

# Juniper Apstra Cloud Services User Guide

Published  
2024-05-21

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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

*Juniper Apstra Cloud Services User Guide*  
Copyright © 2024 Juniper Networks, Inc. All rights reserved.

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 | vi](#)

1

## **Introduction**

[Juniper Apstra Cloud Services Overview | 2](#)

[Juniper Apstra Cloud Services Overview | 2](#)

[Marvis Virtual Network Assistant for Data Center | 3](#)

[User Activation and Login | 3](#)

[Reset Your Password | 6](#)

2

## **Administration**

[Organization Management | 9](#)

[Organization and Sites Overview | 9](#)

[Add an Organization | 10](#)

[Delete an Organization | 11](#)

[Manage Organization Settings | 11](#)

[Authentication Methods Overview | 16](#)

[Manage Identity Providers | 17](#)

[Add an Identity Provider | 18](#)

[Edit an Identity Provider | 19](#)

[Delete an Identity Provider | 19](#)

[Manage Roles | 19](#)

[Add a User-Defined Role | 20](#)

[Edit a User-Defined Role | 20](#)

[Delete a User-Defined Role | 21](#)

[Manage API Tokens | 21](#)

[Add an API Token | 22](#)

[Edit an API Token | 22](#)

[Delete an API Token | 23](#)

Configure Webhooks to Receive Event Notifications in Third-Party Applications | 23

Integrate Your Juniper Support Resources to Your Organization | 25

## **Site Management | 27**

About the Sites Page | 27

## **User Management | 29**

About the Administrators Page | 29

Predefined User Roles Overview | 30

Add Users to an Organization | 32

Invite Users | 33

Manage Users and Invites | 36

- Edit User Role | 36

- Reinvite a User | 37

- Cancel an Invitation | 37

- Revoke a User | 38

Manage Your Account | 38

## **Inventory Management | 41**

About the Inventory Page | 41

## **Audit Logs | 43**

Audit Logs Overview | 43

About the Audit Logs Page | 44

# 3

## **Marvis VNA for Data Center**

**Monitor and Troubleshoot Data Center Events | 47**

Adopt Apstra Edge in Juniper Apstra Cloud Services | 47

About the Marvis Page | 49

Event Types Displayed in Marvis Actions | 49

View Data Center Events in Marvis Actions | 51

Access Juniper Apstra from Juniper Apstra Cloud Services | 52

Monitor and Troubleshoot Data Center Events from Mist | 53

[Search Documentation Using Marvis Conversational Interface](#) | 57

## **Configure Alerts** | 59

[About the Alerts Page](#) | 59

[Configure an Alert Template](#) | 60

[Configure E-mail Notification for Alerts](#) | 61

# About This Guide

Use this guide to understand the features and tasks that you can perform from the Juniper Apstra Cloud Services application. This guide provides feature overviews and procedures that help you understand the features and perform the various tasks.

Juniper Apstra Cloud Services is a SaaS-based Day 2 observability platform for data centers that are managed using Juniper Apstra. The AI-powered Marvis Virtual Network Assistant for Data Center in Juniper Apstra Cloud Services enables you to monitor data center events and anomalies in real-time and resolve them proactively before they impact network traffic.

# 1

PART

## Introduction

---

[Juniper Apstra Cloud Services Overview](#) | 2

---

# Juniper Apstra Cloud Services Overview

## IN THIS CHAPTER

- [Juniper Apstra Cloud Services Overview | 2](#)
- [Marvis Virtual Network Assistant for Data Center | 3](#)
- [User Activation and Login | 3](#)
- [Reset Your Password | 6](#)

## Juniper Apstra Cloud Services Overview

Obtaining real-time visibility into the functioning of the data center is critical to providing an unmatched user experience. It is important that administrators have the ability to resolve data center events and anomalies proactively, in the same way as administrators resolve campus network events using Mist.

For this, administrators should have visibility into the operations of the data center in real-time. The Juniper Apstra Cloud Services application, which can receive, process, and perform root cause analysis of networks events from an Apstra-managed data center, can enable network administrators to proactively respond to data center events ensuring that users' application experience remains unaffected.

Juniper Apstra Cloud Services is a SaaS-based Day 2 observability platform for data centers that are managed using Juniper Apstra. By utilizing the AIOps capability of Marvis, Juniper Apstra Cloud Services analyzes the events information received from the Apstra-managed data center and displays them in Marvis Actions view along with recommended actions to resolve those events.

Juniper Apstra Cloud Services runs as an independent application in the cloud, receiving and analyzing events information from Apstra. You can also integrate Juniper Apstra Cloud Services with Mist. When integrated with Mist, you can view the total number of data center events in the **Data Center/ Application** category in Marvis Actions along with other event types for the campus and branch networks. You can then access Juniper Apstra Cloud Services and view more detailed information about those data center events in Marvis Actions. This way, network administrators get complete visibility into the operations of the entire enterprise network, comprising the campus, branch, and data center networks. Administrators can resolve network issues proactively, which in turn enables enterprises to improve operational efficiency and reduce operational cost and downtime.



In addition to the AIOps-based Marvis Actions, Juniper Apstra Cloud Services also provides the generative AI-based Marvis Conversational Interface (CI), which enables administrators to quickly search within product documentation for relevant troubleshooting information to resolve the events.

## Marvis Virtual Network Assistant for Data Center

A key component of Juniper Apstra Cloud Services is the Marvis Virtual Network Assistant (VNA) for Data Center, which is the AI-native virtual network assistant for data center operations. Marvis VNA for Data Center combines the power of AI and the intent-driven approach of Apstra in building and operating data center.

Marvis VNA ingests the network event information received from the Apstra Edge component, analyzes them and provides network administrators actionable insights and recommendations to resolve an event. Marvis VNA performs root cause analysis for the events received from the edge and displays them in Marvis Actions under different event categories. Administrators can quickly examine such events at the click of a button or, if more troubleshooting is required, they can access Juniper Apstra and perform the recommended steps to resolve the issue. All these can happen in real-time before network traffic is affected.

In addition to Marvis Actions, Juniper Apstra Cloud Services also provides Marvis Conversational Interface (CI), which supports natural language processing (NLP), to search documentation in Juniper Networks Documentation and Knowledge Base. Network administrators can use Marvis CI to ask queries in natural language and Marvis CI will look up relevant documentation repositories and generate the answer. This will enable network administrators to resolve the issues faster without having to manually navigate through different documents to obtain the required information.

## User Activation and Login

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

Juniper Apstra Cloud Services application initiates user activation when:

- You create an account and an organization and access Juniper Apstra Cloud Services 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 Apstra Cloud Services application account or a new user without a Juniper Apstra Cloud Services application account.

1. To log in as the first admin user without an invite:

- a. Access the GUI directly at <https://dc.ai.juniper.net>.

**NOTE:** Juniper Networks recommends that you use the latest version of Chrome, Firefox, or Safari browsers to access Juniper Apstra Cloud Services application.

- b. Click **Create Account**.

- 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 Apstra Cloud Services application sends a verification e-mail to activate your account.



**You've requested to be registered!**

Hello from Mist Systems!

Thanks for your registration request. Please click **Validate me!** link below to finish your registration.

**Validate me!**

- 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. Click **Back** to return to the Select an Organization page.

- g. Click **Create Organization**.

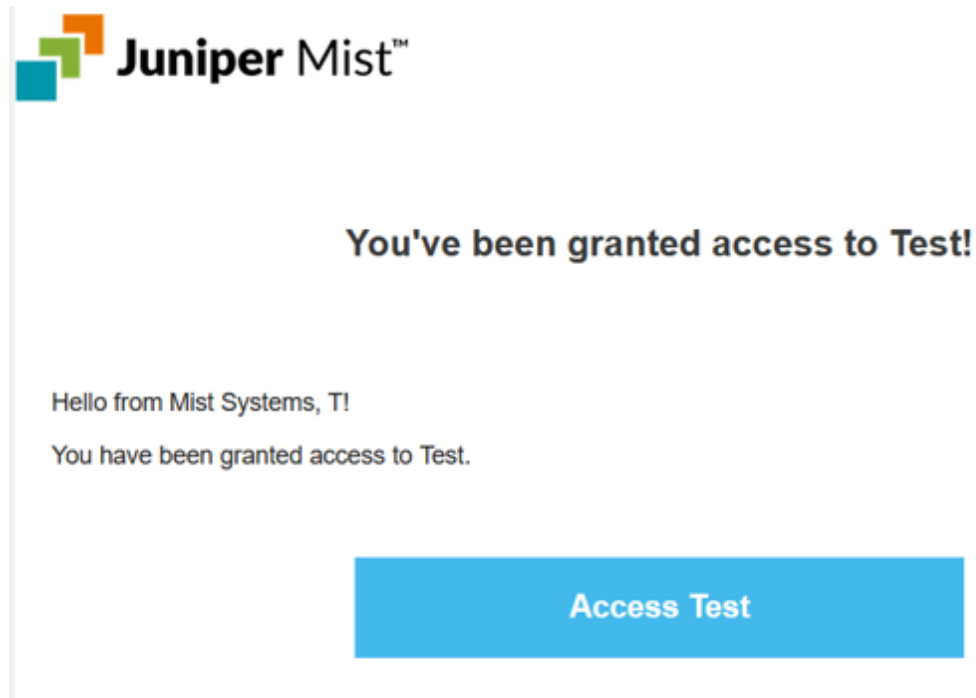
- h. Type a unique name for your organization and click **Create**.

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:

You receive an invite from an administrator to join an existing organization.



a. Click **Access *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 Apstra Cloud Services application sends a verification 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 are logged in to the application and can access the selected organization's GUI. The tasks you can perform in this organization depends on your user role. See "[Predefined User Roles Overview](#)" on page 30 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 Apstra Cloud Services page appears.
- c. Enter your username and click **Next**.  
The Juniper Apstra Cloud Services 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 and can access the selected organization's GUI. The tasks you can perform depends on your role. See "[Predefined User Roles Overview](#)" on page 30 for more information.

## RELATED DOCUMENTATION

| [Manage Your Account](#) | 38

## Reset Your Password

You can reset your password on the login page in the Juniper Apstra Cloud Services GUI. If you had enabled two factor authentication for your account, it will be disabled when you reset your password. You must re-enable two factor authentication after logging into the GUI using your new password.

To reset your password:

1. On the login page, click **Forgot Your Password?**  
The Reset Password page appears.
2. Type your e-mail address in the box and click **Send Reset Link**.  
A message confirms that the link to reset password is sent to your e-mail address.  
The Juniper Apstra Cloud Services login page appears.

3. Click **Reset My Password** in the message body of the password recovery e-mail in your inbox.

The Set New Password page appears.

4. Type a new password in the Change Password box and click **Change Password**.

A password must contain eight or more characters that are a combination of upper case and lower case letters, numbers 0-9, and special characters.

The Juniper Apstra Cloud Services login page appears.

5. Type your e-mail address and click **Next**.

6. Enter your new password and click **Log in**.

The Select an Organization page appears.

7. Select or create an organization.

You are logged into the Juniper Apstra Cloud Services GUI and can view the dashboard of the organization.

# 2

PART

## Administration

---

[Organization Management](#) | 9

[Site Management](#) | 27

[User Management](#) | 29

[Inventory Management](#) | 41

[Audit Logs](#) | 43

---

# Organization Management

## IN THIS CHAPTER

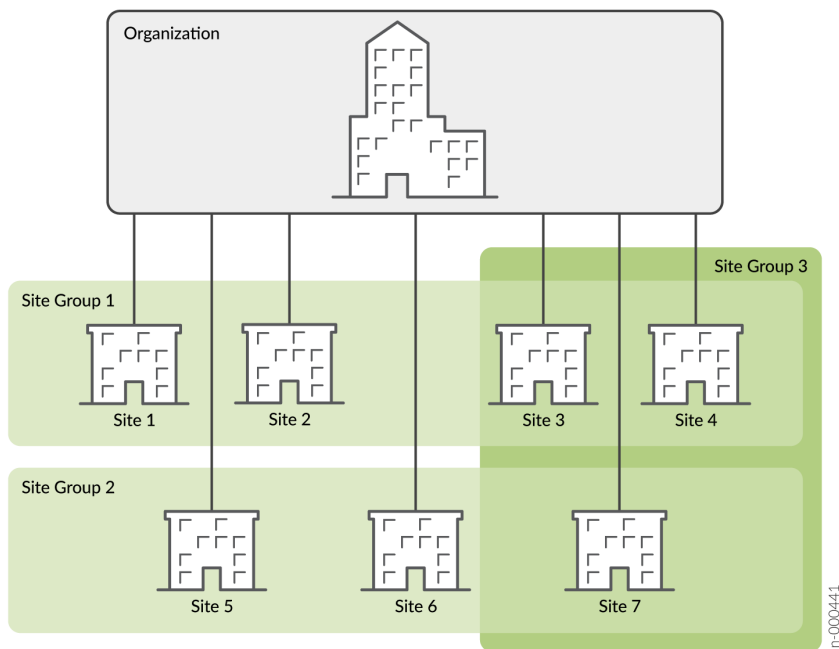
- [Organization and Sites Overview | 9](#)
- [Add an Organization | 10](#)
- [Delete an Organization | 11](#)
- [Manage Organization Settings | 11](#)
- [Authentication Methods Overview | 16](#)
- [Manage Identity Providers | 17](#)
- [Manage Roles | 19](#)
- [Manage API Tokens | 21](#)
- [Configure Webhooks to Receive Event Notifications in Third-Party Applications | 23](#)
- [Integrate Your Juniper Support Resources to Your Organization | 25](#)

## 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 data centers 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 1 on page 10](#) represents the relation between an organization, sites, and site groups. In [Figure 1 on page 10](#), 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 1: 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 Apstra Cloud Services or by clicking the **Utilities** option in My Account page.

To add an organization:

1. Click **Create Organization** on the login page.  
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 for the 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 33](#), 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 Apstra Cloud Services and navigate to **Organization > 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 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, modify the organization name, and assign organization to a Managed Service Provider (MSP).
- 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.
- Add, modify, and delete identity providers.
- Add, modify, and delete custom roles.
- Enable or disable the Juniper Networks support team access to the organization for troubleshooting.
- Configure webhooks for the organization.

- Add Juniper account to link Juniper Networks devices to the organization.
- Generate, edit, and delete API tokens for various roles in the organization.

To configure and to manage organization settings:

1. Click **Organization > 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 12](#).
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.
Managed Service Provider	Assign the organization to a Managed Service Provider (MSP), if any.
Password Policy	Enable or disable (default) password policy. If you enable the password policy, configure the password policy parameters; see <a href="#">Table 2 on page 13</a> .
Session Policy	Configure the time, in minutes, after which the logged in session with the application should timeout; see <a href="#">Table 3 on page 14</a> .
Identity Providers	View identity providers configured in the organization. Add, edit, or delete the identity providers; see <a href="#">"Manage Identity Providers" on page 17</a> .
Roles	View roles configured for SSO. Add, edit, or delete the roles; see <a href="#">"Manage Roles" on page 19</a> .
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 <a href="#">Table 4 on page 14</a> .

**Table 1: Organization Settings Parameters (Continued)**

Field	Description
API Tokens	Generate and view API tokens to authenticate users when they retrieve data by using REST APIs; see <a href="#">"Manage API Tokens" on page 21</a> .
Support Access	<p>Enable (default) or disable the Juniper Networks support team access to the organization for troubleshooting.</p> <p>It is recommended to disable this feature except during specific time frames when you are working with support to resolve an issue. In such scenarios, temporarily enable access, and disable it when the issue is resolved.</p> <p>When this feature is enabled, the support personnel can see information about all the devices in the organization.</p>
Juniper Account Integration	Add your Juniper Networks account to link your Juniper Networks devices to the organization; see <a href="#">Table 5 on page 15</a> .

**Table 2: Parameters to Configure Password Policy**

Field	Description
Required minimum password length	<p>Enter the minimum number of characters that should be present in the password of a user's account. Default is 8 characters.</p> <p>Range: 8 to 32</p>
Require special characters	Click to enable (default) or disable the use of special characters in the password.
Require 2-Factor Authentication	<p>Click to enable or disable (default) two-factor authentication for users accessing the organization.</p> <p>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.</p>

**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
Status	Select to enable or disable webhooks. The values are: <ul style="list-style-type: none"> <li>• Enabled: Webhooks is enabled and you can get notifications on third-party applications when events you have subscribed to occur in the organization.</li> <li>• Disabled: Webhooks is not enabled and you cannot get notifications on third-party applications when events occur in your organization.</li> </ul>
Webhook Type	Select the format in which notifications are to be sent when a subscribed event occurs. The options are: <ul style="list-style-type: none"> <li>• HTTP POST</li> <li>• Splunk</li> </ul>
Name	Enter the name of the server or application to which notifications for subscribed events are to be sent.

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

Field	Description
URL	<p>Enter the URL of the server or application where the notifications are to be sent when a subscribed event occurs.</p> <p>You must configure webhooks to send notifications to third-party applications, when events you have subscribed to are triggered on the managed devices.</p> <p>To receive webhook notifications in a format that is compatible with the third-party application, 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 <a href="#">"Configure Webhooks to Receive Event Notifications in Third-Party Applications" on page 23</a>.</p>
Topics	Select the events for which you want to receive webhook notifications.
<b>Advanced Settings</b>	
Verify Certificate	Enable or disable verification of certificates.
Secret	Enter the secret to validate that the notifications received are from valid hosts.
<b>Custom Headers</b>	
Key	Enter a unique key that the webhook endpoint can use to authenticate the event notifications.
Value	Enter a unique value for the key.

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 | 16](#)

Juniper Apstra Cloud Services provides different authentication methods to authenticate users.

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

- Juniper Apstra Cloud Services account—Users can create a Juniper Apstra Cloud Services 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)—Super User can configure third-party Identity Providers (IdP) to authenticate users in the organization.

While users have the necessary permission to configure and use their accounts to log in, administrators can configure Single Sign-On for users in the organization.

Super Users can create and manage users in an organization. User management includes inviting users to join an organization and revoking users' access to the organization.

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 the default roles to the IdP profiles. Secure Assertion Markup Language (SAML 2.0) is supported 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.

### 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 | 18](#)
- [Edit an Identity Provider | 19](#)
- [Delete an Identity Provider | 19](#)

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

[Table 6 on page 17](#) 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: <ul style="list-style-type: none"> <li>• SHA1</li> <li>• SHA256 (default)</li> <li>• SHA384</li> <li>• SHA512</li> </ul>
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, <a href="https://www.google.com">https://www.google.com</a> .
Custom Logout URL	Enter the URL to redirect the users after logging out. For example, <a href="https://www.juniper.net">https://www.juniper.net</a> .
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 **Organization > Settings** in the navigation menu.  
The Organization Settings page appears.
2. Click the **Add 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 17](#).
4. Click **Save**.  
The identity provider is created and listed in the Identity Providers table.

**NOTE:** If you configure IdP, the roles assigned in IdP takes precedence over the roles assigned from the Administrators page.



## Edit an Identity Provider

To edit an identity provider:

1. Click **Organization > 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 17](#).

**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 Apstra Cloud Services account.

To delete an identity provider:

1. Click **Organization > 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 | 20](#)
- [Edit a User-Defined Role | 20](#)
- [Delete a User-Defined Role | 21](#)

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 in Juniper Apstra Cloud Services.

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 20](#) 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	<p>Select an access level for the role:</p> <ul style="list-style-type: none"> <li>• Super User</li> <li>• Network Admin</li> <li>• Observer (default)</li> <li>• Helpdesk</li> </ul> <p>See "<a href="#">Predefined User Roles Overview</a>" on page 30 for details on privileges of each role.</p>

## Add a User-Defined Role

A Super User can add a user-defined role and map it to a pre-defined role in Juniper Apstra Cloud Services.

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

1. Click **Organization > 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 20](#).
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 **Organization > 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 20](#).
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 Apstra Cloud Services to continue accessing the resources in Juniper Apstra Cloud Services.

To delete a user-defined role:

1. Click **Organization > 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 | 22](#)
- [Edit an API Token | 22](#)
- [Delete an API Token | 23](#)

API tokens use REST APIs to authenticate users when they try to retrieve information from Juniper Apstra Cloud Services. 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 22 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: <ul style="list-style-type: none"> <li>• Super User</li> <li>• Network Admin</li> <li>• Observer</li> <li>• Helpdesk</li> </ul>
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 **Organization > 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 22](#).
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 **Organization > 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 22](#).
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 Juniper Apstra Cloud Services resources cannot access the resources after the API token is deleted.

1. Click **Organization > 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 Third-Party Applications

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

To receive webhook notifications in the required format, 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 the desired format. 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 the application supports and is then delivered to the application.

For information on Scenario in Make, see [Scenario](#).

To configure webhooks to send notifications:

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 (Organization > 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.

**NOTE:**

- You must have access to the third-party application to view the event notifications.
- 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
Status	<p>Select to enable or disable webhooks. The values are:</p> <ul style="list-style-type: none"> <li>• Enabled: Webhooks is enabled and you can get notifications on third-party applications when events you have subscribed to occur in the organization.</li> <li>• Disabled: Webhooks is not enabled and you cannot get notifications on third-party applications when events occur in your organization.</li> </ul>
Webhook Type	<p>Select the format in which notifications are to be sent when a subscribed event occurs. The options are:</p> <ul style="list-style-type: none"> <li>• HTTP POST</li> <li>• Splunk</li> </ul>
Name	<p>Enter the name of the server or application to which notifications for subscribed events are to be sent.</p>

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

Field	Description
URL	<p>Enter the URL of the server or application where the notifications are to be sent when a subscribed event occurs.</p> <p>You must configure webhooks to send notifications to third-party applications, such as ServiceNow, when events you have subscribed to are triggered on the managed devices.</p> <p>To receive webhook notifications in a compatible format, you need to configure an intermediary that can interact with the sending and receiving applications. The recommended intermediary platform is Make.</p>
Topics	<p>The select the types of events for which you want to receive webhook notifications.</p> <p>Select <b>Audits</b> or <b>Data Center Events</b> to receive notification when an audit log or data center event is generated.</p>
<b>Advanced Settings</b>	
Verify Certificate	Enable or disable verification of certificates.
Secret	Enter the secret to validate that the notifications received are from valid hosts.
<b>Custom Headers</b>	
Key	Enter a unique key that the webhook endpoint can use to authenticate the event notifications.
Value	Enter a unique value for the key.

## Integrate Your Juniper Support Resources to Your Organization

To enable the correlation of devices maintained within Juniper's support databases to your Juniper Support Insight experience, you must associate your organization with your Juniper support resources. To create this association, use your Juniper Support credentials (created through the [Juniper Support Portal](#)), to integrate your support resources to your organization.

For more information on device specific details collected from the cloud-connected devices, see No Link Title.

To integrate your Juniper support resources to your organization:

1. Click **Organization** > **Settings** to open the Organization Settings page.

**NOTE:** If no Juniper account is currently associated with the organization, the Installed Base tab on the Inventory page will display a link to add a Juniper account. Clicking on the **Add Juniper Account** link will open the Organization Settings page.

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

The Juniper Account Integration (**Organization** > **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.



## CHAPTER 3

# Site Management

**IN THIS CHAPTER**

- [About the Sites Page | 27](#)

## About the Sites Page

**IN THIS SECTION**

- [Tasks You Can Perform | 27](#)
- [Field Description | 28](#)

Sites are the physical locations that host devices, such as data centers within an organization's network. In Juniper Apstra Cloud Services, a site is representation of a blueprint deployed in Apstra. Whenever a new blueprint is deployed in Apstra, a new site corresponding to the blueprint is created automatically in Juniper Apstra Cloud Services.

To access the Sites page, click **Organization > Site Configuration**.

### 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.
- Filter the data displayed in the table—You can filter site information using keywords. Enter the search term in the text box next to the search icon (magnifying glass) and press Enter. The search results are displayed on the same page. You can also add one or more filters and clear filters.

## Field Description

Table 10 on page 28 describes the fields displayed on the Sites page.

**Table 10: Fields on the Sites Page**

Fields	Description
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.

## CHAPTER 4

# User Management

**IN THIS CHAPTER**

- [About the Administrators Page | 29](#)
- [Predefined User Roles Overview | 30](#)
- [Add Users to an Organization | 32](#)
- [Invite Users | 33](#)
- [Manage Users and Invites | 36](#)
- [Manage Your Account | 38](#)

## About the Administrators Page

**IN THIS SECTION**

- [Tasks You Can Perform | 29](#)
- [Field Descriptions | 30](#)

To access the Administrators page, click **Organization > Administrators** 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 address, invite status of the user, and role assigned is displayed. See [Table 11 on page 30](#) for field descriptions.
- Invite administrators; see ["Invite Users" on page 33](#).

- Manage administrator invitations; see ["Manage Users and Invites" on page 36](#).

## Field Descriptions

[Table 11 on page 30](#) describes the fields on the Users page.

**Table 11: Fields on the Users Page**

Fields	Description
First Name	The first name of the user.
Email	The e-mail address the user would use to access Juniper Apstra Cloud Services.
Status	<p>Indicates a user's account status:</p> <ul style="list-style-type: none"> <li>• Active: The user's account is active and the user can access the organization.</li> <li>• 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.</li> <li>• Invite Expired: The e-mail invitation sent to the user has expired. An invitation expires after seven days.</li> </ul>
Role	<p>The role assigned to a user.</p> <p>See <a href="#">"Predefined User Roles Overview" on page 30</a> for details about the user roles.</p>

## RELATED DOCUMENTATION

[Add Users to an Organization](#) | 32

## Predefined User Roles Overview

Juniper Apstra Cloud Services provides four predefined administrator roles and three predefined limited roles to manage access privileges of users, based on the tasks they need to perform.

A superuser 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 the 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.

The roles are:

### **Administrator Roles**

- Super User
- Network Admin
- Observer
- Helpdesk

### **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.
- Helpdesk
  - Monitor selected sites in an organization.

### **Limited Roles**

- Reporting
- DC Edge Admin

- Super Observer

### User Roles and their Responsibilities

The access privileges are limited for these role.

The six predefined limited roles are:

- Reporting
  - Can access all the analytics tools.
- DC Edge Admin
  - Can onboard datacenter edges and monitor device status during onboarding for a defined grace period set by the superuser.
- Super Observer
  - Monitor all sites.
  - View all pages under Organization menu.

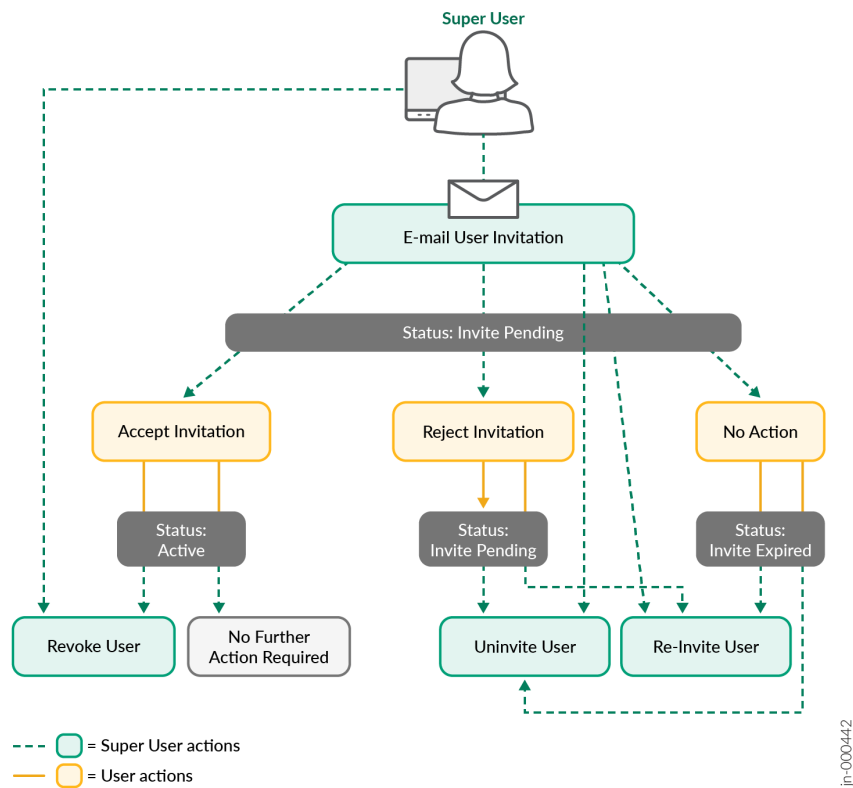
## Add Users to an Organization

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 Apstra Cloud Services account.

[Figure 2 on page 33](#) illustrates the workflow for inviting a new user to an organization.

Figure 2: 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 Administrators 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 an organization in Juniper Apstra Cloud Services. However, a user can be a member of multiple organizations within Juniper Apstra Cloud Services, and can have different roles in each organization. For more information on roles, see ["Predefined User Roles Overview" on page 30](#).

To invite a user:

1. Click **Organization > Administrators**.

The Administrators page appears.

2. Click the **Invite Administrators** icon.

The Administrators: New Invitation page appears.

3. Enter user details and assign a role according to the guidelines provided in [Table 12 on page 34](#).

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. The status is displayed as Invite Pending. 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 37](#) and ["Reinvite a User" on page 37](#).

**Table 12: 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	The e-mail address the user would use to access Juniper Apstra Cloud Services.



Table 12: Fields on the Invite User Page *(Continued)*

Field	Description
Role	<p>Assign a role to the user. You can assign only one role to a user in an organization.</p> <p>You can assign:</p> <p><b>Administrator Roles</b></p> <ul style="list-style-type: none"> <li>• Super User</li> <li>• Network Admin</li> <li>• Observer</li> <li>• Helpdesk</li> </ul> <p><b>Limited Roles</b></p> <ul style="list-style-type: none"> <li>• Reporting</li> <li>• DC Edge Admin</li> <li>• Super Observer</li> </ul> <p>See <a href="#">"Predefined User Roles Overview"</a> on page 30 for information about user roles.</p>
Site Access	<p>Select the sites the user can access in the organization. You must select at least one site. The options are:</p> <ul style="list-style-type: none"> <li>• All Sites: The user can access all sites in the organization.</li> <li>• Site Groups: The user can access specific site groups. Click <b>Add (+)</b> icon to add one or more site groups from the drop-down list.</li> <li>• Specific Sites: The user can access specific sites in the organization. Click <b>Add (+)</b> icon to add specific sites from the drop-down list.</li> </ul>

## Manage Users and Invites

### IN THIS SECTION

- [Edit User Role | 36](#)
- [Reinvite a User | 37](#)
- [Cancel an Invitation | 37](#)
- [Revoke a User | 38](#)

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 Administrators page.

### Edit User Role

On the Administrators: *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 **Organizations > Administrators**.

The Administrators page appears.

2. Select the user whose role or site access you want to edit.

The Administrators: *Name* page appears.

3. Modify the role or site access as needed. See ["About the Administrators Page" on page 29](#) for more information about user roles.

#### NOTE:

- If you modify the role or site access of a user whose invitation status is Active, the user is not notified about the modification in the role.
- If you modify the role or site access 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 Administrators 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 or site access needs to be modified for users with Invite Pending or Invite Expired invitation status.

To reinvite a user to the organization:

1. Click **Organizations > Administrators**.

The Administrators page appears.

2. Select the user you want to reinvite and click **Re-invite**.

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 33](#).

An invitation e-mail is sent to the user and the user account is listed on the Administrators 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 an administrator if the invitation status is Invite Pending or Invite Expired on the Administrators page.

**NOTE:** An invite expires after seven days.

To uninvite a user:

1. Click **Organizations > Administrators**.

The Administrators page appears.

2. Select the user you want to uninvite and click **Uninvite**.

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

The Administrators page appears.

2. Select the user whose access needs to be revoked and click **Revoke Access**.

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

**NOTE:** Juniper Apstra Cloud Services 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 Account

You can manage your 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**.

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

- [Change account information](#)
- [Change your password](#)
- [Enable two-factor authentication](#)
- [Set time preference and MAC address format](#)
- [Enable e-mail notifications for superusers and network administrators](#)
- [Enable social sign-in](#)
- [Create an organization](#)
- [Delete your 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.

To change your e-mail address, click **CHANGE**. In the Change Email window, enter the new e-mail address.

A verification link is sent to the new e-mail address and the address is updated in the Juniper Apstra Cloud Services after authentication.

- 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. Enable **Two Factor Authentication** check box, under 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 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 set your time preference and MAC address format:

You can format the way time and MAC address is displayed on the GUI.

- a. Under Preferences, select the MAC address format you prefer. The three options are xx:xx:xx:xx:xx:xx, xx-xx-xx-xx-xx-xx, xxxx.xxxx.xxxx.

- b. Under Preferences, select 24-Hour Time if you prefer that time format, or leave the box unchecked if you prefer a 12-hour time format.

- c. Click **Save**.

**5. 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. You can also enable e-mail notifications at the organization level.

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

The Enable Email Notifications page appears.

- b. Click the **Enable Org Notifications** toggle button to enable e-mail notifications at the organization level.

- 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.

**6. 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 Apstra Cloud Services links your Google account and redirects to the My Account page. A message confirms that Juniper Apstra Cloud Services has linked your Google account.

**7. To create an organization:**

- a. Click **Utilities > Create Organization**.

The Create Organization window appears.

- b. Enter a name for the organization.

- c. Click **OK**. The new organization opens in a new tab.

**8. To delete your account:**

- a. Click **Utilities > Delete Account**.

A confirmation message appears.

- b. Click **Yes**.

# Inventory Management

## IN THIS CHAPTER

- [About the Inventory Page | 41](#)

## About the Inventory Page

## IN THIS SECTION

- [Tasks You Can Perform | 41](#)
- [Field Description | 41](#)

The Inventory page lists the devices in an organization. In Juniper Apstra Cloud Services, the Inventory page displays the Apstra Edge devices registered in the organization.

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

### Tasks You Can Perform

You can perform the following tasks on the Inventory page:

- Adopt Apstra Edge devices—You can register an Apstra Edge Device by clicking Adopt Apstra Edge and complete the registration process. See "[Adopt Apstra Edge in Juniper Apstra Cloud Services](#)" on [page 47](#).
- View Apstra Edge devices registered in Juniper Apstra Cloud Services.

### Field Description

[Table 13 on page 42](#) lists the fields on the Inventory page.

**Table 13: Fields on the Inventory Page**

Field	Description
Name	Name of the Apstra data center edge device.
Registration Status	Indicates the registration status of Apstra data center edge device. The edge device installed in Apstra-managed data center must be registered in Apstra Cloud Services application to receive data center event information from Apstra.
Management URL	URL of the Juniper Apstra instance.
Cloud Connectivity	Connectivity status of Apstra Cloud Services application with Juniper Apstra data center edge device. Apstra Cloud Services application can receive event information from Juniper Apstra only if it is connected with the edge device.
Apstra Connectivity	Connectivity status of Juniper Apstra Edge with Juniper Apstra.
Blueprint Name	Name of the blueprint deployed in the data center.
Location	Location of the blueprint.
Status	Status of the blueprint as received from Apstra.



# Audit Logs

## IN THIS CHAPTER

- [Audit Logs Overview | 43](#)
- [About the Audit Logs Page | 44](#)

## Audit Logs Overview

An audit log is a record of activities initiated by a user. You can view a record of user-initiated activities such as accessing, creating, updating, or deleting any resource or component. 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.
- added or deleted a site.

## RELATED DOCUMENTATION

| [About the Audit Logs Page | 44](#)

## About the Audit Logs Page

### IN THIS SECTION

- [Tasks You Can Perform | 44](#)
- [Field Descriptions | 45](#)

To access this page, select **Organization > 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 to view basic information about the log, such as timestamp, the name of the user who initiated the task, the log message, and site details. The View Details field appears for logs generated based on modifications made by the user to existing settings. Click **View Details** to view details about the update.
- Filter the data displayed in the table—You can filter the audit logs based on time interval, administrators, sites, and log messages.
  - To filter logs based on time interval you select, click *Time Interval* (by default it is set to Today). You can choose Last 60 Minutes, Last 24 Hours, Last 7 Days, Custom Date (enter a custom date) Today, Yesterday, This Week, or Custom (enter a custom time range).
  - To filter logs based on administrators, click **admins** (by default it is set to All Admins) or on the downward arrow, from the drop-down list, select the check box next to the administrators whose activities you want to view.
  - To filter logs based on sites, click **sites** (by default it is set to All Sites) or on the downward arrow, from the drop-down list, select the check box next to the sites for which you want to view the activities.
  - To filter logs based on messages, in the **Search by message** field, enter one or more keywords.

To remove the administrators and sites filter criteria, clear the corresponding check boxes in the drop-down list. To remove the messages filter criteria, click **Close** (x) in the check box.

## Field Descriptions

Table 14 on page 45 describes the fields on the Audit Logs page.

**Table 14: Fields on the Audit Logs Page**

Field	Description
Timestamp	Date and time at which the audit log was recorded.
Admin Name	Name and e-mail address of the user who initiated the task.
Message	Description of the logged task.
Site	Name of the site in which the task was initiated.
View Details	Displays a clickable <b>View Details</b> link if any modifications were made by the user to existing settings, such as updating user roles, site settings, and so on.

## RELATED DOCUMENTATION

[Audit Logs Overview](#) | 43

# 3

PART

## Marvis VNA for Data Center

---

[Monitor and Troubleshoot Data Center Events | 47](#)

[Configure Alerts | 59](#)

---

# Monitor and Troubleshoot Data Center Events

## IN THIS CHAPTER

- [Adopt Apstra Edge in Juniper Apstra Cloud Services | 47](#)
- [About the Marvis Page | 49](#)
- [Event Types Displayed in Marvis Actions | 49](#)
- [View Data Center Events in Marvis Actions | 51](#)
- [Access Juniper Apstra from Juniper Apstra Cloud Services | 52](#)
- [Monitor and Troubleshoot Data Center Events from Mist | 53](#)
- [Search Documentation Using Marvis Conversational Interface | 57](#)

## Adopt Apstra Edge in Juniper Apstra Cloud Services

Apstra Edge is a hardware-agnostic virtual device that runs within a container in the data center. Apstra Edge functions like a proxy device in an Apstra-managed data center and maintains connectivity with Juniper Apstra Cloud Services. The edge does not process the events that it receives from Apstra, it just forwards all the event information it receives from Apstra to Juniper Apstra Cloud Services.

To enable Apstra edge to send event information to Juniper Apstra Cloud Services, you need to register Apstra Edge in Juniper Apstra Cloud Services by adopting it. Once the edge is successfully registered, a registration ID is generated for the edge. This registration ID must be configured in Apstra Edge in the Apstra-managed data center.

To set up the edge in Apstra, you need to initialize the docker container and then configure the registration ID that Juniper Apstra Cloud Services generated for the edge. During the registration process the edge retrieves the organization ID, secret, and the device ID. Once registration is completed, the edge can communicate with Juniper Apstra Cloud Services and Juniper Apstra Cloud Services starts receiving event information from Apstra Edge.



**CAUTION:** Apstra Edge uses the edge registration ID generated by Juniper Apstra Cloud Services to retrieve unique organization ID, secret, and device ID during edge

installation. These IDs must be stored securely as they cannot be retrieved after the initial setup is completed.

The docker container on which the edge runs can be installed anywhere in the data center — either on the same virtual machine on which Apstra is running or on a different virtual machine. If edge is installed on the same virtual machine as Apstra is installed, you need to take care during upgrades to ensure that the edge installation is not removed.

After the edge is initialized and configured, the status of the edge will be displayed in Juniper Apstra Cloud Services as **Registered**. The **Cloud Connectivity** status indicates that the edge is connected with the cloud and **Apstra Connectivity** status indicates that the edge is connected with Apstra Controller. That is, you can monitor status of connectivity between Juniper Apstra Cloud Services and the edge and between the edge and Apstra from Juniper Apstra Cloud Services itself without having to access Apstra.

To adopt Apstra Edge:

1. Log in to Juniper Apstra Cloud Services.
2. Navigate to **Organization > Inventory**.
3. Click **Adopt DC Edge**.
4. Enter edge name, management URL (for example, <https://10.28.52.3>), and the user name and password to access Apstra.
5. Click **Adopt**.

The newly added edge is listed on the Inventory page with the status **Unregistered** and **Disconnected**.

6. Install and set up Apstra Edge as described in [Juniper Apstra Edge Setup Guide](#).

The status of Apstra Edge will be displayed as **Registered** and **Connected**, indicating that the edge is registered and connected. A site corresponding to the blueprint deployed in the data center is created on the Sites page.

**NOTE:** Deleting the adopted edge from Juniper Apstra Cloud Services also removes the connectivity with edge. Once the edge is deleted, Juniper Apstra Cloud Services will not be able to receive event information from Apstra. To continue receiving events, you need to complete the registration process again.

## About the Marvis Page

### IN THIS SECTION

- [Tasks You Can Perform](#) | 49

To access this page, click **Marvis**.

### Tasks You Can Perform

- View data center events—View total number of events recorded. You can click an event type to view information about the events reported for the selected event type. You can view more information about the event and the recommended resolution.
- Cross-launch Juniper Apstra—Click **View More** from the event details to view more information about the event. From the pop-up that appears, click **Details** to launch Juniper Apstra and troubleshoot the event.
- View summary of the events reported for the last seven days.
- Search for relevant information—Click **Ask a question** and enter your query. Marvis searches for the requested information in documentation and populates the results.

## Event Types Displayed in Marvis Actions

Marvis Actions in Juniper Apstra Cloud Services displays data center events received from an Apstra-managed data center.

**NOTE:** Though the intent-based analytics in Juniper Apstra supports several predefined probes, Marvis Actions in Juniper Apstra Cloud Services supports only a limited set of probes. [Table 15 on page 50](#) lists the predefined probes that Marvis Actions supports.

Marvis Actions doesn't display all the events that occur in the network. It displays only those events that are actionable. There could be events that might need additional troubleshooting to resolve the issue.

**Table 15: Events displayed in Marvis Actions Dashboard**

Event Type	Events
Layer 1 & 2	<ul style="list-style-type: none"> <li>• Incorrect Cabling</li> <li>• Bad Optics</li> <li>• Interface Flapping</li> <li>• Link Status Mismatch</li> <li>• Packet Discard</li> </ul>
Connectivity	<ul style="list-style-type: none"> <li>• Missing Routes</li> <li>• BGP Mismatch</li> <li>• LAG Imbalance</li> <li>• MLAG Imbalance</li> <li>• BGP Flapping</li> <li>• EVPN Host Flapping</li> <li>• Type-3 Missing Routes</li> <li>• Type-5 Missing Routes</li> <li>• VXLAN Flow Lists Mismatch</li> </ul>
Device	<ul style="list-style-type: none"> <li>• Config Deviation</li> <li>• Deployment Status Mismatch</li> <li>• Resource Health Issues</li> <li>• Environment Health Issues</li> </ul>



Table 15: Events displayed in Marvis Actions Dashboard (*Continued*)

Event Type	Events
Virtual Infra	<ul style="list-style-type: none"> <li>• Config Mismatch</li> <li>• Missing VLANs</li> <li>• MTU Issues</li> <li>• Non-Redundant Hosts</li> </ul>
Security	802.1x Issues
Traffic Capacity	<ul style="list-style-type: none"> <li>• Spine Faults</li> <li>• Critical Services Alerts</li> <li>• Hot/Cold Interface Warning</li> </ul>

## View Data Center Events in Marvis Actions

The Marvis Actions dashboard in the Juniper Apstra Cloud Services application provides network administrators a high-level view of the data center events received from Juniper Apstra-managed data center.

1. Log into Juniper Apstra Cloud Services.

The Marvis Actions dashboard appears displaying the total number of events under each predefined event category.

2. Click an event category to view all the events recorded for that event category.

3. Click an event to view details of that event.

Details of the event and the recommended action are displayed.

4. Click **View More**.

More details about the event such as the site where the event is reported, the device affected, and the date and the time of the event are displayed.

You can mark the status of the event as **In Progress** to indicate that an administrator is working on resolving the event. The event information is removed automatically after the issue is resolved.

**NOTE:** To view the most recent data center events in Marvis Actions, you must refresh the page by using the **Refresh** button in the browser window. Marvis Actions dashboard does not refresh automatically.

## Access Juniper Apstra from Juniper Apstra Cloud Services

Make sure that you have completed the following:

- Installed and set up Apstra Edge.
- Registered Apstra Edge in Juniper Apstra Cloud Services.

Juniper Apstra Cloud Services provides detailed insights into the operations of the data center. The events that Juniper Apstra Cloud Services receives from Apstra Edge are organized in to six event types and displayed in the Marvis Actions dashboard. Each leg in Marvis Actions dashboard corresponds to an event type. You can click the Marvis Actions leg for an event type to view all the events for the selected event type. Click an event to know the reason for the event and recommended resolution. You can then launch Juniper Apstra from Juniper Apstra Cloud Services to troubleshoot and resolve the event. As the information in the Marvis Actions dashboard is real time, network administrators can resolve events even before they impact network traffic.

### 1. Log into Juniper Apstra Cloud Services.

Marvis Actions dashboard is displayed. The Marvis Actions dashboard for data center displays the events categorized by events type. Each Marvis Actions leg displays the total number of events reported for an event type.

### 2. Click the Marvis Actions leg to view the events for the selected event type.

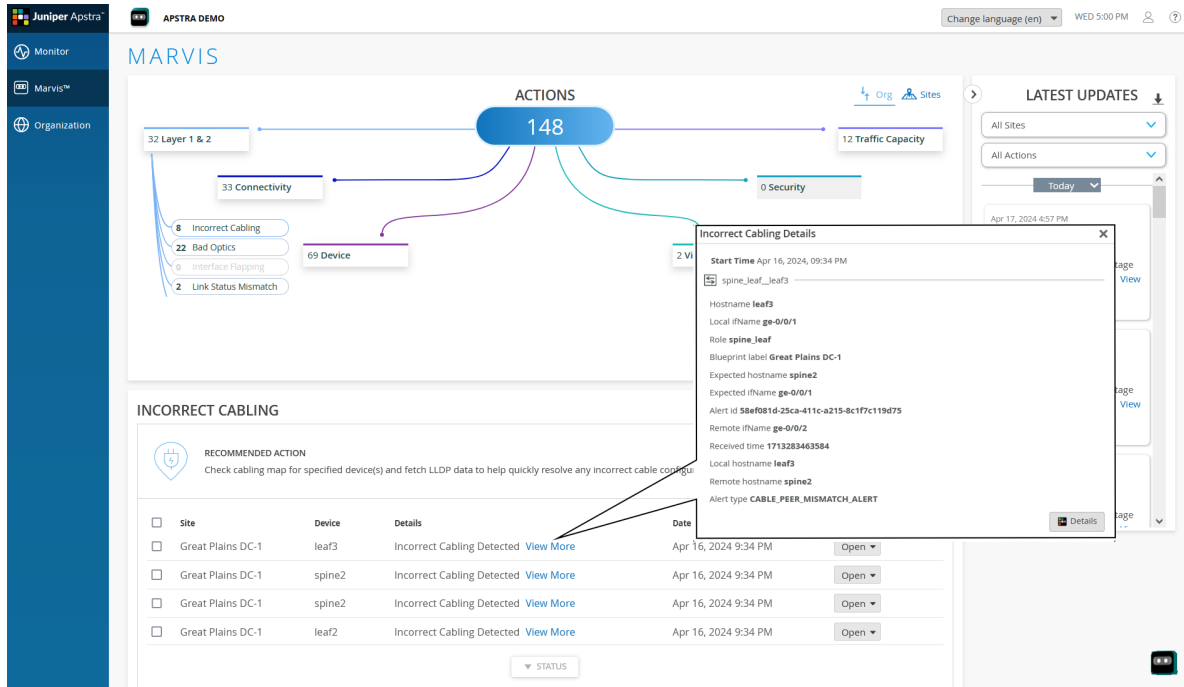
The various events reported for the event type are displayed.

### 3. Click an event.

More details about the event such as the site where the event is reported, the device affected, and the date and the time of the event are displayed.

### 4. Click **View More** to view more information about the event.

A pop-up appears displaying more information about the event.



5. Click **Details** to access Juniper Apstra application.

Juniper Apstra opens in a new browser window or tab.

## Monitor and Troubleshoot Data Center Events from Mist

If you manage your enterprise network using Mist and data center using Apstra, you can monitor data center events too from Mist by linking the organization in Mist with the organization in Juniper Apstra Cloud Services. Once the organization in Mist is linked with the organization in Juniper Apstra Cloud Services, you can view the total number of data center events in **Data Center/Application** category in Marvis Actions in Mist. You can also access Juniper Apstra Cloud Services by clicking **Data Center/Application** and view more detailed information about an event.

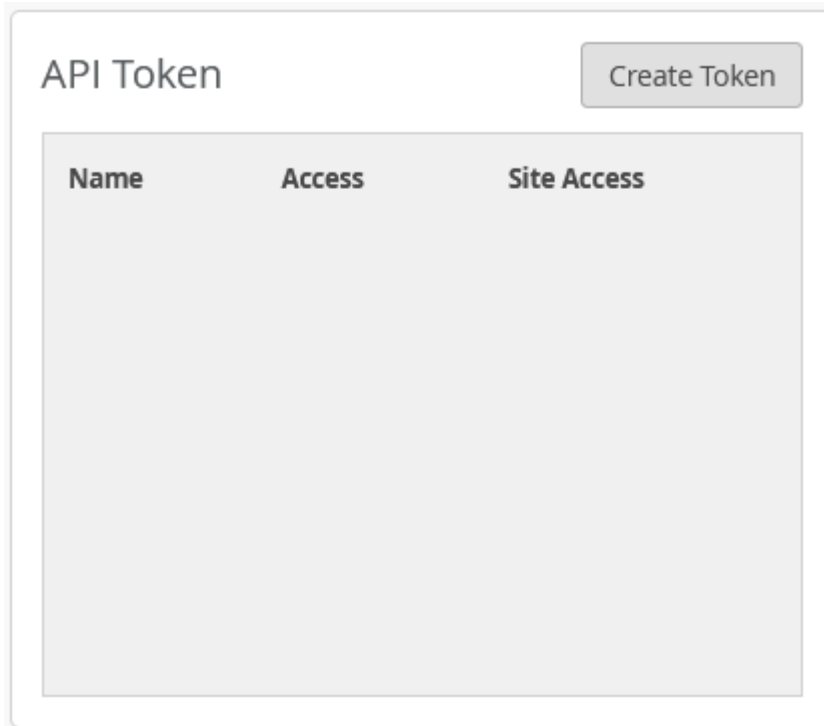
**NOTE:** You must be a user with the superuser role to link the organizations in Juniper Apstra Cloud Services and Mist.

Make sure you have the following:

- Login credentials to access Juniper Apstra Cloud Services
- Login credentials to access Mist
- API token generated in Juniper Apstra Cloud Services

To access Juniper Apstra Cloud Services from Mist:

1. Log in to Juniper Apstra Cloud Services and navigate to the **Organization > Settings** page.
2. Locate the API Token tile and click **Create Token**.



The screenshot shows a web interface for managing API tokens. At the top left, the text "API Token" is displayed. To its right is a button labeled "Create Token". Below these elements is a large, empty rectangular area with a light gray background, which serves as a table for listing tokens. The table has three columns: "Name", "Access", and "Site Access".

Name	Access	Site Access
------	--------	-------------

3. Enter a name for the token and click **Generate**.

## Create Token ✕

Please save your key to a safe place. You will see the key only once upon creation. You won't be able to retrieve it later

### Name

### Access Level

☒ **Super User**  
Full access to organization and all its sites, able to create new sites, and unable to manage API tokens

☐ **Network Admin**  
Full access to selected sites

☐ **Observer**  
Monitor only access to selected sites

☐ **Helpdesk**  
Helpdesk monitoring and workflow for selected sites


### Site Access

All Sites

Site Groups

Specific Sites

### Key



Done

Cancel

- After the token is generated, click the **Copy** button.

**NOTE:** Store the API token key in a secure location. You can copy the key only once and cannot be retrieved later.

5. Click **Done**.
6. Log in to the Mist portal.
7. Navigate to **Organization > Settings** page.
8. Locate the **Apstra Cloud Services Integration** tile.

The screenshot shows the Juniper Mist APSTRA DEMO interface. The left sidebar contains navigation links: Monitor, Marvis™, Clients, Access Points, Switches, WAN Edges, Mist Edges, Private 5G, Location, Analytics, Site, and Organization. The main content area displays several configuration tiles. The 'Apstra Cloud Services Integration' tile is highlighted with a blue border and contains the following fields:

- Connect your Data Center managed by Apstra.
- Organization ID:
- API Token Name:
- API Token:

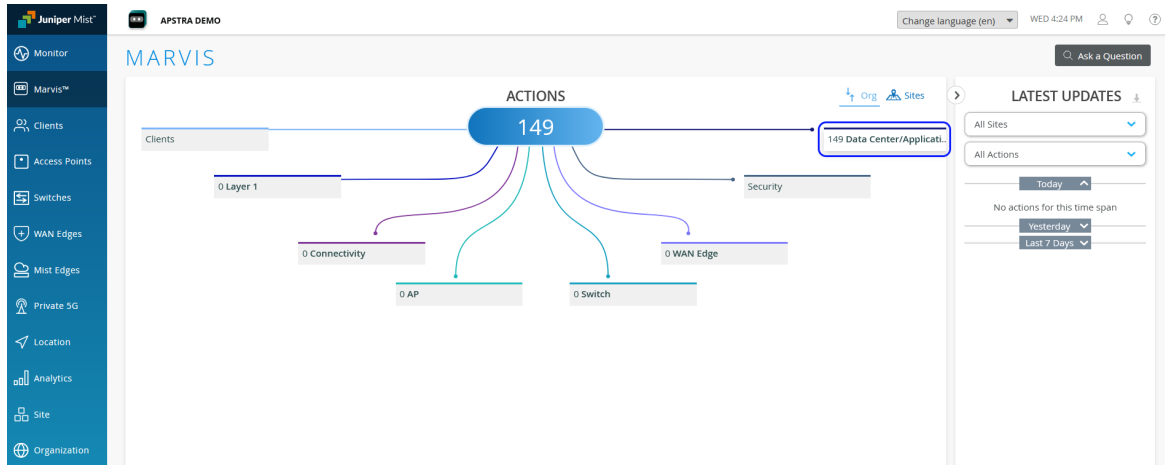
Other visible tiles include 'Third Party Token' with a 'Name' field (containing 'X-CP-API-ID') and an 'Add Credentials' button; 'Marvis Minis' with a 'Disable Marvis Minis' checkbox and 'Custom URLs' section; and 'Application Insights Integration' with a 'Link Account' dropdown and a table with columns: Status, Application, Company Name, and Limit Daily A.

Enter the following information:

- **Organization ID**—Copy the organization ID from Juniper Apstra Cloud Services and paste it here.
- **API Token Name**—Enter API token name that you defined in Juniper Apstra Cloud Services.
- **API Token**—Copy the API token generated in step 3 in Juniper Apstra Cloud Services and paste it here.

9. Click **Save**.

The organizations in Mist and Juniper Apstra Cloud Services are linked now. In a few minutes, you'll notice that the **Data Center/Application** event category is active and displays the total number of data center events.



- Click **Data Center/Application** to launch Juniper Apstra Cloud Services. Juniper Apstra Cloud Services opens in a new browser window or tab.



## Search Documentation Using Marvis Conversational Interface

Marvis Conversational Interface (CI) is an AI-enabled search interface that administrators can use to search documentation. Marvis CI supports natural language processing (NLP). Network administrators can use Marvis CI to quickly search for information about events or network issues from Juniper Networks Documentation (TechLibrary) and Knowledge Base. Marvis CI looks up relevant documentation repositories and generates the answer. This enables network administrators to resolve the issues faster without having to depend on multiple resources to obtain the required information.

- Log into Juniper Apstra Cloud Services.
- Click **Marvis CI** icon at the top left near the organization name or at the bottom right of the UI. Marvis CI panel appears at the bottom right of the page.
- Enter the search string or key word that you want to look up. Marvis CI generates a response to your query and provides links to additional resources that provide the requested information.

**NOTE:** This feature is provided as a technology preview. For more information about technology previews, see [Juniper Apstra Technology Preview](#).



## CHAPTER 8

# Configure Alerts

## IN THIS CHAPTER

- [About the Alerts Page | 59](#)
- [Configure an Alert Template | 60](#)
- [Configure E-mail Notification for Alerts | 61](#)

## About the Alerts Page

### IN THIS SECTION

- [Tasks You Can Perform | 60](#)

To access this page, click **Monitor > Alerts**.

The Alerts page displays the alerts generated to notify administrators about anomalies in the network. To monitor specific alerts, you can apply an alert template for your organization. Alert templates filter the alert list to display only those alerts that are tracked in the template. You can also choose to receive e-mail notifications for the alerts.

The widgets display the total number of critical alerts that need immediate attention, warning alerts, and informational alerts.

**NOTE:** To receive e-mail notifications, you must configure Webhooks on the **Organization > Settings** page.

## Tasks You Can Perform

- View alerts—View Alerts for the selected period and their severity for the entire organization or for specific sites in the organization.
- Configure e-mail notification for alerts—Configure to send email notification to site administrator or organization administrator when an alert is generated.
- Create an alert template—Create an alert configuration template that you can apply at the site or organization-level.
- Download alert details in a CSV file—Click the download button next to **Alerts Configuration**.

## Configure an Alert Template

Juniper Apstra Cloud Services allows you to create alert templates to notify administrators about specific event types. You can apply an alert template to an organization to display only a filtered list of alerts on the Alerts page or send email notifications. If an alert template is not configured, all generated alerts are displayed on the Alerts page.

To create an alert template:

1. Log into Juniper Apstra Cloud Services.
2. Click **Monitor > Alerts > Alerts Configuration**.
3. Click **Create Template**.
  - a. Specify whether the template applies to the entire organization or for specific sites only.
  - b. Specify a template name.
  - c. Specify who should receive e-mail notifications (organization administrators, site administrators, or other specified e-mail addresses)
  - d. Select **Enable Alert** and select the alert types that should be displayed on the Alerts page, and **Email Notification** to send email notification for the selected alerts.
4. Click **Create**.

The alert template is created.

## Configure E-mail Notification for Alerts

As an administrator, you can configure Juniper Apstra Cloud Services to send alert notification through e-mail. This enables administrators to respond to events quickly. You also create an alert template and apply at the site-level or at the organization-level.

Follow these steps to configure alert notification:

1. Log into Juniper Apstra Cloud Services.

2. Click **Monitor > Alerts**.

The Alerts page is displayed.

- Select **To organization admins** to send e-mail notifications to administrators of the organization
- Select **To site admins** to send e-mail notifications to administrators of the site

3. From the Alert Types, select the alerts that you want to be notified in e-mail.

- Enable Alerts—Select to display alerts on the Alerts page.
- Send Email Notification—Select to send e-mail notifications.

4. Click **Save**.

You will receive an e-mail notification when an alert is generated.