mail address, and configure a password.

      The password can contain up to 32 characters, including special characters, based on the password policy of the organization.

   d. Click **Create Account**.

      Juniper Cloud sends a confirmation e-mail to activate your account.

   e. In your confirmation e-mail, click **Validate Me**.

      The New Account page opens in your default browser.

   f. Click the organization for which you received the invite.

      You can access the selected organization's GUI in the application. The tasks you can perform in this organization depends on your user role. See "Predefined User Roles Overview" on page 34 for more information.

3. To access an invite as an existing user:

   a. Click **Access *organization-name*** in the e-mail body.

      The Invite to Organization page opens in your default browser.

   b. Click **Sign In to Accept**.

      The Juniper Cloud page appears.

   c. Enter your username and click **Next**.

      The Juniper Cloud login page appears.

   d. Enter your password and click **Log In**.

The Invite to Organization page appears.

e. Click **Continue**.

The Select an Organization page appears.

f. (Optional) You can click **View Account** to verify your account details and click **Back** to return to the Select an Organization page.

g. Click the organization for which you received the invite.

You are logged in to the application. The tasks you can perform depends on your role. See "Predefined User Roles Overview" on page 34 for more information.

RELATED DOCUMENTATION

Manage Your Juniper Cloud Account | 42

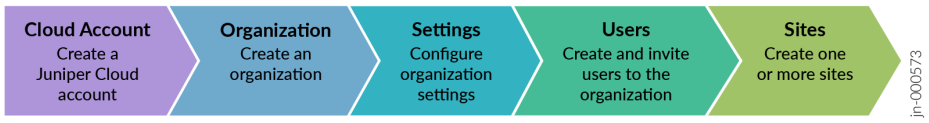
Administration Workflow

After you purchase a Juniper Cloud-hosted application, you receive an e-mail from Juniper Networks that contains instructions to create an account in Juniper Cloud and access the application.

Typically, the first user who accesses the application is an IT or system administrator (of a service provider or an enterprise). The administrator is assigned the Super User role by default.

After logging in, the administrator must create an organization, which consists of users, devices, and geographical sites in the network. Next, the administrator must perform administration tasks. "Figure" on page 6 shows the high-level sequence of tasks that IT or system administrators perform, starting with account creation.

Figure 1: Administrator Workflow



The tasks that an administrator needs to perform are as follows:

1. Create and activate your account in Juniper Cloud and log in to the application.

See "User Activation and Login" on page 4.

2. Create an organization.

   See "Add an Organization" on page 9.

3. Configure organization settings—You must configure the following for your organization:

   - Password policy
   - Single sign-on (SSO) if you want to authenticate and authorize users using a third-party Identity Provider (IdP)
   - Integrate your Juniper Networks account with your organization

   You can optionally configure other organization settings such as session and inactivity timeouts, API tokens, and so on.

   See "Manage Organization Settings" on page 11.

4. Invite users to the organization—You can invite users in either of the following ways:

   - By assigning a role to a user and sending the user an invitation to join the organization. The tasks that a user performs depends on the assigned role. See "Invite Users" on page 38 to send invites and "Manage Users and Invites" on page 39 to manage users and invites in an organization.

     NOTE: Users must create an account in Juniper Cloud when they access the organization invite.

   - By configuring a third-party identity provider (IdP) that authenticates and authorizes users based on the role mapped to each user. See "Manage Identity Providers" on page 16.

5. Create one or more sites—A site represents a geographical location with one or more devices in your network. However, a device can be associated with only one site. See "Manage Sites" on page 29.

After you perform the initial administration tasks, you can explore other tasks in the Administration menu such as inventory management and monitoring audit logs. See "About the Inventory Page" on page 46 and "About the Audit Logs Page" on page 64.

2

CHAPTER

Organization Management

Organization and Sites Overview | 9

Add an Organization | 9

Delete an Organization | 10

Manage Organization Settings | 11

Authentication Methods Overview | 15

Manage Identity Providers | 16

Manage Roles | 18

Manage API Tokens | 21

Configure Webhooks to Receive Event Notifications in Slack Channels | 23

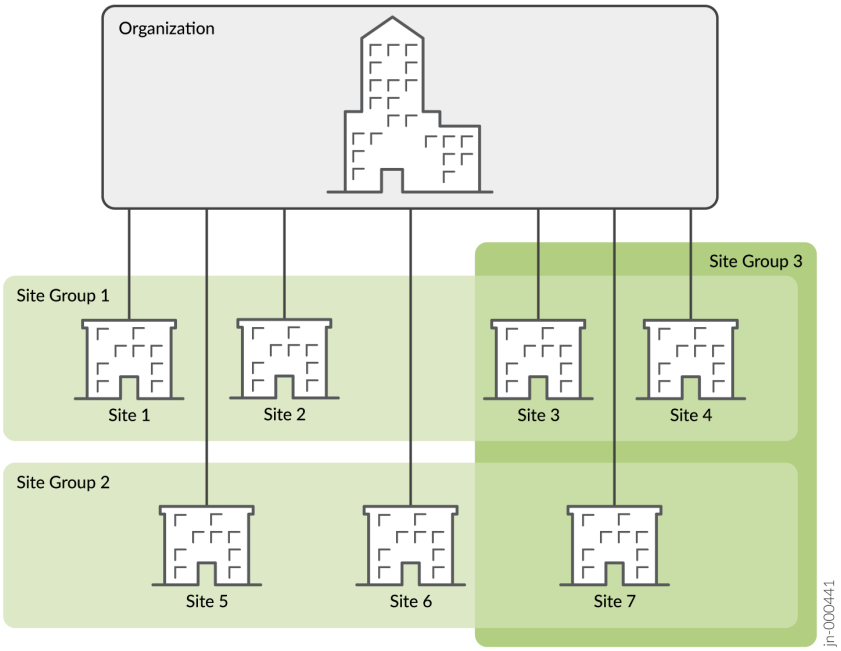
Link Your Juniper Networks Account to Your Organization | 26

Organization and Sites Overview

An organization represents a customer (for a service provider) or a branch (for an enterprise). An organization can have multiple sites representing the locations where routers, switches, and firewalls are installed. While a site can have more than one device, a device can be associated with only one site.

You can group sites based on regions, functions, or other parameters for efficient management of the devices. "Figure" on page 9 represents the relation between an organization, sites, and site groups. In "Figure" on page 9, an organization has seven sites and three sites groups (Site Group 1, Site Group 2, and Site Group 3). Site 3 and Site 4 are a part of Site Group 1 and Site Group 3 while Site 7 is part of Site Group 2 and Site Group 3.

Figure 2: Organization, Sites, and Site Groups



Add an Organization

An organization represents the customer (for a service provider) or a branch (for an enterprise). You can add an organization from:

- The Login page when you log in to Juniper Cloud and access the application.
- The organization list (next to the Help icon) on the top right-corner of the application GUI.

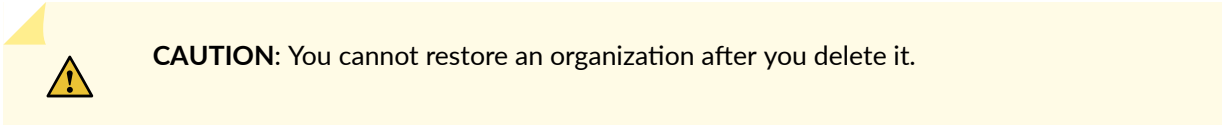
To add an organization:

1. Click **Create Organization** on the Login page or in the Organization drop-down list at the top-right corner of the GUI.
   The Create Organization page appears.
2. In the **Organization Name** field, enter a name for the organization.
3. Click **OK**.
   The organization appears in the organization list and on the Login page.
4. Click the organization to access the organization.

You are the superuser (Super User in Juniper Cloud)for an organization that you create. After you create an organization, you can configure the organization settings and invite users to access the organization. For more information, see "Manage Organization Settings" on page 11 and "Invite Users" on page 38, respectively.

Delete an Organization

You can delete an organization that you no longer manage or if you want to decommission the organization. You must be a user with the Super User role to delete an organization.



CAUTION: You cannot restore an organization after you delete it.

To delete an organization:

1. Log in to Juniper Cloud and navigate to **Administration > Settings**.
2. Click **Delete Organization**.
   The Delete Organization page appears.
3. As a confirmation for deleting the organization, enter the name of the organization in the **Organization Name** field.
4. Click **Delete Organization**.
   The organization is deleted and the Juniper Cloud Login page appears.

RELATED DOCUMENTATION

Organization and Sites Overview | 9

Manage Organization Settings

A superuser can configure the organization settings and do the following tasks:

- View organization name and organization ID and modify the organization name.
- Add, modify, and delete identity providers.
- Enable or disable the password policy for the organization and modify the password policy when the password policy is enabled.
- Modify the session timeout policy for the organization.
- Generate, edit, and delete API tokens for various roles in the organization.
- Configure webhooks for the organization.
- Add Juniper account to link Juniper Networks devices to the organization.

To configure and to manage organization settings:

1. Click **Administration > Settings** in the navigation menu.

   The Organization Settings page appears.

2. Configure or modify the organization settings as needed. Refer to Table 1 on page 11.

3. Click **Save** to save the settings.

   Verify that the settings are saved and close the Organization Settings page.

Table 1: Organization Settings Parameters

Field	Description
Organization Name	Name of the organization. You can edit the organization name here.
Organization ID	The ID for the organization. The value is auto-generated. This is a read-only field.
Single Sign On (SSO)	
Identity Providers	View identity providers configured in the organization. Add, edit, or delete the identity providers; see "Manage Identity Providers" on page 16.

Table 1: Organization Settings Parameters *(Continued)*

Field	Description
Roles	View roles configured for SSO. Add, edit, or delete the roles; see "Manage Roles" on page 18.
Password Policy	Enable or disable (default) password policy. If you enable the password policy, configure the password policy parameters; see Table 2 on page 12.
Session Policy	Configure the time, in minutes, after which the logged in session with the application should timeout; see Table 3 on page 13.
API Tokens	Generate and view API tokens to authenticate users when they retrieve data by using REST APIs; see "Manage API Tokens" on page 21.
Webhooks	Webhooks enable you to get notifications when the events that you have subscribed for occur. Click to enable or disable (default) webhooks. If you enable webhooks, you must select the type of events for which you want to receive notifications; see Table 4 on page 13.
Juniper Account Integration	Add your Juniper Networks account to link your Juniper Networks devices to the organization; see Table 5 on page 14. If no Juniper Networks account is integrated, you can also link your Juniper account from the **Installed Base** tab (**Administration > Inventory**). For more information, see "Link Your Juniper Networks Account to Your Organization" on page 26.

Table 2: Parameters to Configure Password Policy

Field	Description
Required minimum password length	Enter the minimum number of characters that should be present in the password of a user's account. Default is 8 characters. Range: 8 to 32
Require special characters	Click to enable (default) or disable the use of special characters in the password.

Table 2: Parameters to Configure Password Policy *(Continued)*

Field	Description
Require 2-Factor Authentication	Click to enable or disable (default) two-factor authentication for users accessing the organization. If you enable two-factor authentication, a code is sent to an authenticator app. A user must enter the code in addition to the password to access an organization.

Table 3: Parameters to Configure Session Policy

Field	Description
Session Timeout (minutes)	Enter the number of minutes after which the session should timeout. Default is 20160 minutes.
Inactivity Timeout (minutes)	Enter the number of minutes of inactivity after which the session should timeout. Default is 0, indicating that the session does not time out because of inactivity. Range: 0 to 480 minutes

Table 4: Parameters to Configure Webhooks

Field	Description
Name	Enter the name of the server or application to which notifications for subscribed events are to be sent.
URL	Enter the URL of the server or application where the notifications in the form of HTTP POST requests are to be sent when a subscribed event occurs. You must configure webhooks to send notifications to third-party applications, such as Slack, when events you have subscribed to are triggered on the managed devices. To receive webhook notifications in a format that is compatible with Slack, you need to configure an intermediary that can interact with the sending and receiving applications. The recommended intermediary platform is Make. For more information, see "Configure Webhooks to Receive Event Notifications in Slack Channels" on page 23.
Secret	Enter the secret to validate that the notifications received are from valid hosts.

Table 4: Parameters to Configure Webhooks *(Continued)*

Field	Description
Webhook Header	
Header Key	Enter a unique key that the webhook endpoint can use to authenticate the event notifications.
Header Value	Enter a unique value for the key.
Streaming API	
Alerts	Click to enable or disable (default) receiving notifications when subscribed alerts are generated on the managed devices.
Audits	Click to enable or disable (default) receiving notifications when an organization is accessed or any setting in the organization is changed.
Device Status	Click to enable or disable (default) receiving notifications when the device status changes due to events such as a link going up or down, or the device getting disconnected from Juniper Cloud and so on.
Device Alarms	Click to enable or disable (default) receiving notifications when subscribed alarms are generated on the managed devices.

Table 5: Parameters to Add Juniper Account

Field	Description
Email Address	The e-mail address associated with your Juniper Networks account.
Password	The password associated with your e-mail address.

Authentication Methods Overview

IN THIS SECTION

- Benefits of Single Sign-On | 15

Juniper Clouid provides different authentication methods to authenticate users.

You can use one of the following authentication methods to log in to the application GUI.

- Juniper Cloud account—Users can create a Juniper Cloud account to access the application GUI.
- Social Sign-In—All users can enable Google social media sign-in (or single sign-on) on their user account page.
- Single Sign-On (SSO)—You can configure third-party Identity Providers (IdP) to authenticate users in the organization.

While users have the necessary permission to configure and use Juniper Cloud and social media sign-in to log in, administrators can configure Single Sign-On for users in the organization. To use the Juniper Cloud account to log in, individual users must create their user account in Juniper Cloud. Superusers can create and manage users in an organization. User management includes inviting users to join an organization and revoking users' access to the organization. However, superusers cannot delete users.

You can use Google as an authentication provider to sign in to the application. Google sign-in uses OpenID Connect (OIDC) to authenticate users by verifying their Google account credentials. As an alternative, superusers can configure IdP in the Organization Settings page and map default roles in Juniper Cloud to the IdP profiles. Juniper Cloud supports Secure Assertion Markup Language (SAML 2.0) for SSO authentication using third-party IdPs. The IdP asserts a user's identity and allows the user to access the web GUI based on the user's role. This enables a superuser to create a Juniper Cloud account and authenticate other users to the organization using IdP. If you configure IdP, you manage the user account credentials in your organization.

Benefits of Single Sign-On

- Users can use a single account to log in to multiple platforms and applications.

- SSO simplifies password management for users and administrators through centralized authentication by IdP.

Manage Identity Providers

IN THIS SECTION

- Add an Identity Provider | 17
- Edit an Identity Provider | 18
- Delete an Identity Provider | 18

Identity providers enable the use of third-party credentials, such as the credentials of your Google or Facebook account, to log in into an account in Juniper Cloud.

Table 6 on page 16 lists the parameters to add identity providers to an organization.

Table 6: Parameters to Add Identity Providers

Field	Description
Name	Enter a name for the identity provider.
Type	Displays the type of identity provider. The default identity provider is SAML and cannot be modified.
Issuer	Enter the unique URL that identifies your SAML identity provider. For example, Google and Microsoft.
Name ID Format	Select the unique identifier for the user. The options are e-mail and unspecified. If you select e-mail, the identity provider uses your e-mail address to authenticate you. If you select unspecified, the identity provider generates a unique identifier to authenticate you.

Table 6: Parameters to Add Identity Providers *(Continued)*

Field	Description
Signing Algorithm	Select a signing algorithm from the following: • SHA1 • SHA256 (default) • SHA384 • SHA512
Certificate	Enter the certificate issued by the SAML identity provider.
SSO URL	Enter the URL to redirect the users to the SAML identity provider for authentication. For example, https://www.google.com.
Custom Logout URL	Enter the URL to redirect the users after logging out. For example, https://www.juniper.net.
ACS URL	The URL that the identity provider should redirect an authenticated user to after signing in. The value is auto-generated and not editable.
Single Logout URL	The URL that the identity provider should redirect when a user logs out of an authentication session. The value is auto-generated and not editable.

Add an Identity Provider

To add an identity provider:

1. Click **Administration > Settings** in the navigation menu.
   The Organization Settings page appears.
2. Click the **Create IDP (+)** icon above the Identity Providers table.
   The Create Identity Provider page appears.
3. Configure the identity provider by using the guidelines in Table 6 on page 16.
4. Click **Create**.
   The identity provider is created and listed in the Identity Providers table.

Edit an Identity Provider

To edit an identity provider:

1. Click **Administration > Settings** in the navigation menu.
   The Organization Settings page appears.
2. Click the identity provider you want to edit in the Identity Providers table.
   The Edit Identity Provider page appears.
3. Edit the identity provider by using the guidelines in Table 6 on page 16.

   NOTE: You cannot edit identity provider type, ACS URL, and Single Logout URL.

4. Click **Save**.
   You are returned to the Organization Settings page, where you can view the changes in Identity Providers table.

Delete an Identity Provider

After you delete an identity provider, a user can log in only by using their Juniper Cloud account.

To delete an identity provider:

1. Click **Administration > Settings** in the navigation menu.
   The Organization Settings page appears.
2. Click the identity provider that you want to delete.
   The Edit Identity Provider page appears.
3. Click **Delete**.
   You are returned to the Organization Settings page, where you can view that the identity provider is removed from the Identity Provider table.

Manage Roles

IN THIS SECTION

- Add a User-Defined Role | 19

Edit a User-Defined Role | 20
Delete a User-Defined Role | 20

A user with the Super User role can create a new role that maps a user role in an enterprise to a pre-defined role. For example, you can configure an administrator role and map it to the Network Admin role so that the administrator role has the access privileges of the Network Admin user. The Network Admin role can be assigned to any enterprise user. Table 7 on page 19 lists the parameters to add custom roles to an organization.

Table 7: Parameters to Add Roles

Field	Description
Name	Enter a name for the role.
Role	Select an access level for the role: • Super User • Network Admin • Observer (default) • Installer See "Predefined User Roles Overview" on page 34 for details on privileges of each role.

Add a User-Defined Role

A superuser can add a user-defined role and map it to a pre-defined role in Juniper Cloud.

To add a user-defined role that maps to a pre-defined role:

1. Click **Administration > Settings** in the navigation menu.
   The Organization Settings page appears.
2. Click the **Create Role (+)** icon.
   The Create Role page appears.

3. Configure the new role by following the guidelines in Table 7 on page 19.
4. Click **Create**.
   The new role is listed in the Roles table.

Edit a User-Defined Role

To edit a user-defined role:

1. Click **Administration > Settings** in the navigation menu.
   The Organization Settings page appears.
2. Click the role that you want to edit.
   The Edit Role page appears.
3. Edit the name and role by following the guidelines in Table 7 on page 19.
4. Click **Save**.
   You are returned to the Organization Settings page, where you can verify the changes in the Roles table.

Delete a User-Defined Role

After you delete a user-defined role, users assigned to the user-defined role must be assigned one of the roles defined in Juniper Cloud to continue accessing the resources in Juniper Cloud.

To delete a user-defined role:

1. Click **Administration > Settings** in the navigation menu.
   The Organization Settings page appears.
2. Click the role that you want to delete.
   The Edit Role page appears.
3. Click **Delete**.
   You are returned to the Organization Settings page, where you can verify that the custom role is not listed in the Roles table.

Manage API Tokens

IN THIS SECTION

- Add an API Token | 21
- Edit an API Token | 22
- Delete an API Token | 22

API tokens use REST APIs to authenticate users when they try to retrieve information. By using API tokens, users can avoid authentication for each request they make. An API token provides visibility into the resources accessed by a user, enabling you to have better control over access to resources.

Table 8 on page 21 lists the parameters for configuring API tokens.

Table 8: Parameters to Configure API Tokens

Field	Description
Name	Name of the API token.
Role	Role to which the API token is applicable: • Super User • Network Admin • Observer • Installer
Key	The key auto-generated to identify the application the user is using to access the resources.

Add an API Token

To add an API token for a role:

1. Click **Administration > Settings** in the navigation menu.
   The Organization Settings page appears.
2. Click the **Create Token (+)** icon.
   The Create API Tokens page appears.
3. Enter values by following the guidelines in Table 8 on page 21.
4. Click **Generate**.
   The API token is populated in the **Key** field.
5. Click **Close** to return to the Organization Settings page.

Edit an API Token

To edit an API token:

1. Click **Administration > Settings** in the navigation menu.
   The Organization Settings page appears.
2. Click the API token that you want to edit.
   The Edit API Token page appears.
3. Edit the name, role, and site access by following the guidelines in Table 8 on page 21.
4. Click **Save**.
   You are returned to the Organization Settings page, where you can verify the changes in the API Tokens table.

Delete an API Token

To delete an API token:

NOTE: Users using API tokens to access resources cannot access the resources after the API token is deleted.

1. Click **Administration > Settings** in the navigation menu.
   The Organization Settings page appears.
2. Click the API token that you want to delete.
   The Edit API token page appears.
3. Click **Delete**.
   You are returned to the Organization Settings page, where you can verify that the API token is not listed in the API Tokens table.

Configure Webhooks to Receive Event Notifications in Slack Channels

You use webhooks to automate sending event notifications from a source application to a destination application. You can configure webhooks to send notifications to third-party applications, such as Slack, when events you have subscribed to are triggered on the managed devices.

To receive webhook notifications in a format that is compatible with Slack, you need to configure an intermediary that can interact with the sending and receiving applications. The recommended intermediary platform is Make. To process notifications, Make uses a workflow called Scenario, which converts the notifications to a format that Slack supports. Each event notification is sent to a URL that is generated for the Scenario in Make. The notification is then converted into a format that Slack supports and delivered to the configured Slack channel.

For information on Scenario in Make, see Scenario.

To configure webhooks to send notifications to a Slack channel:

1. Log in to Make, https://www.make.com/en/login. From the home page, navigate to Scenario on the left navigation menu.
2. Configure the scenario settings as described, see Creating a Scenario.

   Make generates a URL. Whenever an event is triggered, webhook notifications are sent to this URL.
3. Navigate to Organization Settings (**Administration > Settings**).

   The Organization Settings page appears.
4. In the Webhooks tile, enable webhooks.
5. Configure the webhooks settings. See Table 9 on page 24 for webhooks field descriptions.

   NOTE: In the URL field, enter the URL generated in step 2.
6. (Optional) Verify Webhook-Slack integration by logging in to the CLI of a device and generating an event.

   For example, run the following commands in the device CLI to generate an alert.

```
user@host# set interfaces et-0/0/1 disable
user@host# commit
user@host# run show interfaces terse | grep et-0/0/1
et-0/0/1                down  down
user@host# delete interfaces et-0/0/1 disable
```

```
user@host# commit user@host# run show interfaces terse | grep et-0/0/1
et-0/0/1     up    down
```

7. (Optional) Verify that:
   - The event you generated is listed on the Events page (**Observability > Events**).
   - You received a notification for the event in the Slack channel.

> **NOTE**:
> - You must have access to the Slack channel to view event notifications in Slack.
> - You must be an administrator with the Network Admin role to perform corrective action for the notification received.

Table 9: Parameters to Configure Webhooks

Field	Description
Name	Enter a name for the webhook. The name can contain alphanumeric and special characters.
URL	Enter the URL generated in Make for the scenario.
Secret	Enter the secret to validate that the notifications received are from valid hosts. The secret can contain a string of alphanumeric and special characters.

Table 9: Parameters to Configure Webhooks *(Continued)*

Field	Description
Webhook Header	Webhook custom headers are key-value pairs that provide additional information about the notifications. You can add multiple custom headers to: • Provide additional information in plain text, along with the default headers, about the webhook notifications being sent to the configured endpoint. • Provide security, such as API keys, to verify end-to-end data integrity, for authorization, and so on. Click the **Add** icon (+) to add webhook headers. The Webhook Header page appears. • Header Key—Enter a unique key. • Header Value—Enter a unique value for the key. The value can contain alphanumeric characters. Click the **Delete** icon (trash can) to remove the webhook headers.
Streaming APIs	Enable the events for which you want to receive notifications. You can subscribe to events such as, alerts, audits, device status, and device alarms to get real-time notifications when the event occurs. • Alerts—Click to enable or disable receiving notifications when subscribed alerts are generated on the managed devices. Alerts notification is disabled by default. • Audits—Click to enable or disable receiving notifications when a user accesses an organization or modifies organization settings. Audits notification is disabled by default. • Device Status—Click to enable or disable receiving notifications when the device status changes due to events such as a link going up or down, or the device getting disconnected from Juniper Cloud, and so on. The Device Status notification is disabled by default. • Device Alarms—Click to enable or disable receiving notifications when subscribed alarms are generated on the managed devices. Device Alarm notification is disabled by default.

Link Your Juniper Networks Account to Your Organization

You must link your Juniper Networks account to your organization to view the installed base information for the devices linked to that Juniper Networks account.

The **Installed Base** tab on the Inventory page provides device-specific details along with the status information collected from the installed devices. For more information, see "About the Inventory Page" on page 46.

NOTE: You must be a superuser to link your Juniper Networks account to your organization.

To add your Juniper Networks account to your organization:

1. Click **Administration** > **Settings** and then locate the **Juniper Account Integration** tile.
2. On the **Juniper Account Integration** tile, click **Add**.

   The **Add Juniper Account** window appears.
3. Enter the access credentials (e-mail address and password) of the Juniper Networks account to be linked, and then click **OK**.

   Juniper Cloud validates the Juniper Networks account, adds the user's primary Juniper account to the organization, and populates the Installed Base (**Administration** > **Inventory** > **Installed Base**) page with the details of the devices assigned to the account.

   The Juniper Account Integration (**Administration > Settings**) tile displays your Juniper Networks account name.

   NOTE: To remove an account, click the delete (trash can) icon against the account name on the **Juniper Account Integration** tile. When you remove a user account, the associated devices are removed from the **Installed Base** page.

3

CHAPTER

Site Management

About the Sites Page | 28

Manage Sites | 29

About the Sites Page

IN THIS SECTION

- Tasks You Can Perform | 28
- Field Description | 29

Sites are the physical locations that host devices, such as routers, switches, and firewalls within an organization's network. The superuser (Super User in Juniper Cloud) can create sites and add devices to those sites. Sites are used to identify the location of the devices in an organization. Multiple sites can be grouped into site groups for easy management. For more information on organizations and sites, see "Organization and Sites Overview" on page 9.

To access the Sites page, click **Administration > Sites**.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details about the sites in an organization—You can view the site name, country, time zone, address, the site group the site belongs to, and notes about the site.
- Add, modify, or delete sites; see "Manage Sites" on page 29.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. The search results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).

Field Description

Table 10 on page 29 describes the fields displayed on the Sites page.

Table 10: Fields on the Sites Page

Fields	Description
ID	Identifier for the site.
Name	Displays the name of the site.
Country	Displays the country where the site is located.
Timezone	Displays the time zone of the site.
Address	Displays the address of the site.
Site Groups	Displays the site groups to which the site belongs, if any.
Notes	Displays additional information about the site.

Manage Sites

A site identifies the location of the devices in an organization. The superuser (Super User in Juniper Cloud) can add, modify, or delete sites in an organization.

To add a site:

1. Click **Administration > Sites**.

   The Sites page appears.
2. Click **Create Site** (+) icon.

   The Create Site page appears.
3. Enter the site parameters, select a valid location, and site groups according to the guidelines provided in Table 11 on page 30.
4. Click **OK**.

   A confirmation message indicating that the site is created is displayed, and the site is listed on the Sites page.

Table 11: Fields on the Create Site Page

Fields	Description
Name	Enter a unique name for the site. The site name can contain upto 64 characters.
Location	Click the location of the site on the map or enter the coordinates or location in the search field to choose the location. Choosing a location automatically updates the fields for country and time zone.
Country	Select the country where the site is located. If you select a location on the map, or enter coordinates or location, the field is updated with the respective country. However, if you select a country from the drop-down list, the same is not reflected on the map.
Timezone	Select the timezone of the site. If you select a location on the map, or enter coordinates or location, the field is updated with the respective timezone. However, if you select a country from the drop-down list, the same is not reflected on the map.
Site Groups	Select the site groups to which the site should belong, if any. If no site group is available, you can type a name for the site group and press **Enter** to create the site group.
Notes	Enter additional information about the site. The notes can contain up to 1000 characters.

NOTE:

- To modify the site details, select the site and click **Edit Site** (pencil) icon.
- To decommission a site, you need to delete the site from the organization. You can delete a site by selecting the site and clicking **Delete Site** (trash) icon. The site is removed permanently from the organization.

RELATED DOCUMENTATION

About the Sites Page | 28

CHAPTER 4

User Management

About the Users Page | 33

Predefined User Roles Overview | 34

Add Users to an Organization | 36

Invite Users | 38

Manage Users and Invites | 39

Manage Your Juniper Cloud Account | 42

About the Users Page

IN THIS SECTION

- Tasks You Can Perform | 33
- Field Descriptions | 34

To access the Users page, click **Administration > Users** in the navigation menu.

Tasks You Can Perform

An administrator with the Super User role can perform the following tasks from this page:

- View details of the existing users and the users who are invited to access the organization—The basic information about the users, such as first name, last name, e-mail ID, invite status of the user, and role assigned is displayed. See Table 12 on page 34 for field descriptions.
- Invite users; see "Invite Users" on page 38.
- Manage user invitations; see "Manage Users and Invites" on page 39.
- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filter operation is case insensitive, so you can add the filter criteria in uppercase or lowercase. The filtered results are displayed on the same page.
- Search by using keywords—Click the search icon (magnifying glass), enter the search term in the text box, and press Enter. You can also save the search term as a quick filter. The search operation is case insensitive, so you can enter the keyword in uppercase or lowercase. The search results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).

Field Descriptions

Table 12 on page 34 describes the fields on the Users page.

Table 12: Fields on the Users Page

Fields	Description
First Name	The first name of the user.
Last Name	The last name of the user.
Email	The e-mail ID the user would use to access the application hosted on Juniper Cloud.
Status	Indicates a user's account status: • Active: The user's account is active and the user can access the organization. • Invite Pending: The user is yet to accept the e-mail invitation sent to them and doesn't have access to the organization or the user has rejected the invitation to access the organization. • Invite Expired: The e-mail invitation sent to the user has expired. An invitation expires after seven days.
Role	The role assigned to a user. See "Predefined User Roles Overview" on page 34 for details about the user roles.

RELATED DOCUMENTATION

Add Users to an Organization | 36

Predefined User Roles Overview

Juniper Cloud provides four predefined roles to manage access privileges of users, based on the tasks they need to perform. The roles are:

- Super User

- Network Admin
- Observer
- Installer

A superuser (Super User in Juniper Cloud) creates an organization, adds users to predefined roles depending on the requirements of the organization. For example, an organization with a large number of networking devices would require multiple users performing different roles to efficiently manage the organization, whereas, in a small organization, a single user can perform the tasks to be carried out by users with all four roles. Different types of users in an organization, such as a network architect, network planner, NOC engineer, and field technician, all derive their access privileges from the predefined roles assigned to them.

User Roles and their Responsibilities

The four predefined roles are:

- Super User
  - Is the administrator of the organization.
  - Creates organization, invites users, assigns user roles, creates sites, adopts devices, and so on.
  - Superuser doesn’t need to be a person with a high-level of networking domain expertise.
- Network Admin
  - Is a networking expert who monitors, verifies, and troubleshoots an organization's network.
- Observer
  - Monitors events in the organization's network.
  - Observer cannot take corrective action. The observer brings issues to the notice of the network administrator for resolution.
- Installer
  - Onboards devices and monitors device status during onboarding.
  - Installer can access only the Onboard a Device and Device List pages.

Table 13 on page 36 displays the access privileges of the four user roles to the menu items.

Table 13: User roles and their access privileges

Menu	Super User	Network Admin	Observer	Installer
Administration				
Users	✓	✗	✗	✗
Audit Logs	✓	✓	✗	✗
Inventory	✓	✓	✓	✗
Settings	✓	✗	✗	✗
Sites	✓	✗	✗	✗

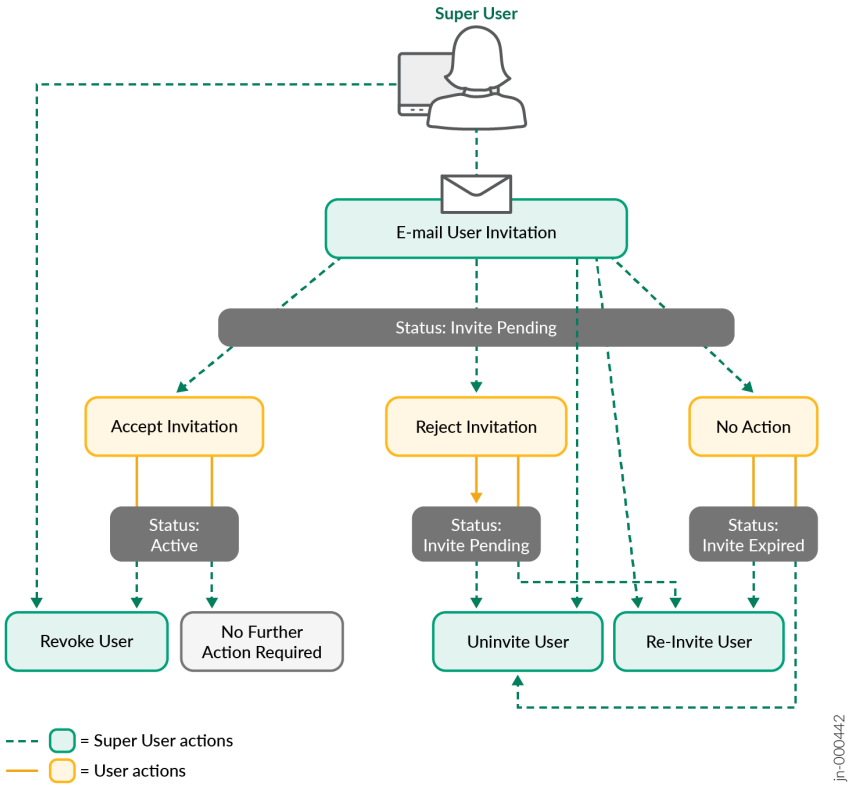
Add Users to an Organization

An administrator with the Super User role can add users to an organization and provide role-based access by sending an invitation to the user's e-mail ID. The user needs to accept the invitation to be a member of the organization.

Existing users can access their organization by using their Juniper Cloud account.

"Figure" on page 37 illustrates the workflow for inviting a new user to an organization.

Figure 3: Add users to an organization



The status of the invitation is shown as Invite Pending until the user:

- Accepts the invitation to get role-based access to the organization.
- Rejects the invitation to access the organization.
- Doesn't accept or reject the invitation within seven days. The status of such invitations is displayed as Invite Expired.

If the user accepts the invitation and has role-based access to the organization, but if the Super User wants to take away the user's access, the Super User can revoke the invitation.

If the user invitation expires, the Super User can re-invite the user or cancel the invitation.

Invite Users

An administrator with the Super User role can add users to an organization by sending an e-mail invitation from the Users page.
The user must accept the invitation within seven days, after which the invitation expires.

A user's access privileges within the organization is based on the role assigned to the user. A user can be assigned only one role in Juniper Cloud. For more information on roles, see "Predefined User Roles Overview" on page 34.

To invite a user:

1. Click **Administration > Users**.

   The Users page appears.
2. Click the **Invite User** (+) icon.

   The Users: New Invite page appears.
3. Enter user details and assign a role according to the guidelines provided in Table 14 on page 38.
4. Click **Invite**.

   A confirmation message indicating that the user is invited is displayed, and the user details are listed on the Users page.
5. Check the status of the user. If the status changes to Invite Expired, you can delete the user, reinvite the user or cancel the invitation. For more information, see "Cancel an Invitation" on page 41 and "Reinvite a User" on page 40.

Table 14: Fields on the Invite User Page

Field	Description
First Name	Enter the first name of the user. First name can contain up to 64 characters.
Last Name	Enter the last name of the user. Last name can contain up to 64 characters.
Email	Enter the e-mail ID that a user would use to access the application hosted on Juniper Cloud.

Table 14: Fields on the Invite User Page *(Continued)*

Field	Description
Role	Assign a role to the user. You can assign only one role to a user in an organization. You can assign: • Super User • Network Admin • Observer • Installer See "Predefined User Roles Overview" on page 34 for information about user roles.

RELATED DOCUMENTATION

- Add Users to an Organization | 36

Manage Users and Invites

IN THIS SECTION

- Edit User Role | 40
- Reinvite a User | 40
- Cancel an Invitation | 41
- Revoke a User | 42

You must be an administrator with the Super User role to manage users and user invitations. You can edit user role, reinvite, cancel invitations, and revoke users from the Users page.

Edit User Role

On the User: *Name* page, you can edit the role of a user. The first name, last name, and e-mail ID of a user cannot be modified.

To edit user role:

1. Click **Administration > Users**.
   The Users page appears.
2. Select the user whose role you want to edit and click **Edit User** (pencil) icon.
   The User: *Name* page appears.
3. Modify the role as needed. See Table 12 on page 34 for field descriptions.

   NOTE:
   - If you modify the role of a user whose invitation status is Active, the user is not notified about the modification in the role.
   - If you modify the role of a user whose invitation status is Invite Pending or Invite Expired, a new invitation e-mail is sent to the user to access the organization with the new role-based access privileges.
4. Click **Save**.
   A confirmation message indicating that the user invitation is updated is displayed and you are returned to the Users page, where you can view the changes you made.

Reinvite a User

You can reinvite a user if:

- The user invitation expired.
- The user invitation is pending.
- The user role needs to be modified for users with Invite Pending or Invite Expired invitation status.

To reinvite a user to the organization:

1. Click **Administration > Users**.
   The Users page appears.
2. Select the user you want to reinvite and do one of the following:

- Click **Edit User** (pencil) icon **> Re-invite**.
- Click **More > Re-invite User**.
- Right-click the user and click **Re-invite User**.

The Re-invite User confirmation window appears.

You can reinvite a user whose status is Invite Expired or Invite Pending. For users whose access is revoked or deleted, you must click the **Invite User** (+) icon to reinvite the user; see "Invite Users" on page 38.

When you reinvite from the Edit User page, you can modify the role of a user.

3. Click **Save**.

   An invitation e-mail is sent to the user and the user account is listed on the Users page with status Invite Pending.

   If the user doesn't accept the invitation within seven days, the invitation expires.

Cancel an Invitation

You can invalidate an invitation by canceling the invitation. You can uninvite a user if the invitation status is Invite Pending or Invite Expired on the Users page.

NOTE: An invite expires after seven days.

To uninvite a user:

1. Click **Administration > Users**.

   The Users page appears.

2. Select the user you want to uninvite and do one of the following:
   - Click **Edit User** (pencil) icon > **Uninvite**.
   - Click **More > Uninvite**.
   - Right-click the user and click **Uninvite**.

   The Delete Invitation confirmation window appears.

3. Click **OK** to uninvite the user.

   A confirmation message indicating that the invite is canceled is displayed and you are returned to the Users page. The details about the user invitation is no longer listed in the Users table.

Revoke a User

If the user accepts the invitation and has role-based access to the organization, but you want to take away the user's access, you can revoke the invitation. Revoking a user's access deletes the user from the organization. You can revoke access only for active accounts.

To revoke a user's access to an organization:

1. Click **Administration > Users**.

   The Users page appears.
2. Select the user whose access needs to be revoked and do one of the following:
   - Click **Edit User** (pencil) icon > **Revoke**.
   - Click **More > Revoke User**.
   - Right-click the user and click **Revoke User**.

   The Delete User confirmation window appears.
3. Click **OK**.

   The user is deleted from the organization and cannot access the organization.

> **NOTE**: Juniper Cloud maintains a log of the user's activities in the organization even after the user's account is deleted or their access gets revoked. For example, the user's activities recorded in the audit logs will remain even if they no longer have access to the organization.

Manage Your Juniper Cloud Account

You can manage your Juniper Cloud account information from the My Account page. You can access the My Account page by clicking the user account icon in the top right corner of the GUI. From the list, choose **My Account**. The **My Account** page displays the user's role in the organization as an immutable field. The user role is assigned by the administrator when they send the invite to the user to join the organization.

You can perform the following tasks in the My Accounts page:

- Change account information
- Change your password
- Enable two-factor authentication

- Enable e-mail notifications for superusers and network administrators
- Enable social sign-in
- Delete your Juniper Cloud account

1. To change account information:
   a. Click your user account icon at the top-right corner and click **My Account** from the list.
   b. Change your e-mail address, name, and phone number, as necessary, in the Account Information section.
   c. Click **Save**.
      Your user account information is successfully updated.
2. To change your password:
   a. Type a password in the New Password box.
      The superuser configures the password policy for the organization. A password can contain up to 32 characters including special characters.
   b. Click **Save**.
      A message confirms that your user data is successfully updated.
3. To enable two-factor authentication:
   a. Toggle the switch on to enable **Two Factor Authentication**.
   b. Click **Save**.
      A message confirms updating your user data. A verify button appears near the two-factor authentication option.
   c. Click **Verify**.
      The Verification of Two Factor Authentication page displays a QR code.
   d. Open your authenticator application and click the add icon (**+**) to add a new account.
   e. Scan the QR code displayed.
      Your Juniper Cloud account appears in your authenticator application.
   f. Enter the token number from your authenticator application in the Verification of Two Factor Authentication page.
   g. Click **Verify**.
      A green check mark appears beside the Two Factor Authentication option on your My Account page. The two-factor authentication is active for your account. You can log out and log back in to the cloud portal.
4. To enable e-mail notifications:

You must enable e-mail notification on the My Account page to receive e-mail notifications for all or selected sites.

a. Click **Enable** in the Email Notification section.

   The Enable Email Notifications page appears.

b. Click the **Enable Org Notifications** toggle button.

The Enable Email Notifications page appears.

a. Click the toggle button against a site to receive e-mail notifications specific to the site.

b. Click **Close**.

   The Enable Email Notification section shows that you have enabled notifications for your current organization.

5. To enable social sign-in:

   a. Enable the Sign In With Google option in the Social Sign In section.

      A message asks your permission for redirection to link your Google account.

   b. Click **Yes**.

      You will be redirected to the Google sign in page.

   c. Enter your Google e-mail and password and click **Next**.

      Juniper Cloud links your Google account and redirects to the My Account page. A message confirms that Juniper Cloud linked your Google account.

6. To delete your account:

   a. Click **Delete Account**.

      A confirmation message appears.

   b. Click **Yes**.

      The application logs you out and deletes your Juniper Cloud account.

> **NOTE**: After you delete your user account, the audit logs related to your activities in the organization is stored for 30 days.

5
CHAPTER

Inventory Management

About the Inventory Page | 46

Adopt a Device | 58

Assign a Device to a Site | 61

About the Inventory Page

IN THIS SECTION

- Tasks You Can Perform | 46
- Field Description | 49

The Inventory page lists the devices in an organization grouped as routers, switches, and firewalls. You can view the device details such as host name, model, a serial number, and so on.

In the **Installed Base** tab, you can view device details, including the site where the device is located, the start and end date of the device's service contract, end of life (EOL) and end of service (EOS) for the device, and so on, for all the Juniper Networks devices in your network.

To access the Inventory page, click **Administration > Inventory** on the navigation menu.

Tasks You Can Perform

You can perform the following tasks on the Inventory page:

- View details of a device (router, switch, or firewall) present in the organization—To view details of a device, click the respective tab of the device, and click the **Details** icon that appears next to the check box beside a device name. The Device Details pane appears on the right side of the page displaying the basic device information and the site where the device is located. See Table 16 on page 50.
- Adopt a device; see "Adopt a Device" on page 58.
- Release a device—Releasing a device implies removing the device from the management of Juniper Cloud due to reasons such as end of life (EOL) of the device. When you release a device, the SSH configuration that establishes the connection between the device and the Juniper Cloud is removed from the device and the device cannot connect with Juniper Cloud.

  Select the device (under the appropriate tab) and click **Release *Device*** and click **Yes** on the Confirm *Device* Release page.

> **NOTE**: Releasing the device only removes the outbound ssh configuration. You can add the ssh configuration when you adopt the device again.

- Export details of all the routers in the CSV format—To export details of all routers, on the Routers tab, click the **Export** button. The details are exported to an CSV that you can download to your local system.
- Assign one or more devices to a site; see "Assign a Device to a Site" on page 61.
- View information about the Juniper Networks devices linked to your organization from the **Installed Base** tab. You can also onboard supported devices to the JSI service from this tab. For more information, see "Adopt a Device to JSI Service" on page 60.

  > **NOTE**: To access information about the Juniper Networks devices from the **Installed Base** tab, you must first link your Juniper Networks account to your organization from the Settings (**Administration** > **Settings**) page. For more information, see "Link Your Juniper Networks Account to Your Organization" on page 26.

  The information includes device-specific details along with the status information collected from the installed devices. The installed base information helps you decide whether you should connect a device to Juniper Cloud. Once the Juniper account is linked to your organization, the page displays the following banners:

  - The total count of your devices that are currently assured (connected to Juniper Cloud-hosted application), attached (connected to JSI service), and not connected (not onboarded) to Juniper Cloud.
  - The total number of devices whose hardware EOS dates are in the immediate future (in less than 3 months) and the total number of devices that are approaching their hardware EOS dates (in 3 to 6 months).
  - The total number of devices whose software EOS dates are in the immediate future (in less than 3 months) and the total number of devices that are approaching their software EOS dates (in 3 to 6 months).

    > **NOTE**: You can view this informationonly for connected devices.

  For more information on the fields on the Installed Base tab, see Table 17 on page 51.
- You can also view the following information on the **Installed Base** tab:

- General and contract information, and hardware and software EOL dates for devices on the **Device Quick View** panel or the **Overview** tab in the *Device* Details page.

  > **NOTE**: You can view the software EOL dates only for connected devices.

  To view the **Device Quick View** panel, select the device and click the Quick View icon beside the **Download** icon.

  To view the **Overview** tab in the *Device* Details page, click the serial number of a device.

  For more information on the fields on the *Device* Quick View pane and *Device* Details page, see Table 18 on page 53.

- Information on the security vulnerabilities published by the Juniper Security Incident Response (SIRT) team for the devices linked to your Juniper Networks account on the **SIRT** tab.

  To view the **SIRT** tab, click the serial number of the device to open the *Device* Details page, and click the **SIRT** tab. The **SIRT** tab displays a banner with the total counts of critical, high, medium, and low severity vulnerabilities for all devices.

  > **NOTE**: If Juniper Networks device is connected, the **SIRT** tab displays a list of security vulnerabilities specific to the Junos OS version installed on the Juniper Networks device. If a Juniper device is not connected, the **SIRT** tab displays a generic list of security vulnerabilities. To connect a device to Juniper Cloud, click **Adopt Device**, copy the outbound SSH commands and commit them on the device. For more information, see "Adopt a Device" on page 58.

  From the **SIRT** tab, you can access the **Device SIRT Quick View** to view more information about an advisory.
  To view the **Device SIRT Quick View** pane, select an entry in the **SIRT** tab and click the Quick View icon beside **Adopt Device**.

  For more information on the fields on the SIRT tab and *Device* SIRT Quick View pane, see Table 19 on page 55.

- Proactive bug notifications (PBNs) that provide information about the issues that affect the devices linked to your Juniper Networks account on the **PBN** tab.
  To view the **PBN** tab, click the serial number of the device to open the *Device* Details page, and click the **PBN** tab. The **PBN** tab displays a banner with the total counts of critical, major, and minor known problems for the device.

To view the **Device PBN Quick View** pane, select an entry in the **PBN** tab and click the Quick View icon beside **Adopt Device**.

For more information on the fields on the PBN tab and *Device* Quick View pane, see Table 20 on page 57.

- Download the Installed Base data in CSV format by clicking the Download icon on the top-right corner of the Installed Base table. The downloaded file has a column named 'Type' to indicate whether the device is a switch or a firewall.

  NOTE: If you open the downloaded CSV file with Microsoft Excel on a Mac computer, any non-English characters in the file might appear as special characters. To avoid this issue, follow the steps below:

  1. Open a new Excel file and then select **File > Import > CSV File > Import**.
  2. Select the file to be opened and then click **Get Data**.

     The **Text Import Wizard** window appears.
  3. Select **Unicode (UTF-8)** as **File Origin**.
  4. Click **Finish**.

- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).

Field Description

Table 15 on page 49 lists the fields on the Inventory page.

Table 15: Fields on the Inventory Page (for the Routers, Firewalls, and Switches tabs)

Field	Description
ID	ID of the device.

Table 15: Fields on the Inventory Page (for the Routers, Firewalls, and Switches tabs) *(Continued)*

Field	Description
Name	Name of the device.
Status	Status of the device: • Connected—Device is connected to Juniper Cloud and assigned to a site.. • Disconnected—The device is not assigned to a site. The device may or may not be connected to Juniper cloud.
IP Address (for routers and firewalls)	Management IP address assigned to the device.
MAC Address (for switches)	MAC address assigned to the device.
Model	Device model; for example ACX7100-48L, ACX7100-32C, and MX240.
Site	Site to which the device is assigned.
Serial Number	Serial number of the device.
Software Version	Version of operating system installed on the device.
Product	Device type; for example, MX, ACX.
Vendor	Manufacturer of the device.
Operating System	Operating system installed on the device; for example, Junos or Junos Evolved.

Table 16: Fields on the *Device* Details Pane

Field	Description
General	
Name	Host name of the device.
Model	Device model; for example ACX7100-32C.

Table 16: Fields on the *Device* Details Pane *(Continued)*

Field	Description
IP Address	Management IPv4 address assigned to the device.
Created Time	Date and time when the device was onboarded to the application.
Modified Time	Date and time when a device detail was modified.
Site Displayed only if a site is assigned to the device.	
Name	Name of the site where the device is installed.
Address	Address of the site where the device is installed.
Country Code	Country where the device is installed.
TimeZone	Time zone where the device is installed.

Table 17: Fields on the Installed Base Tab

Field	Description
Serial Number	Unique ID mapped to the device.
Model	Model of the device.

Table 17: Fields on the Installed Base Tab *(Continued)*

Field	Description

Status	Shows device connection status. Values include:
	• Assured—The device is onboarded to the application from the Routers, Switches, or Firewalls tabs. A colored icon indicates the current connection status of the device. The icon colors are:
	  • Green—Device is connected to the application.
	  • Red—Device is either offline or got disconnected from the application.
	• Attached—The device is onboarded to the JSI service from the Installed Base tab. A colored icon indicates the current connection status of the device. The icon colors are:
	  • Green—Device is connected to the JSI service.
	  • Red—Device is either offline or got disconnected from JSI service.
	• Not Connected—The device is neither onboarded to a Juniper Cloud hosted application or the JSI service.

Installed Address	Address of the site where the device is installed.
Contract ID	Service contract number assigned to the device.
Product Number	Stock Keeping Unit (SKU) number assigned to the device.
HW EoL Date	End of Life date for the device.
HW EoS Date	End of Service date for the device.
Customer PO	Customer purchase order number for the device.
Sales Order	Sales order number for the device.
Product Number	Stock Keeping Unit (SKU) number assigned to the device.
Contract Type	Type of active support coverage provided for the device. Example: Maintenance.
Contract SKU	SKU assigned to the active support coverage associated with the device.

Table 17: Fields on the Installed Base Tab *(Continued)*

Field	Description
Contract Start	Service contract start date for the device.
Contract End	Service contract end date for the device.
Ship Date	Date on which the device was shipped to your company's site.
Reseller	Reseller of the device.
Distributor	Distributor of the device.
Warranty Type	Warranty type associated with the device. Example: Standard Hardware Warranty.
Warranty Start Date	Start date of warranty for the device.
Warranty End Date	End date of warranty for the device.

Table 18: Fields on the Device Quick View Pane and *Device* Details Page

Field	Description
General	
Model	Model of the device.
Installed Address	Address of the site where the device is installed.
Product Number	Stock Keeping Unit (SKU) number assigned to the device.
Recommended Software Release	Recommended Junos OS software version for the device.
Last Updated	Date on which the recommended Junos OS software was last updated.
Junos Software Versions-Suggested Releases	Links to a Juniper Support Portal Knowledge Base article with a list of recommended Junos OS version for each Juniper platform.

Table 18: Fields on the Device Quick View Pane and *Device* Details Page *(Continued)*

Field	Description
Contract	
Contract SKU	SKU assigned to the device's service contract.
Contract Type	Type of active support coverage provided for the device. Example: Maintenance.
Start Date	Date on which the service contract starts for the device.
End Date	Date on which the service contract ends for the device.
Reseller	Name of the reseller through which your company acquired the device.
Hardware End of Life (Displayed if at least one of the following hardware EOL information is available for the device.)	
End of Life	Date on which the device reaches end of life. Severity icons for hardware End of Life: • Red (critical)—Less than 3 months • Orange—3-6 months • Yellow—6-12 months • No icon—More than 12 months
End of Support	Date on which the device reaches end of support.
Software End of Life NOTE: Software EOL information is available only if the device is connected.	

Table 18: Fields on the Device Quick View Pane and *Device* Details Page *(Continued)*

Field	Description
End of Support	Date on which the Junos OS software installed on the device reaches end of support. Severity icons for software End of Support are: • Red (critical)—Less than 3 months • Orange—3-6 months • Yellow—6-12 months • No icon—More than 12 months
End of Life	Date on which the Junos OS software installed on the device reaches end of life. Severity icons for software End of Life are: • Red (critical)—Less than 3 months • Orange—3-6 months • Yellow—6-12 months • No icon—More than 12 months
First Release Shipping	Date on which the Junos OS software was first released.
View software end of life dates details	Link to the Junos OS Dates & Milestones page in the Juniper support website. This page contains dates of important milestones for all Junos OS versions.

Table 19: Fields on the SIRT Tab and *Device* SIRT Quick View Pane

Field	Description
JSA ID	Unique value that identifies the security advisory on Juniper Networks Support Portal.
Title	Synopsis of the security advisory.

Table 19: Fields on the SIRT Tab and *Device* SIRT Quick View Pane *(Continued)*

Field	Description
Severity	Severity rating of the security advisory. The values are: • Critical • High • Medium • Low
CVSS Score	Common Vulnerability Scoring System (CVSS) severity assessment score of the advisory in the range of 0-10.
Affected Models	Device models affected by the security advisory.
OS Versions Affected	Junos or Junos Evo versions affected by the security advisory.
Release Date	Date on which the security advisory was first published.
JSA Updated Date	Date on which the security advisory was last updated.
Problem	Description of the security advisory.
Solution	Solution for the security vulnerability described in the advisory.
Workaround	Detailed explanation on how to temporarily resolve the problem.
Affected Series	Identifies one or more product series affected by the security advisory.
Release Notes	Short description of the security advisory.
View SIRT details	Link to the advisory in the Juniper Networks Support Portal. You can view this link in the **SIRT Quick View Pane**.

Table 20: Fields on the PBN Tab and *Device* PBN Quick View Pane

Field	Description
ID	Unique value that identifies the Problem Report.
Headline	Synopsis of the problem.
Customer Risk	Classification of the potential impact to the customer if the bug was encountered in the network. The values include: • Critical—Conditions that could severely affect service, capacity or traffic, billing, and maintenance capabilities. • Major—Conditions that could seriously affect system operation, maintenance, administration, and so on. • Minor—Conditions that would not significantly impair the functioning of the network or significantly affect services.
Bug Type	Indicates the phase or activity during which the problem was discovered. Example: Day-1.
Trigger	Describes the events that happened before or at the time the problem occurred, or the event that caused the problem.
Introduced In	Junos or Junos Evo release where the problem was first found and reported.
Fixed In	Junos or Junos Evo release in which the problem was resolved.
Release Notes	Short description of the problem.
Restoration	Indicates how the service can be restored when the problem occurs. Values include: • Self-recovery—Service, traffic, or operation disruptions are automatically restored without any user intervention. • Not-possible—It is not possible to restore the service or traffic. • Manual—User intervention is required to restore the service, traffic, or operation disruption.
Restoration Steps	Steps to restore the service when the problem occurs.

Table 20: Fields on the PBN Tab and *Device* PBN Quick View Pane *(Continued)*

Field	Description
Workaround	Detailed explanation of how to temporarily resolve the problem until a permanent resolution is available.
Workaround Provided	Indicates whether a workaround for the problem is provided or not. Values include: • Yes—Workaround is available and is described in the **Workaround** field. • Not-possible—There are no workarounds to the problem.
Product Family	Identifies one or more products affected by the problem.

Adopt a Device

IN THIS SECTION

- Adopt a Device to Juniper Cloud-hosted Application | **58**
- Adopt a Device to JSI Service | **60**

Adopt a Device to Juniper Cloud-hosted Application

You should be a user with superuser or network administrator privileges to adopt a device (router, switch, or firewall) to a Juniper Cloud-hosted application.

A superuser or network administrator can adopt a device that is already a part of the network, and manage the device from the application. When a device is adopted, management tasks such as updating configurations using configuration templates, applying licenses, and upgrading software can be performed.

The status of a device that is already installed and connected to the network, but is not managed by a Juniper Cloud-hosted application appears as Disconnected on the Inventory page (**Administration >**

Inventory). After the device connects with a Juniper Cloud hosted application, the status of the device changes to Connected, indicating that the device is managed by a Juniper Cloud hosted application.

Before you adopt a device, ensure that:

- The device can reach the gateway.

  > **NOTE**: If a firewall exists between Juniper cloud and the device, configure the firewall to allow outbound access on TCP ports 443, 2200, 6800, and 32,767 from the management port of the device.

- The device can connect to the Internet by pinging the IP address 8.8.8.8.

To adopt a device:

1. Navigate to **Administration > Inventory**.
   The Inventory page appears.
2. On the Installed Base tab, click **Adopt Device**.
   The *Device* Adoption page appears.

   Alternatively, click the **Adopt Router** on the Routers tab. The Router Adoption page appears.
3. Click **Select Site** to select the site where the device is installed.
   The outbound SSH configuration that is required for the device to establish a connection with Juniper Cloud appears.
4. Click **Copy to Clipboard** to copy the CLI commands under **Apply the following CLI commands to adopt a Juniper Device if meets the requirements.** section to the clipboard.
5. Access the device by using Telnet or SSH and log in to the device in configuration mode.
6. Paste the contents of the clipboard and commit the configuration on the device.
   The device connects to Juniper Cloud and can be managed by a Juniper Cloud-hosted application.
7. After you adopt a device, you can verify the device's connectivity with Juniper Cloud by running the following command on the device:

   ```
   user@host> show system connections |match 2200
   ```

   An output similar to the following indicates that the device is connected to Juniper Cloud:

   ```
   tcp 0 0 ip-address:38284 ip-address:2200 ESTABLISHED 6692/sshd: jcloud-s
   ```

Adopt a Device to JSI Service

You must be a superuser or a network administrator privileges to adopt a device (router, switch, or firewall).

In addition to the device models supported by a Juniper Cloud-hosted application, you can also onboard (attach) additional supported devices to a JSI service from the **Installed Base** tab. The JSI service connects the attached devices to Juniper Cloud and provides basic device monitoring services. JSI service collects only limited details and statistics to troubleshoot issues on these attached devices. A superuser or network administrator can adopt a device to JSI service on Juniper Cloud.

The status of a device that is already installed and connected to the network, but is not managed by a Juniper Cloud-hosted application or JSI service appears as Not Connected on the Installed Base tab (**Administration > Inventory**). If the device connects with the application, the status of the device changes to Assured, indicating that the device is managed by the application. If the device connects with JSI service, the status of the device changes to Attached, indicating that the device is managed by JSI service on Juniper Cloud.

Before you adopt a device, ensure that:

- The device can reach the gateway.

  NOTE: If a firewall exists between Juniper cloud and the device, configure the firewall to allow outbound access on TCP ports 443, 2200, 6800, and 32,767 from the management port of the device.

- The device can connect to the Internet (verify by pinging the IP address 8.8.8.8).

To adopt a device:

1. Navigate to **Administration > Inventory**.
   The Inventory page appears.
2. On the Installed Base tab, click **Adopt Device**.
   The Device Adoption page appears.
3. Click **Copy to Clipboard** to copy the CLI commands under **Apply the following CLI commands to adopt a Juniper Device that meets the requirements.** section to the clipboard.
4. Access the device by using Telnet or SSH and log in to the device in configuration mode.
5. Paste the contents of the clipboard and commit the configuration on the device.
   The device connects to Juniper Cloud and can be managed by JSI service.

6. After you adopt a device, you can verify the device's connectivity with Juniper Cloud by running the following command on the device:

```
user@host> show system connections |match 2200
```

An output similar to the following indicates that the device is connected to Juniper Cloud:

```
tcp 0 0 ip-address:38284 ip-address:2200 ESTABLISHED 6692/sshd: jcloud-s
```

Assign a Device to a Site

A site represents the location where the device is installed. Each device must be assigned to a site for efficient management such as for applying policies.

To assign one or more devices to a site:

1. Navigate to **Administration > Inventory**.
   The inventory page appears.
2. On the **Router** tab, select the device that you want to assign to a site and click **More > Assign to a Site**.
   The Assign Devices to a Site page appears.
3. Select the site to assign the devices in the **Select Site** list and click **Done**.
   The device is assigned to the selected site and the Site field on the Inventory page shows the site to which the device is assigned.

After the device is assigned to a site, you can apply all the device management functions on the device.

6
CHAPTER

Audit Logs

Audit Logs Overview | 63

About the Audit Logs Page | 64

Audit Logs Overview

An audit log is a record of activities initiated by a user or by a process in a workflow that the user has initiated.

You can view a record of:

- User-initiated activities such as accessing, creating, updating, or deleting any resource or component.
- System-run activities that are part of different workflows in the application. Such tasks are recorded in the audit logs as system-initiated tasks even though the workflow is initiated by the user during the onboarding process.

Audit logs are useful in tracking and maintaining a history of these activities.

NOTE: Audit logging does not track device-initiated activities. Audit logs are cleared every 30 days.

Superusers and network administrators can view and filter audit logs to determine which users performed which actions at what time.

For example, a super user or network administrator can use audit logs to see who:

- added user accounts on a specific date.
- accessed the organization and at what time.
- updated or deleted an event (alert or alarm) template.
- added or deleted a site.

RELATED DOCUMENTATION

About the Audit Logs Page | 64

About the Audit Logs Page

IN THIS SECTION

- Tasks You Can Perform | 64
- Field Descriptions | 64

To access this page, select **Administration > Audit Logs**. Superusers and network administrators can view and filter audit logs for the organization. The Audit Logs page refreshes automatically and displays the latest logs.

Tasks You Can Perform

- View details of an audit log—Select an audit log and click **More > Detail** or click the **Details** icon on the left. The Details for Audit Log pane appears.

  NOTE: You can hover over the **Period** drop-down list to filter the audit logs based on the time interval you select. You can choose Last 60 Minutes, Last 24 Hours, Last 7 Days, Today, Yesterday, This Week, or Custom (enter a custom time range).

- Filter the data displayed in the table—Click the filter icon (funnel) and select whether you want to show or hide advanced filters. You can then add or remove filter criteria, save criteria as a filter, apply or clear filters, and so on. The filtered results are displayed on the same page.
- Show or hide columns in the table or reset page preferences, using the vertical ellipsis menu.
- Sort, resize, or re-arrange columns in a table (grid).

Field Descriptions

Table 21 on page 65 describes the fields on the Audit Logs page.

Table 21: Fields on the Audit Logs Page

Field	Description
ID	Unique identifier assigned to the log.
Timestamp	Date and time at which the audit log was recorded.
Username	Name and e-mail address of the user who initiated the task.
Source IP	IP address of the device from which the user initiated the task. For tasks that do not have an associated source IP address, this field is blank.
Message	Description of the logged task.
Site	Name of the site in which the task was initiated.
User Agent	Displays information about the Web browser the user used to access the application GUI.
Job	Displays a clickable **Show job details** link if a job is associated with the audit log activity. Click the link to search and display audit logs with the same Job ID.
Job ID	Unique identifier assigned to the job.

RELATED DOCUMENTATION

Audit Logs Overview | 63