JUNIPER NETWORKS | Engineering Simplicity

# Day One+

## JSI on Juniper Support Portal Quick Start (LWC)

IN THIS GUIDE



## Step 1: Begin

IN THIS SECTION



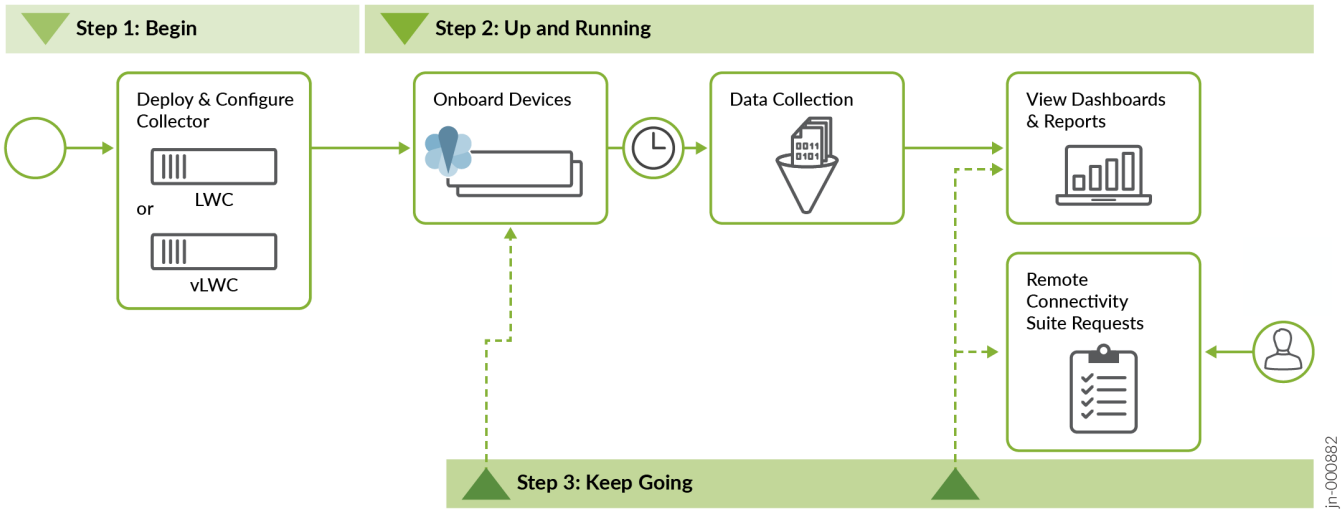
In this guide, we provide a simple, three-step path, to quickly get you up and running with the Juniper Support Insight (JSI) solution. We've simplified and shortened the installation and configuration steps.

# Meet Juniper Support Insights

Juniper® Support Insights (JSI) is a cloud-based support solution that gives IT and network operations teams operational insights into their networks. JSI aims to transform the customer support experience by providing Juniper and its customers with insights that help improve the network performance and uptime. JSI collects data from Junos OS-based devices on customer networks, correlates it with Juniper-specific knowledge (such as service contract status, and End of Life and End of Support states), and then curates that into actionable insights.

At a high level, getting started with the JSI solution involves the following steps:

1. Installing and configuring a Lightweight Collector (LWC) device
2. Onboarding a set of Junos devices to JSI to initiate data collection
3. Viewing notifications about device onboarding and data collection
4. Viewing operational dashboards and reports




**NOTE**: This Quick Start guide assumes that you have ordered the JSI-LWC solution, which is available as part of Juniper Care support service, and that you have an active contract. If you have not ordered the solution, please contact your Juniper Account or Services teams. Accessing and using JSI is subject to the Juniper Purchase and License Agreement (JPLA). For general information on JSI, see Juniper Support Insights Datasheet.

# Install the Lightweight Collector

IN THIS SECTION



The Lightweight Collector (LWC) is a data collection tool that gathers operational data from Juniper devices on customer networks. JSI uses this data to provide IT and network operations teams with actionable operational insights into the onboarded Juniper devices on customer networks.

You can install the LWC on your desktop, in a two-post or four-post rack. The accessory kit that ships in the box has the brackets you need to install the LWC in a two-post rack. In this guide, we show you how to install the LWC in a two-post rack. If you need to install the LWC in a four-post rack, you'll need to order a four-post rack mount kit.

## What's in the Box?

- The LWC device
- AC power cord for your geographic location
- AC power cord retainer clip
- Two rack mount brackets
- Eight mounting screws to attach the mounting brackets to the LWC
- Two SFP modules (2 x CTP-SFP-1GE-T)
- RJ-45 cable with a DB-9 to RJ-45 serial port adapter
- Four rubber feet (for desktop installation)

## What Else Do I Need?

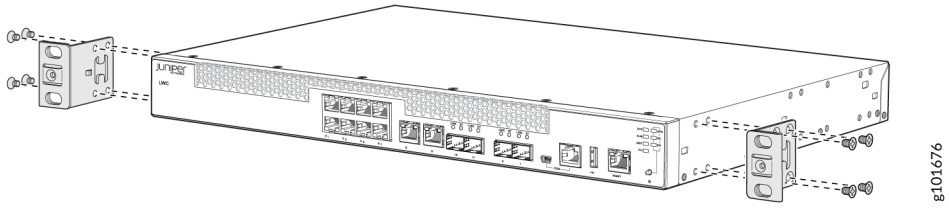
- Someone to help you mount the LWC in the rack.
- Four rack mount screws to secure the mounting brackets to the rack
- A number 2 Phillips (+) screwdriver

# Mount a Lightweight Collector on Two Posts in a Rack

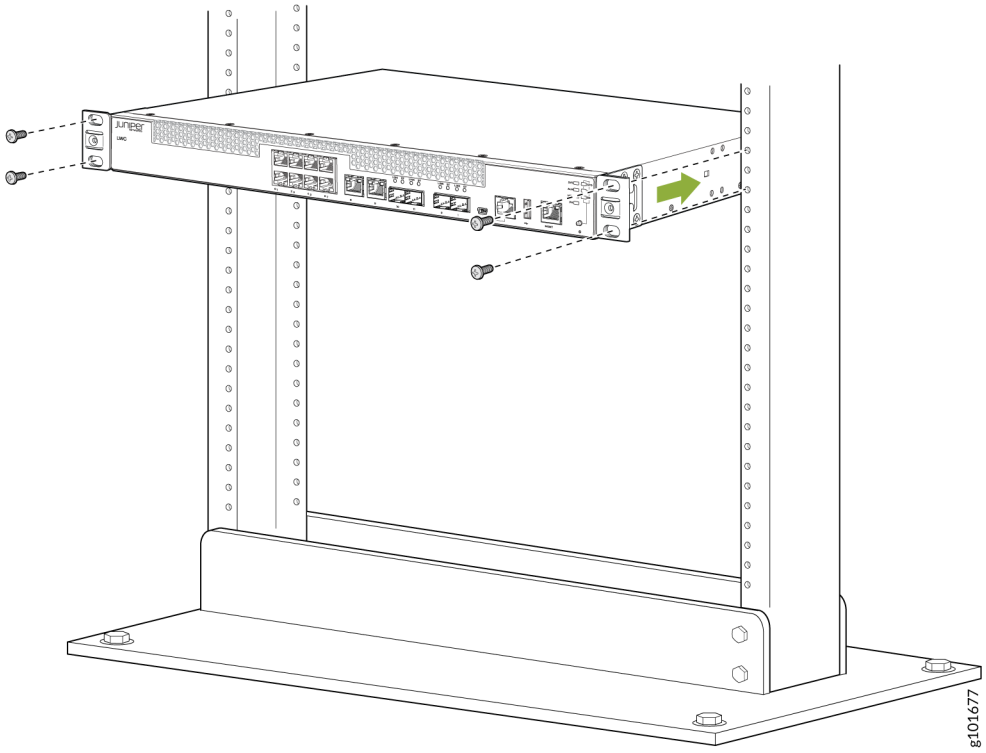
You can mount a Lightweight Collector (LWC) on two posts of a 19-in. rack (either a two-post or a four-post rack).

Here's how to mount the LWC on two posts in a rack:

1. Place the rack in its permanent location, allowing adequate clearance for airflow and maintenance, and secure it to the building structure.
2. Remove the device from the shipping carton.
3. Read General Safety Guidelines and Warnings.
4. Attach the ESD grounding strap to your bare wrist and to a site ESD point.
5. Secure the mounting brackets to the sides of the LWC using eight screws and the screwdriver. You'll notice there are three locations on the side panel where you can attach the mounting brackets: front, center, and rear. Attach the mounting brackets to the location that best suits where you want the LWC to sit in the rack.




6. Lift the LWC and position it in the rack. Line up the bottom hole in each mounting bracket with a hole in each rack rail, making sure the LWC is level.

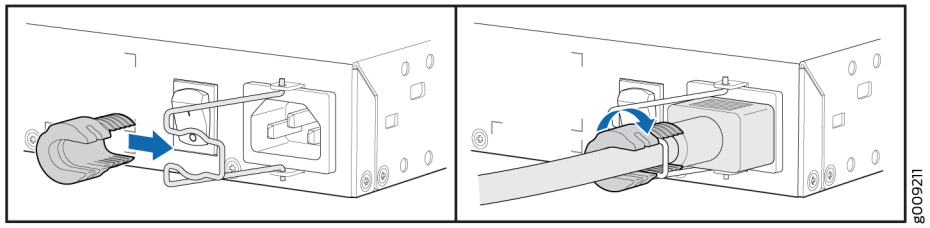



7. While you're holding the LWC in place, have a second person insert and tighten the rack mount screws to secure the mounting brackets to the rack rails. Make sure they tighten the screws in the two bottom holes first and then tighten the screws in the two top holes.

8. Check that the mounting brackets on each side of the rack are level.

## Power On

1. Attach a grounding cable to earth ground and then attach it to the Lightweight Collector's (LWC's) grounding points.
2. Turn off the power switch on the LWC rear panel.
3. On the rear panel, insert the L-shaped ends of the power cord retainer clip into the holes in the bracket on the power socket. The power cord retainer clip extends out of the chassis by 3 inches.
4. Insert the power cord coupler firmly into the power socket.
5. Push the power cord into the slot in the adjustment nut of the power cord retainer clip. Turn the nut until it is tight against the base of the coupler and the slot in the nut is turned 90° from the top of the device.



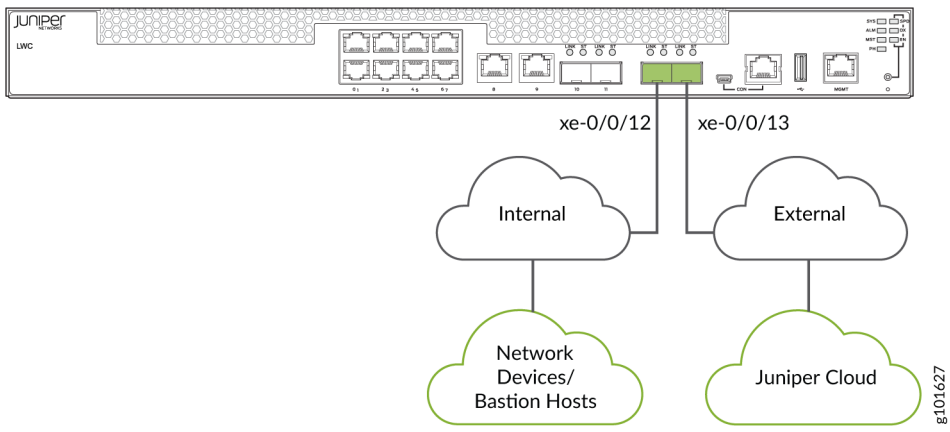

6. If the AC power source outlet has a power switch, turn it off.
7. Plug in the AC power cord to the AC power source outlet.
8. Turn on the power switch on the LWC's rear panel.
9. If the AC power source outlet has a power switch, turn it on.
10. Verify that the power LED on the LWC front panel is green.

## Connect the Lightweight Collector to the Networks

The Lightweight Collector (LWC) uses an internal network port to access the Juniper devices on your network, and an external network port to access Juniper Cloud.

Here's how to connect the LWC to the internal and external network:

1. Connect the internal network to the 1/10-Gigabit SFP+ port **0** on the LWC. The interface name is xe-0/0/12.
2. Connect the external network to the 1/10-Gigabit SFP+ port **1** on the LWC. The interface name is xe-0/0/13.




# Configure the Lightweight Collector

**IN THIS SECTION**



The LWC is preconfigured to support IPv4 and Dynamic Host Configuration Protocol (DHCP) on both the internal and external network ports. When you power on the LWC after completing the required cabling, a zero touch experience (ZTE) process to provision the device is initiated. Successful completion of the ZTE results in the device establishing IP connectivity on both the ports. It also results in the external port on the device establishing connectivity to Juniper Cloud via. discoverable reachability to the Internet. If the device fails to automatically establish IP connectivity and reachability to the Internet, you must configure the LWC device manually, by using the LWC captive portal.

**NOTE**: You must connect to the captive portal from a local IP address. Connection to the captive portal from the browser will fail if the connection request originates from a non-local network.

Before you configure the Lightweight Collector (LWC), refer to the "Internal and External Network Requirements" on page 6.

## Internal and External Network Requirements

The LWC device requires:

- An internal network port (interface xe-0/0/12) that connects the LWC to the Juniper devices on the network.
- An external network port (interface xe-0/0/13) that connects the LWC to the Juniper Virtual Private Cloud.

Before connecting the LWC to the internal network, ensure that you have:

- A DHCP or static IP address.
- IP connectivity to the Domain Name Server (DNS), all the direct devices on the network, and bastion hosts (if applicable) used to access the devices.

  **NOTE**: Bastion hosts utilize a SOCKS5 proxy server to reach target devices in the customer's network. Bastion hosts also support connection hopping, where an SSH session is first established with a customer's Linux-based device, which then initiates a subsequent SSH session to the target device.

- Enabled NETCONF in the Junos OS configuration of all target Juniper devices. The LWC uses SSH credentials to connect to the devices on the network and, if used, bastion hosts.
  See also Establish an SSH Connection for a NETCONF Session.

Before connecting the LWC to the external network, ensure that you have the following ready:

- A DHCP or static IP address.
- A DNS server in case you have selected a static address. In case of any subsequent change to the DNS, you must inform Juniper about it and get it updated. Otherwise, the LWC might lose connectivity to the external endpoints. The LWC supports real static, private static, or DHCP addresses. It prefers Network Address Translation (NAT).
- Accessibility to the DNS and IP addresses specified in Table 1 on page 7 through the IP addresses assigned to xe-0/0/13 on the LWC.

**NOTE**: The internal and external interfaces must each have unique DNS entries.

**Table 1: Outbound Connectivity Requirements**

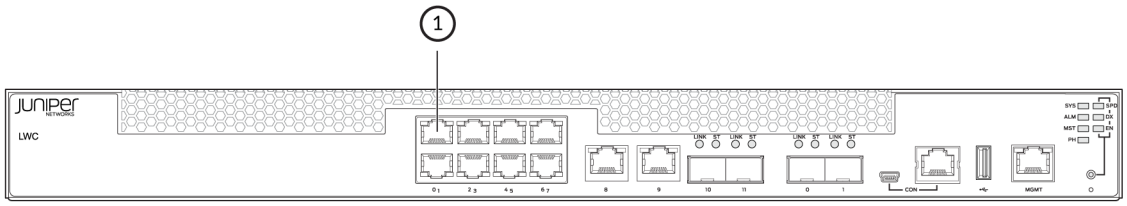
| Description | DNS Name | IP Address | Port |
|---|---|---|---|
| Juniper cloud | AWSProxy-prod.jssprod.junipercloud.net | 52.223.32.79, 35.71.174.221, 35.164.173.102, 52.26.8.178, 54.149.201.209 | 443 |

The internal and external interfaces must be assigned IP addresses from different subnets.

## Configure the LWC Manually

Here's how to configure the LWC device manually, by using the LWC captive portal:

1. Disconnect your computer from the Internet.
2. Connect the computer to the port ge-0/0/0 on the LWC (labeled as **1** in the image below) using an Ethernet cable (RJ-45). The LWC assigns an IP address to the Ethernet interface of your computer through DHCP.




3. Open a browser on your computer and enter the following URL to the address bar: https://cportal.lwc.jssdev.junipercloud.net/.

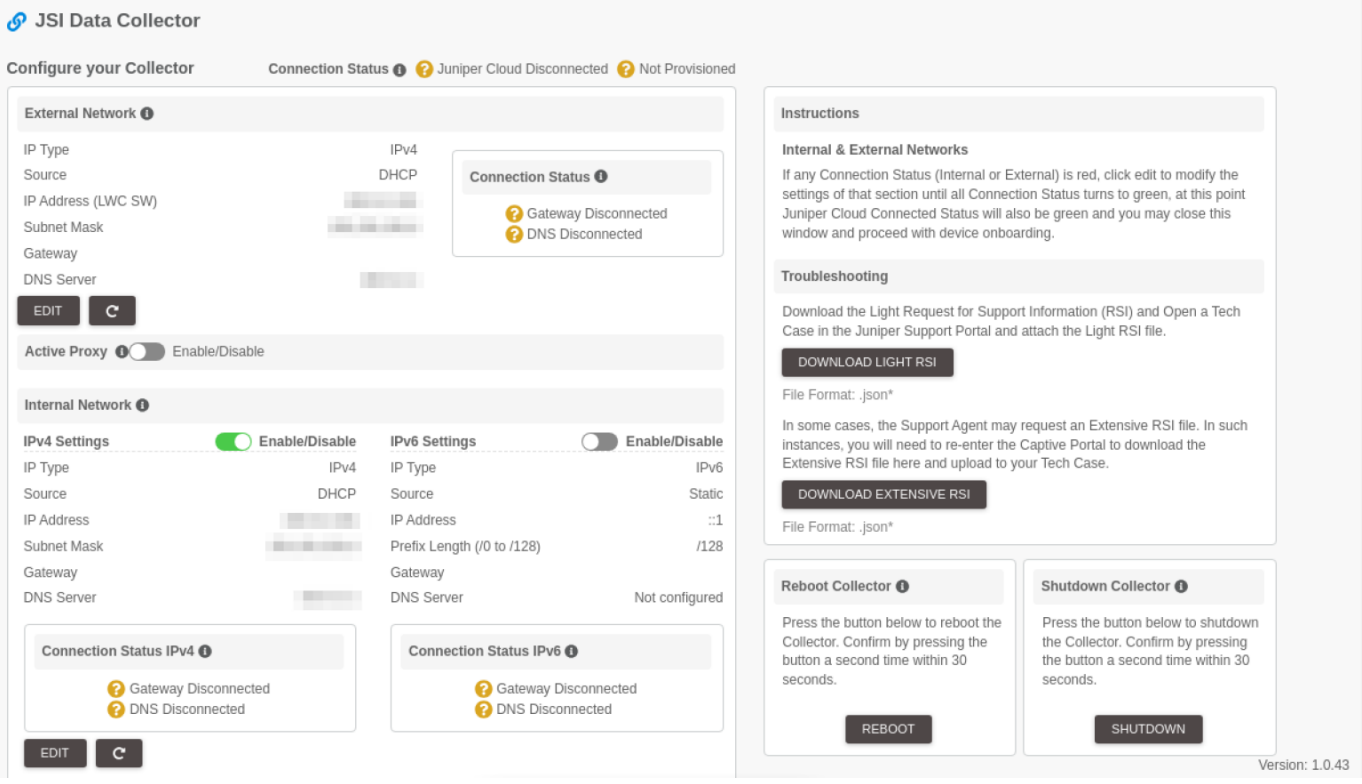
   The **JSI Data Collector** login page appears.

> **NOTE**: On Captive Portal versions earlier than 1.0.43, if you are unable to configure an IP address via. DHCP, you must manually assign an IP address to the connecting device and accept an unsecured connection. For more information, see KB70138.

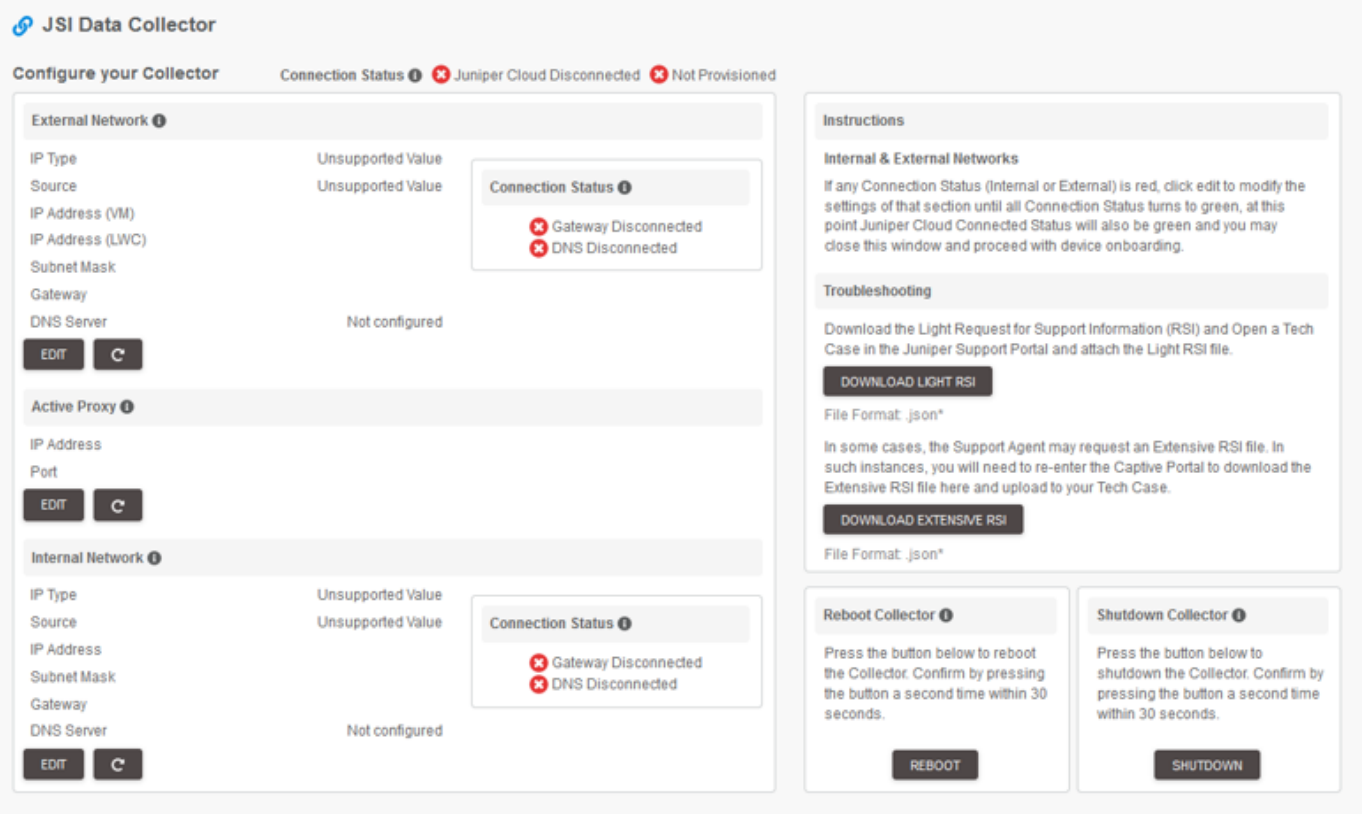
4. Enter the LWC serial number in the **Serial Number** field and then click **Submit** to log in.

   On successful login, the **JSI Data Collector** page appears.

   The following image displays the JSI Data Collector page when the LWC is not connected (version 1.0.43 and later releases).




   The following image displays the JSI Data Collector page when the LWC is not connected (releases earlier than version 1.0.43).




**NOTE**: If the default DHCP configuration on the LWC is successful, the captive portal shows the LWC's connection status as connected, and populates the fields in all the configurations sections appropriately.

Click the **Refresh** icon under the External Network or Internal Network sections to refresh the current connection states for that section.

The **JSI Data Collector** page displays configuration sections for the following:

- **External Network**—Lets you configure external network port that connects the LWC to the Juniper's Cloud. Supports DHCP and static addressing. The External Network configuration is used to perform device provisioning.
- **Internal Networks**—Lets you configure the internal network port that connects the LWC to the Juniper devices on your network. Supports DHCP and static addressing.
- **Active Proxy**—Lets you configure the active proxy IP address as well as the port number if your network infrastructure controls access to the Internet though an active proxy. You need not configure this element if you are not using an active proxy.

5. Click the **Edit** button under the element that needs to be updated.

   You need to modify the fields in:

   - The **Internal Network** and **External Network** sections if their connection states indicate that they are disconnected.

**NOTE**:

- The IP addresses assigned to the internal and external interfaces must be from different subnets. This requirement applies to both DHCP and static configurations.
- The internal and external interfaces must each have unique DNS entries.

  Ensure that these interfaces can reach their respective DNS servers over both UDP and TCP on port 53.

You must not use the same IP address or DNS entry for both the interfaces.

- The **Active Proxy** section if you are using an active proxy. An Active proxy uses SOCKS5 proxies to route connections to the target Juniper devices in the customer's network.

  When configuring an Active Proxy, you must also configure your proxy server to specify a parent proxy that points to `AWSProxy-prod.jssprod.junipercloud.net` on port 443. This parent proxy ensures proper communication between your LWC and the Juniper Cloud.

  For example, if you are using Squid Proxy, add the following configuration:

```
cache_peer awsproxy-prod.jssprod.junipercloud.net parent 443 0 no-query default
acl jsas <ext-IP-address-of-LWC>
never_direct allow jsas
```

  Where, `<ext-IP-address-of-LWC>` is the IP address configured on the LWC's external interface.

  Failure to properly configure the parent proxy will prevent the LWC from establishing connectivity with the Juniper Cloud, even if the proxy IP and port are correctly entered in the LWC configuration. For more information, see KB82549.

  If you choose to use an active proxy, ensure that it forwards all the traffic from the LWC to the AWS cloud proxy. See, Outbound Connectivity Requirements table in Table 1 on page 7 for the AWS cloud proxy URL and ports. Juniper cloud services blocks all the inbound traffic coming through any path other than the AWS cloud proxy.

**NOTE**: If you choose to use an active proxy, ensure that the LWC's external interface IP configuration can reach the active proxy's URL or IP address.

**NOTE**: In version 1.0.43 and later releases, the **Active Proxy** section is collapsed by default if an active proxy is disabled or not configured. To configure, click **Enable/disable** to expand the **Active Proxy** section.

6. After modifying the fields, click **Update** to apply the changes and return to the homepage (the JSI Data Collector page).

   If you want to discard your changes, click **Cancel**.

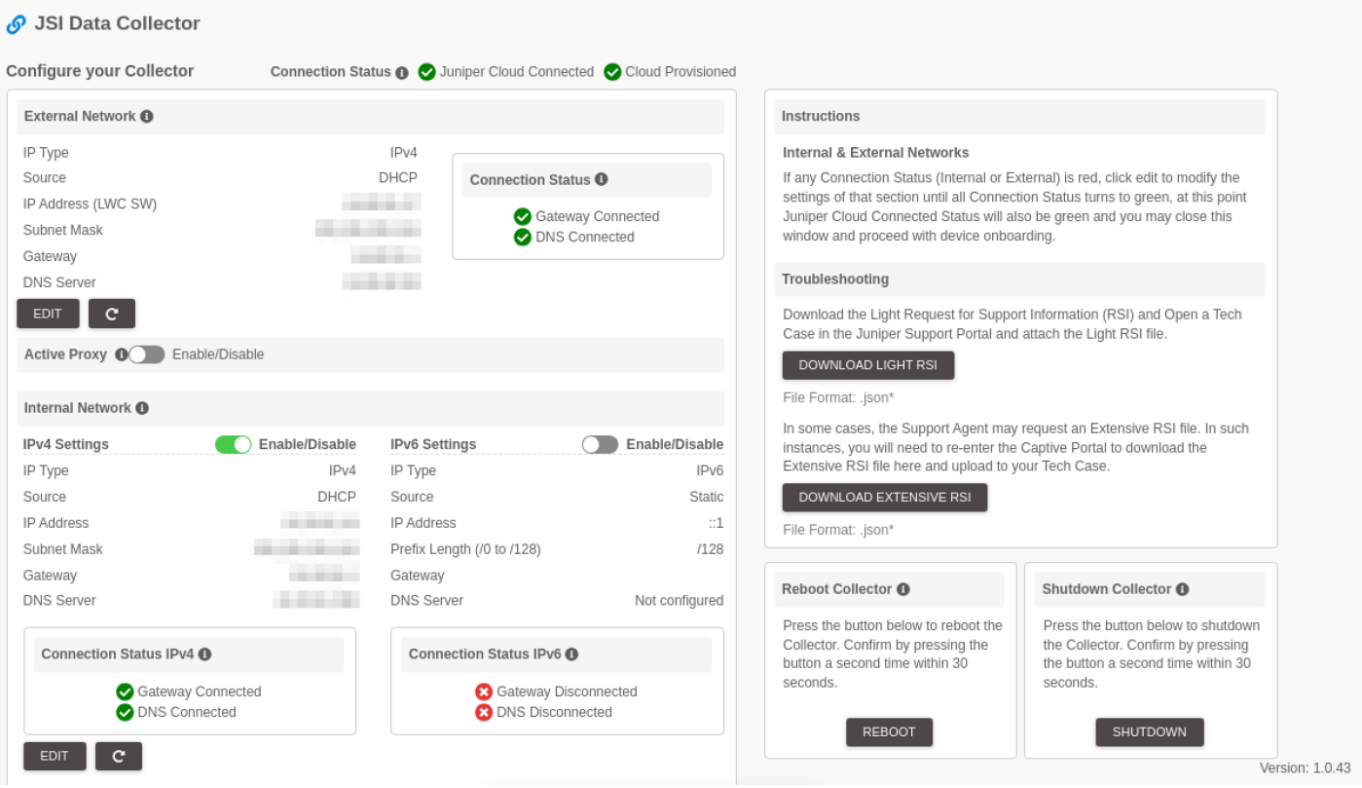
If the LWC connects to the gateway and DNS successfully, the respective configuration element (internal or external network section) on the JSI Data Collector homepage shows the connection status as **Gateway Connected** and **DNS Connected** with green tick marks against them.

The JSI Data Collector homepage displays the **Connection Status** as:

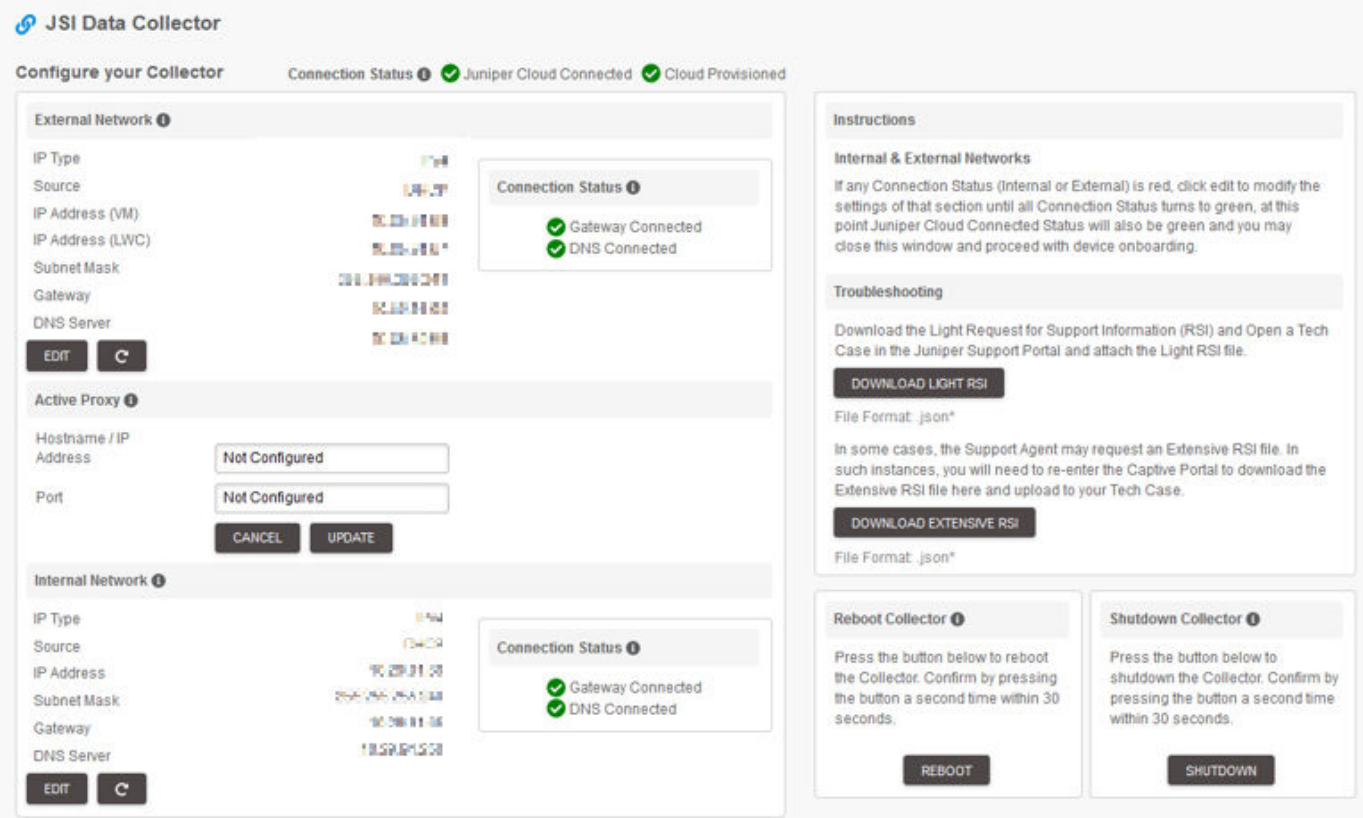
- **Juniper Cloud Connected** if the external connectivity to the Juniper Cloud is established and the active proxy (if applicable) settings are correctly configured.
- **Cloud Provisioned** if the device is connected to Juniper Cloud and has completed the Zero Touch Experience (ZTE) process. After the Cloud connection status becomes **Juniper Cloud Connected**, it takes about 10 minutes for the provision status to become **Cloud Provisioned**.

**NOTE**: Once the LWC is connected to Juniper Cloud and maintains a stable connection for over 24 hours, automatic upgrade will be enabled for the device.

The following image displays the JSI Data Collector page when the LWC is connected successfully (version 1.0.43 and later releases).




The following image displays the JSI Data Collector page when the LWC is connected successfully (releases earlier than version 1.0.43).




If the LWC does not connect to the cloud, click **Download Light RSI** to download the light RSI file, create a Tech Case in the Juniper Support Portal, and attach the downloaded RSI file to the case.

In some cases, the Juniper support engineer might ask you to attach the Extensive RSI file to the case. To download it, click the **Download Extensive RSI**.

The Juniper support engineer might ask you to reboot the LWC for troubleshooting. To reboot the LWC, click **REBOOT**.

If you want to shut down the LWC, click **SHUTDOWN**.

# Step 2: Up and Running

**IN THIS SECTION**

Prepare for a Remote Connectivity Suite Request | 20

Now that you've deployed the Lightweight Collector (LWC), let's get you up and running with Juniper Support Insights (JSI) on Juniper Support Portal!

## Access Juniper Support Insights

To access Juniper Support Insights (JSI), you must register on the User Registration portal. You also require a user role (Super Admin, Admin or Standard) assigned. To get a user role assigned, contact Juniper Customer Care or your Juniper Services team.

JSI supports the following user roles:

- **Standard**—The Standard users can view the device onboarding details, operational dashboards, and reports.
- **Admin**—The Admin users can onboard devices, perform JSI management functions, view the operational dashboards and reports.
- **Super Admin**—The Super Admin users can perform all the functions as a regular admin, and also manage the JSI roles to grant and revoke access (from **Insights** menu > **Advanced Settings** > **User Role Management** page).

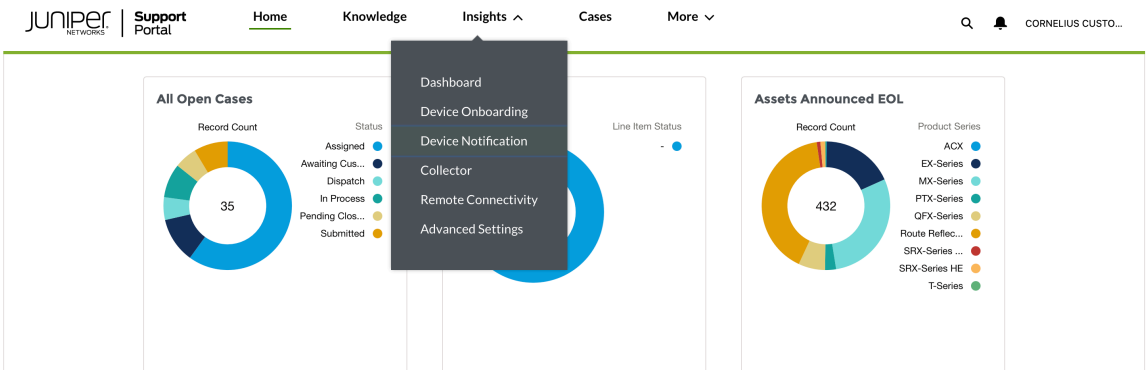
  **NOTE**: Users managed by the super admin must be associated with the same account as the LWC.
  To locate a user, the super admin must enter the full email address (example: jsiuser@email.com) in the search field of the **User Role Management** page. If searching for the user by their full email address does not yield any results, contact your Juniper Services team for assistance.

- **RCS Operator**—The RCS Operator users can view device onboarding details, operational dashboards, and reports. In addition, they can receive and approve RCS requests.

Here's how to access JSI:

1. Log in to Juniper Support Portal (**supportportal.juniper.net**) by using your Juniper Support Portal credentials.
2. On the **Insights** menu, click:
   - **Dashboards** to view of a set of operational dashboards and reports.
   - **Device Onboarding** to perform device onboarding to initiate data collection.
   - **Device Notifications** to view notifications about device onboarding, data collection, and errors.
   - **Collector** to view the details of the LWC associated with the account.
   - **Remote Connectivity** to view and manage Remote Connectivity Suite requests for a seamless device data collection process.

- **Advanced Settings** to configure remote connectivity settings (see "Configure RCS Device Settings" on page 22), and manage JSI user roles.




## View the Lightweight Collector Connection Status

**IN THIS SECTION**



You can view the Lightweight Collector (LWC) connection status on the following portals:

- Juniper Support Portal
- The LWC captive portal. The captive portal provides a more detailed view, and has options that let you change the LWC configuration settings and perform troubleshooting.

### View the Connection Status on Juniper Support Portal

Here's how to view the LWC connection status on Juniper Support Portal:

1. On Juniper Support Portal, click **Insights** > **Collector**.
2. Check the summary table to see the Connection Status of the LWC. The status should be shown as **Connected**.

   If the status is shown as **Disconnected**, check if the LWC is installed and the two ports are cabled correctly. Ensure that the LWC fulfills the Internal and External Network Requirements as specified in the LWC Platform Hardware Guide. In particular, ensure that the LWC meets the Outbound Connectivity Requirements.

### View the Connection Status on the Captive Portal

See "Configure the Lightweight Collector" on page 6 for more information.

# Onboard Devices

You'll need to onboard devices to initiate a periodic (daily) data transfer from the devices to the Juniper Cloud. Here's how to onboard devices in a JSI setup that uses an LWC:

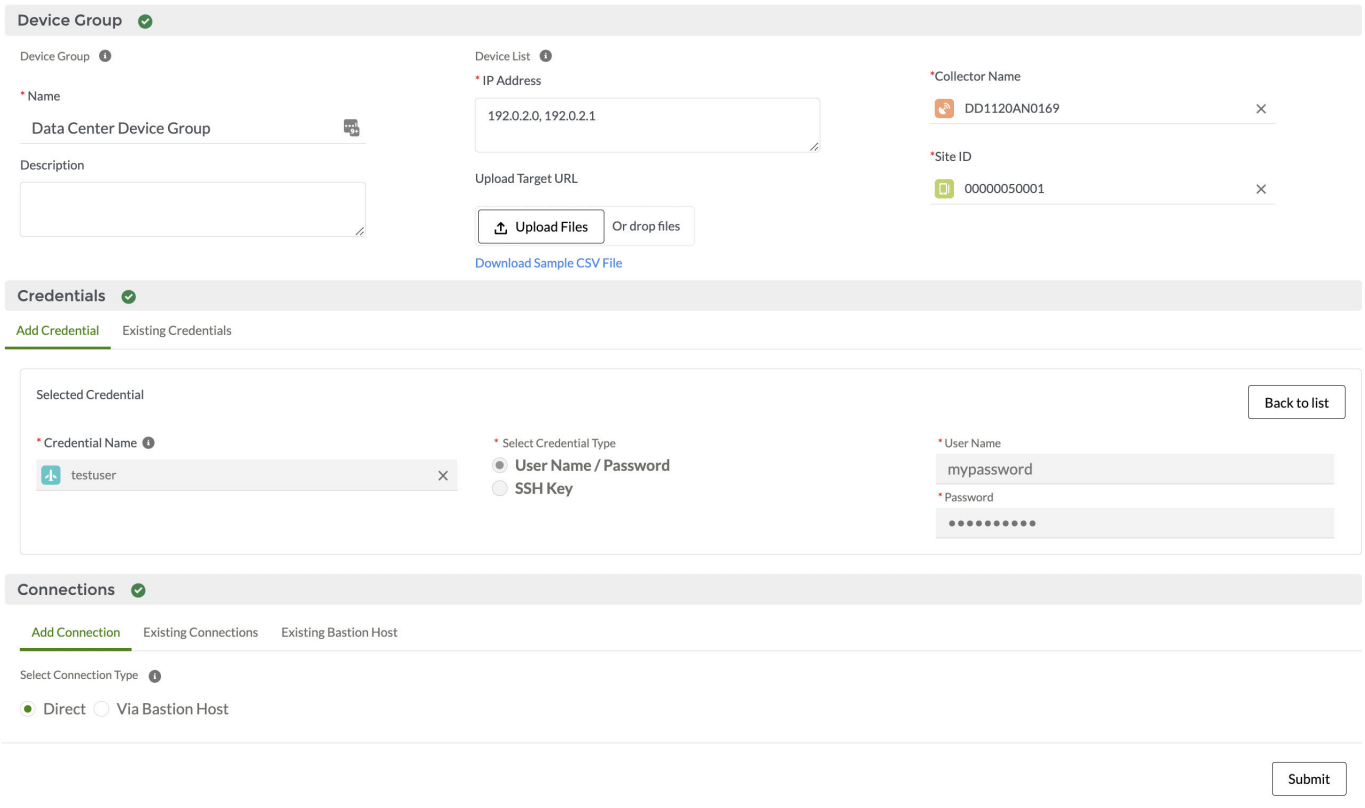
**NOTE**: You must be an admin user to onboard a device.

**NOTE**: Ensure that the NETCONF SSH subsystem is configured on your Juniper devices (on port 22) to onboard these devices to JSI. JSI supports NETCONF SSH sessions on port 22 only. JSI NETCONF sessions on other ports, such as port 830, are currently not supported.

**NOTE**: For information on Junos configurations and permissions required for JSI, see the FAQ - What permissions does the JSI user need in Junos to operate JSI?

Here's how to onboard devices to JSI:

1. On Juniper Support Portal, click **Insights** > **Device Onboarding**.
2. Click **New Device Group**. The following image represents the device onboarding page with some sample data filled in.




3. In the **Device Group** section, enter the following details for the devices to be associated with the LWC:

- **Name**—A name for the device group. A Device Group is a collection of devices with a set of common credentials and modes of connection. The operational dashboards and reports use the device groups to provide a segmented view of the data.

  **NOTE**: Data displayed depends on the end-user type:

  - Customer—View device groups associated with your customer account IDs.
  - Partner—View device groups associated with all customer account IDs that you are authorized to access.

- **IP Address**—IP addresses of the devices to be onboarded. You can provide a single IP address or a list of IP addresses. Alternatively, you can upload the IP addresses through a CSV file.
- **Collector Name**—Automatically populated if you have only a single LWC. If you have multiple LWCs, select from the list of available LWCs.
- **Site ID**—Automatically populated if you have only a single Site ID. If you have multiple Site IDs, select from the list of available Site IDs.

4. In the **Credentials** section, create a set of new credentials or select from the existing device credentials.

   JSI supports SSH keys or usernames and passwords.

5. In the **Connections** section, define a connection mode. You can add a new connection or choose from the existing connections to connect the device to the LWC. You can connect the devices directly or through a set of bastion hosts.

   Bastion hosts utilize a SOCKS5 proxy server to reach target devices in the customer's network. Bastion hosts also support connection hopping, where an SSH session is first established with a customer's Linux-based device, which then initiates a subsequent SSH session to the target device.

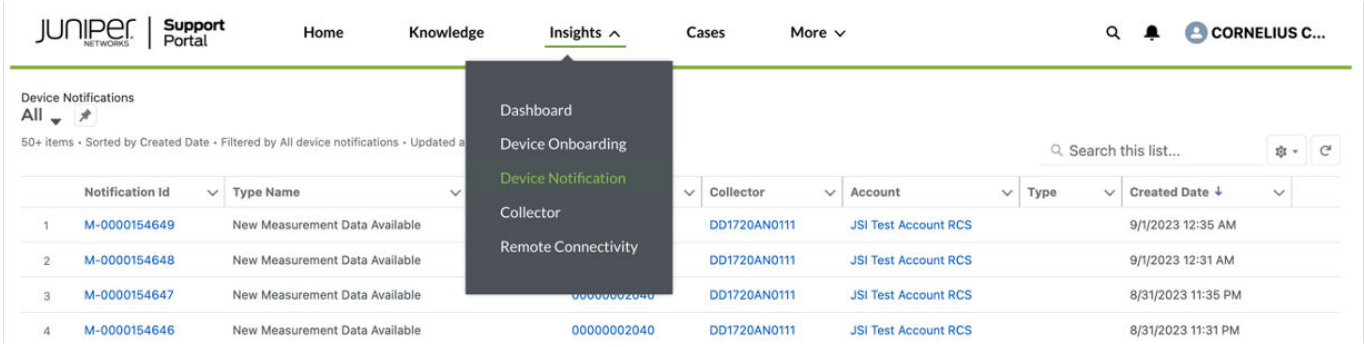
6. After entering the data, click **Submit** to initiate device data collection for the device group.

## View Notifications

Juniper Cloud notifies you about the device onboarding and data collection status. Notification could also contain information about errors that need to be addressed. You can receive notifications in your email, or view them on Juniper Support Portal.

Here's how to view notifications on Juniper Support Portal:

1. Click **Insights** > **Device Notifications**.
2. Click a **Notification ID** to view the content of the notification.




## View Operational Dashboards and Reports

The JSI operational dashboards and reports are dynamically updated based on a periodic (daily) device data collection, which is initiated when you onboard a device. The dashboards and reports provide a set of current, historic, and comparative data insights into the devices' health, inventory, and lifecycle management. The insights include the following:

- Software and hardware systems inventory (chassis to component level detail covering serialized and non-serialized items).
- Physical and logical interface inventory.
- Configuration change based on commits.
- Core files, alarms, and Routing Engine health.
- End of Life (EOS) and End of Service (EOS) exposure.

Juniper manages these operational dashboards and reports.

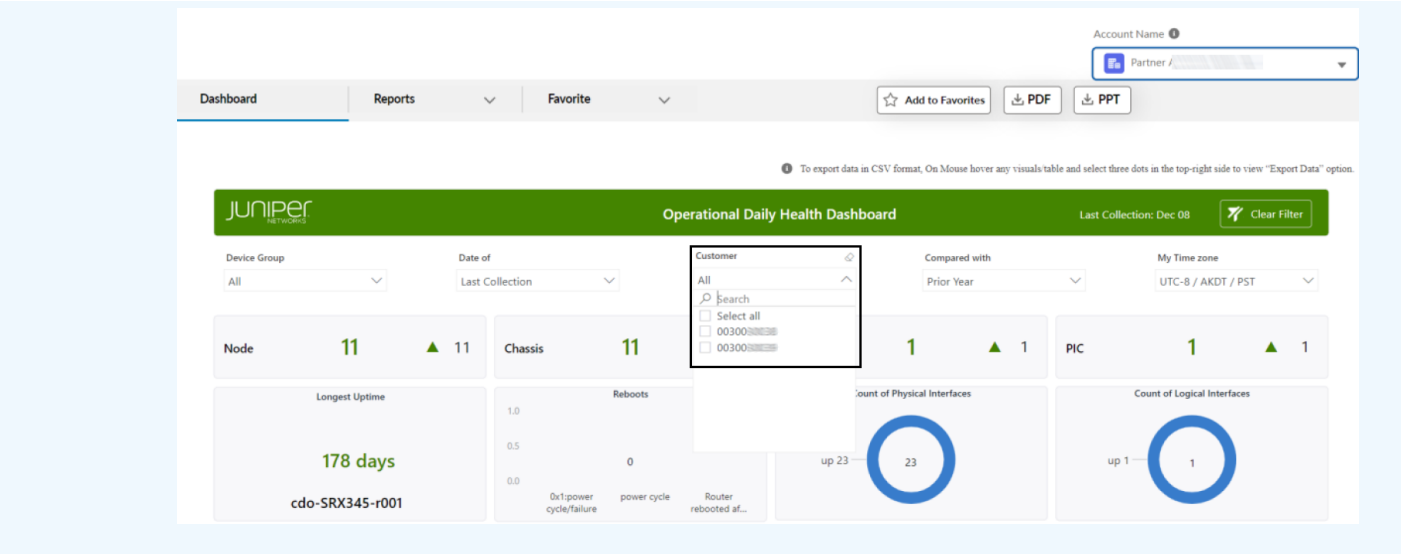
Here's how to view the dashboards and reports on Juniper Support Portal:

**NOTE**: Dashboards and reports are customized based on the end-user type:

- Customer—Displays data insights for the devices associated with the customer account.
- Partner—Displays a consolidated view with device insights from all supported customers.

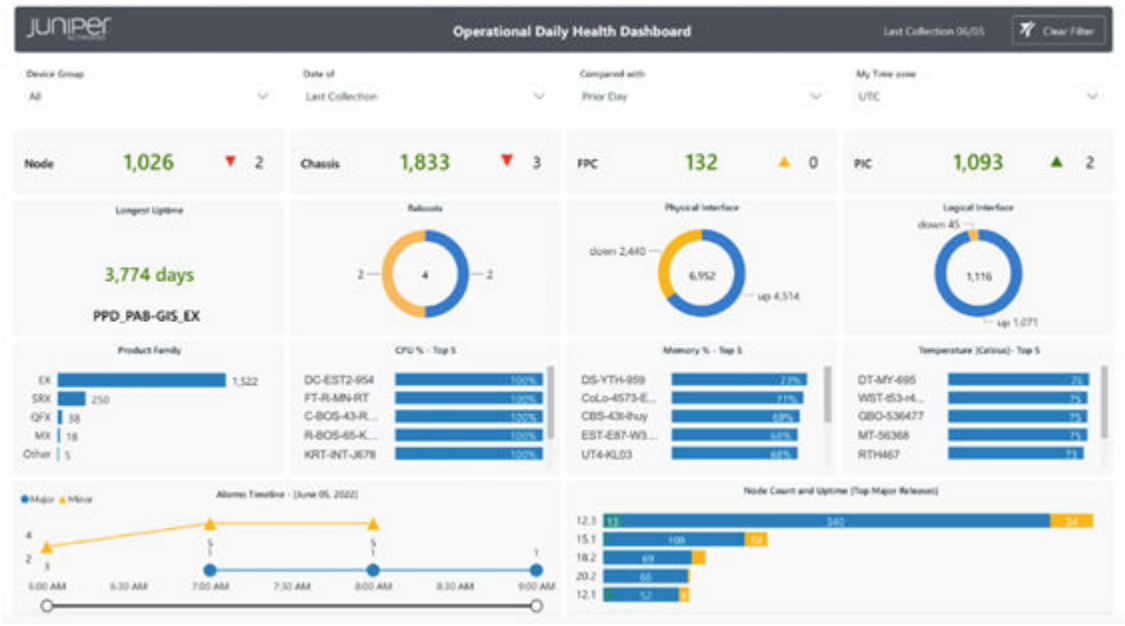
  You can filter the view to display insights specific to individual customers.

  To view insights specific to individual customers, select the customer ID from the Customer drop-down, as shown;

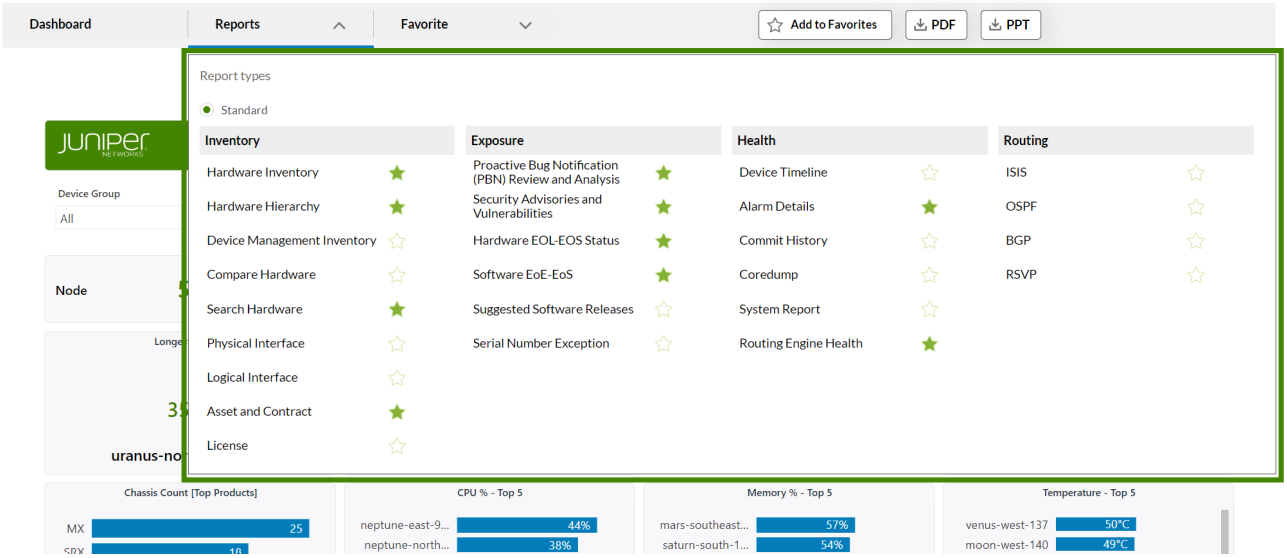



1. Click **Insights** > **Dashboard**.

   The **Operational Daily Health Dashboard** is displayed. This dashboard includes charts that summarize the KPIs associated with the account, based on the last collection date.




2. From the **Reports** menu on the left, select the dashboard or report you want to view.



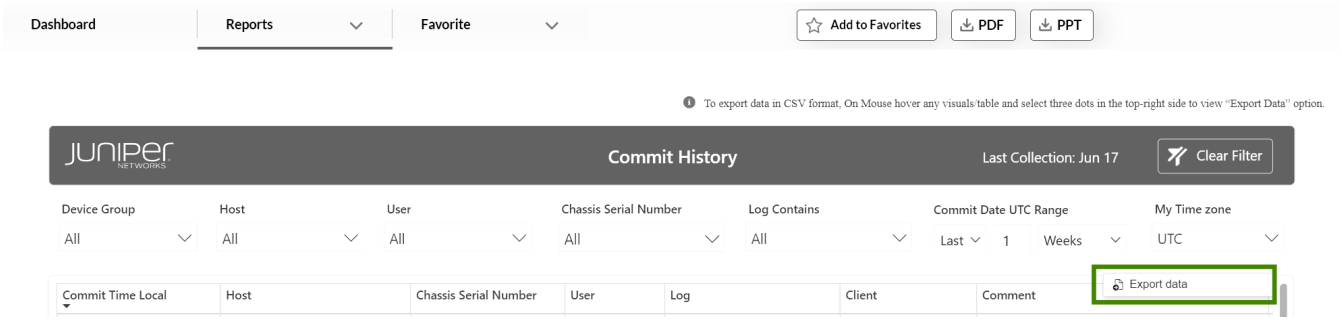

The reports typically consist of a set of filters, an aggregated summary view, and a detailed tabular view based on the data collected. A JSI report has the following features:

- Interactive views—Organize the data in a meaningful way. For example, you can create a segmented view of the data, click through, and mouse-over for additional details.
- Filters—Filter data based on your user type (customer or partner) and requirements.

> **NOTE**: Data filtering based on end-user type:
>
> - Customer—View and filter device groups associated with their customer account IDs.
> - Partner—View and filter device groups associated with all customer account IDs that they are authorized to access.

  You can filter data specific to one or more device groups for a specific collection date and a comparison period.

- Favorites—Tag reports as favorites for ease of access.
- PDF, PTT, and Data formats—Export the reports as PDF or PTT files, or in data format. In data format, you can download the report fields and values for each report component (for example, chart or table) by using the **Export Data** option as shown below:



# Prepare for a Remote Connectivity Suite Request

IN THIS SECTION



The JSI Remote Connectivity Suite (RCS) is a cloud-based solution that streamlines the support and troubleshooting process between Juniper support and customers by making the device data collection process seamless. Instead of iterative exchanges between Juniper support and the customer to obtain the right device data, RCS retrieves this in the background automatically. This timely access to essential device data facilitates swift troubleshooting of the issue.

**NOTE**: RCS is supported on devices connected directly or through Bastion Host via SOCKS5 proxy, but is not supported on devices connected through Bastion Host using connection hopping. Ensure your device connection method is compatible before initiating an RCS request.

At a high level, the RCS request process involves the following steps:

1. Submit a technical support case through the customer portal.
2. A Juniper support engineer will contact you about your technical support case. If necessary, the Juniper support engineer may propose an RCS request to retrieve device data.
3. Depending on the rules from the RCS settings (**Ask Approval** enabled), you may receive an email containing a link to authorize the RCS request.
   a. If you consent to share the device data, click the link in the email, and approve the request.
4. The RCS request will be scheduled for a specified time and the device data is securely relayed to Juniper support.

**NOTE**:

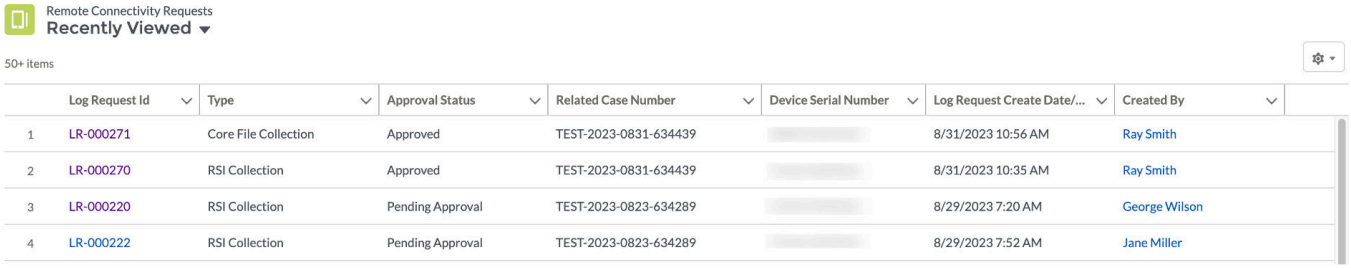
- You must have JSI administrator privileges to configure RCS device settings, and approve or deny RCS requests.
- RCS uses Secure Copy Protocol (SCP) for file transfer. SCP is enabled by default and does not require any configuration changes.

## View RCS Requests

Here's how to view RCS requests on Juniper Support Portal:

1. On Juniper Support Portal, click **Insights** > **Remote Connectivity** to open the Remote Connectivity Requests Lists page.

   The Remote Connectivity Requests Lists page lists all the RCS requests made. You can use the drop-down list on the top left corner of the page to customize your viewing preference.




| | Log Request Id | Type | Approval Status | Related Case Number | Device Serial Number | Log Request Create Date/... | Created By |
|---|---|---|---|---|---|---|---|
| 1 | LR-000271 | Core File Collection | Approved | TEST-2023-0831-634439 | | 8/31/2023 10:56 AM | Ray Smith |
| 2 | LR-000270 | RSI Collection | Approved | TEST-2023-0831-634439 | | 8/31/2023 10:35 AM | Ray Smith |
| 3 | LR-000220 | RSI Collection | Pending Approval | TEST-2023-0823-634289 | | 8/29/2023 7:20 AM | George Wilson |
| 4 | LR-000222 | RSI Collection | Pending Approval | TEST-2023-0823-634289 | | 8/29/2023 7:52 AM | Jane Miller |

2. Click the Log Request Id of an RCS request to open the Remote Connectivity Requests Detail page.

   From the Remote Connectivity Requests Detail page, you can view the RCS request details and perform the following tasks:

   - Modify the serial number.

     You modify the serial number if you provided RCS authorization for the wrong serial number during case creation. Click **Change Serial Number or SSRN** to enter the correct serial number of the device.

     **NOTE**:
     - You must enter the serial number of a JSI-connected device to avail the RCS feature.
     - The updated serial number must be of the same product family as the original device.

       If you want to authorize RCS for a different product family, create a separate case. JTAC has separate support teams for each product family. Opening a separate support case for the desired product family helps the support teams assist you with a quicker solution.

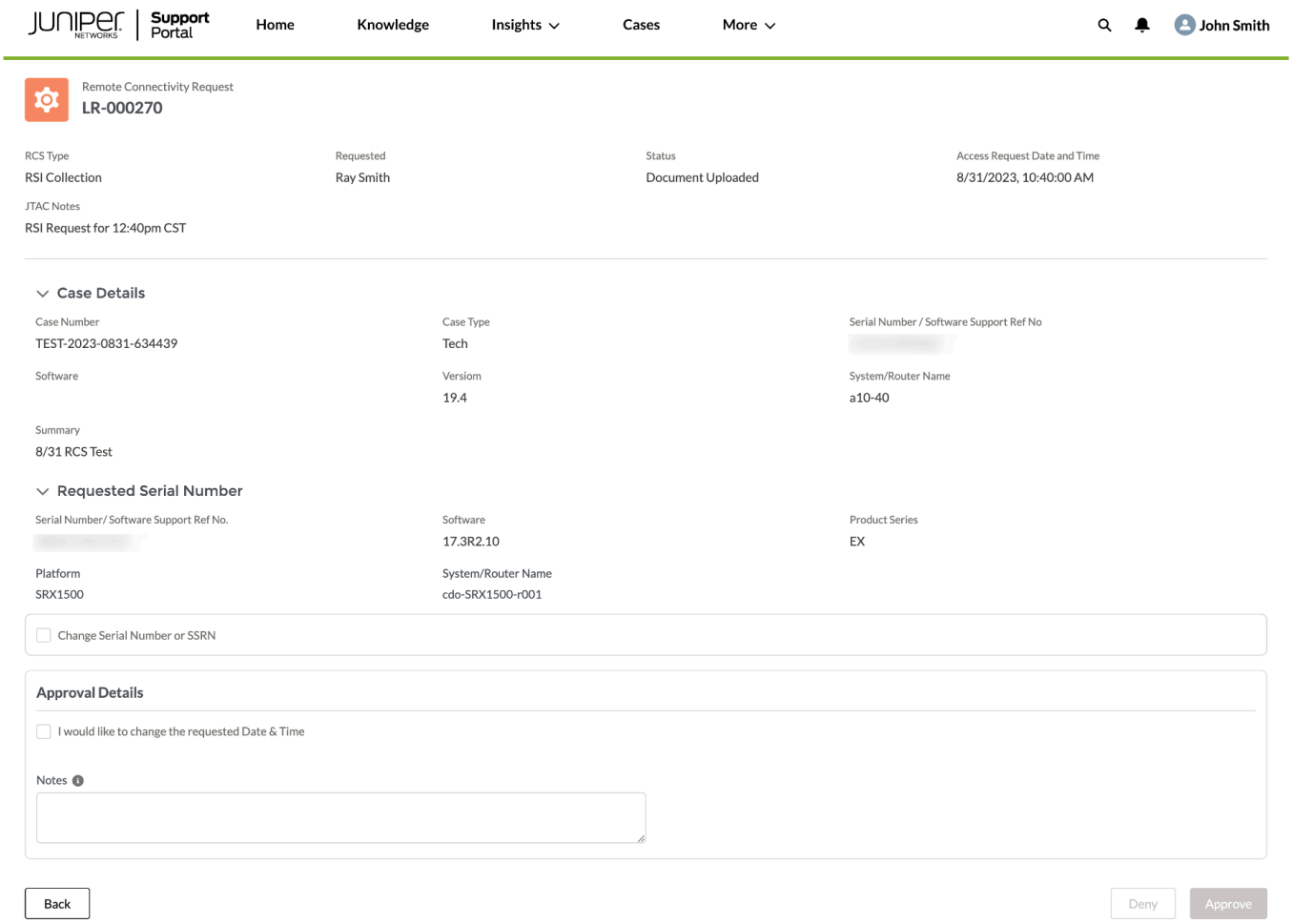
     The **Case Details** section displays the serial number of the device for which the case was opened, and the RCS request was initially authorized.

     The **Requested Serial Number** section displays the updated serial number of the device for which the RCS request is initiated.

   - Adjust the requested date and time (set to a future date/time).

     **NOTE**: If the time zone is not specified in your user profile, the default time zone is Pacific Time (PT).

   - Append notes.
   - Approve or deny the RCS request.

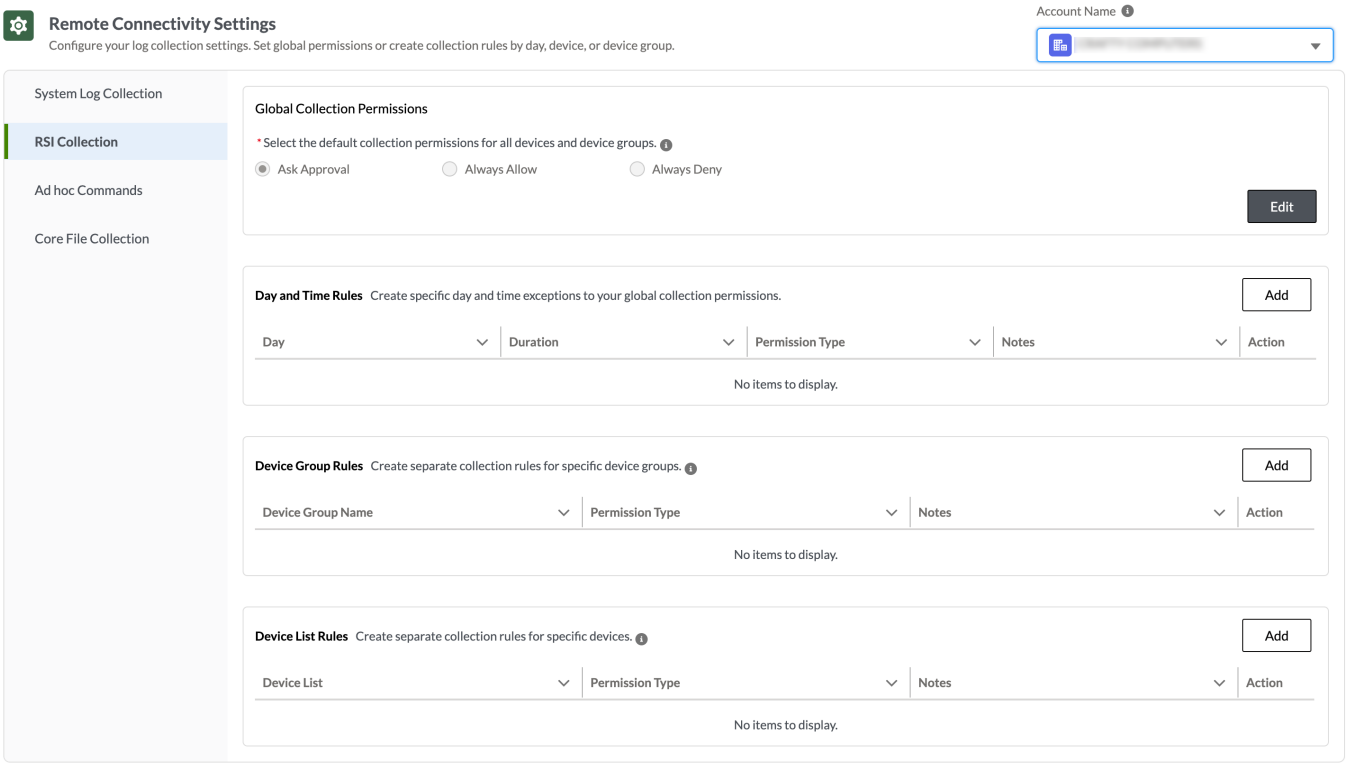



## Configure RCS Device Settings

You can configure both RCS collection and core file collection preferences from the RCS settings page.

Here's how to configure the Remote Connectivity RSI Collection settings on Juniper Support Portal:

1. On Juniper Support Portal, click **Insights** > **Remote Connectivity** to open the Remote Connectivity Requests Lists page.
2. Click **Settings** on the top right corner of the page. The Remote Connectivity RSI Collection Settings page opens. This page enables you to set global collection permissions and create permission exceptions based on different criterias.




3. Global collection permissions are configured at an account level. For multiple JSI-connected accounts, you can select the account using the Account Name drop-down list on the top right corner of the page.

4. To configure global collection permission, click **Edit** in the Global Collection Permissions section and change permission to one of the following:

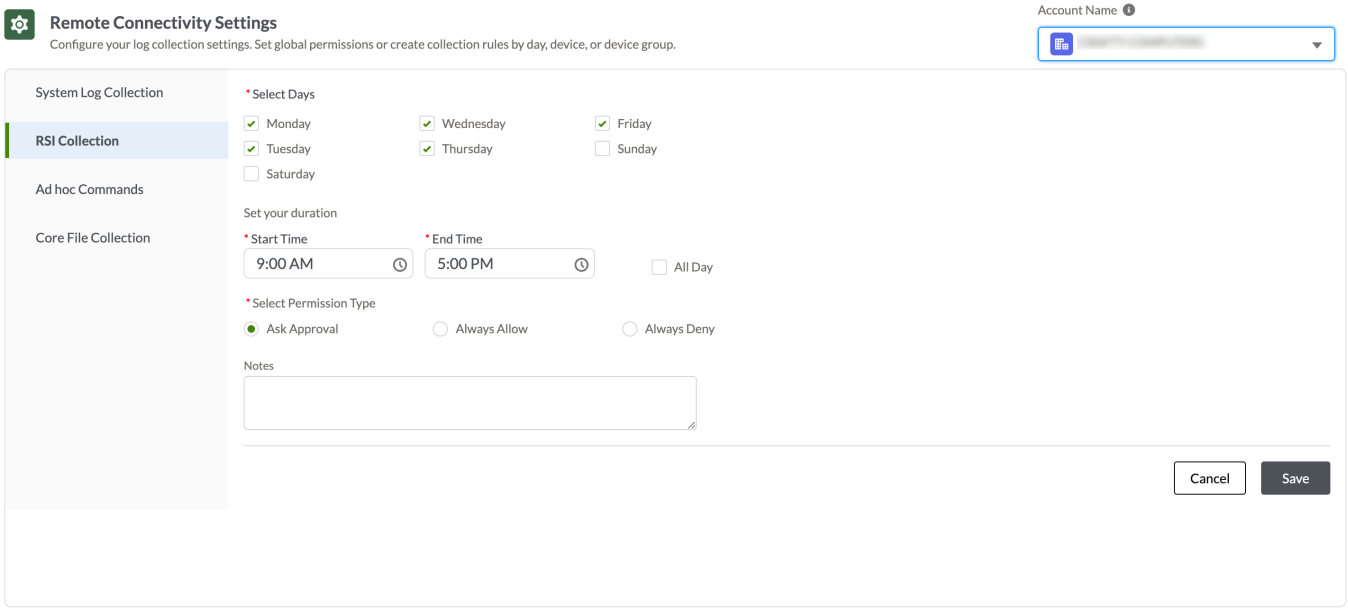
   - **Ask Approval**—An approval request is sent to the customer when Juniper support initiates an RCS request. This is the default setting when no permission is explicitly selected.
   - **Always Allow**—RCS requests initiated by Juniper support are automatically approved.
   - **Always Deny**—RCS requests initiated by Juniper support are automatically declined.

   **NOTE**: When you have the global collection permission, and one or more exceptions configured with conflicting permissions, the following order of precedence will apply:

   - Device list rules
   - Device group rules
   - Day and time rules
   - Global collection permission

5. To create exceptions based on specific day and time, click **Add** in the Date and Time Rules section. The Day and Time Rules Settings page opens.

You can configure an exception based on days and duration, and click **Save** to save the exception and return to the Remote Connectivity RSI Collection Settings page.

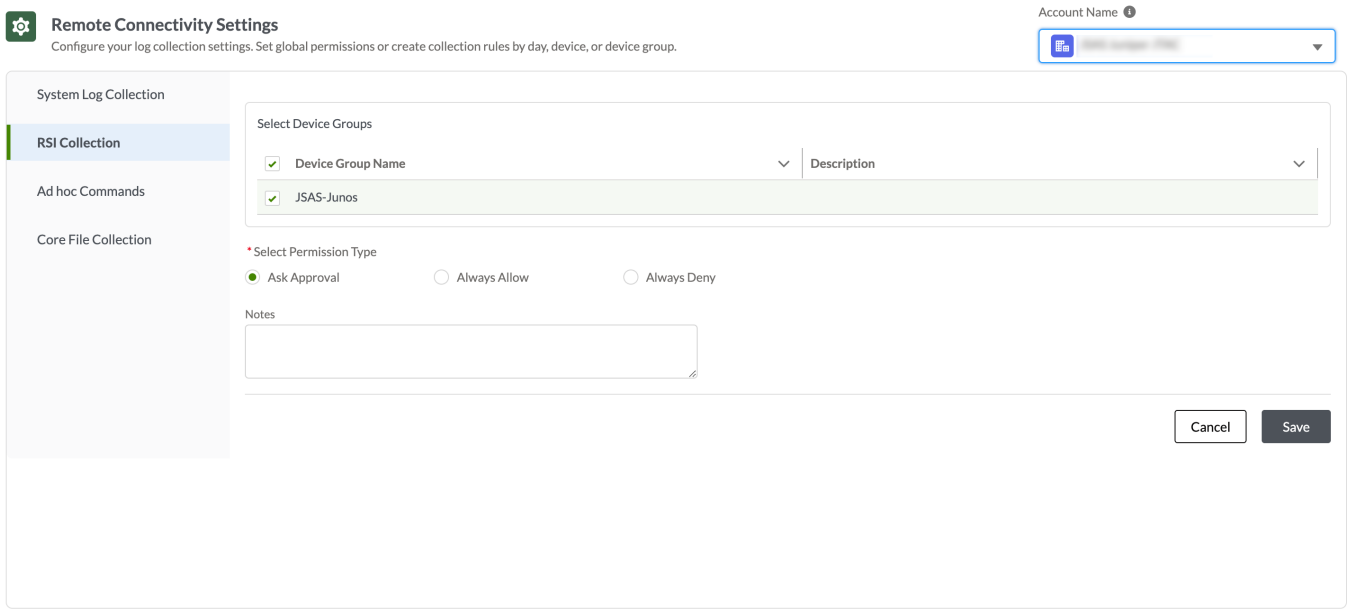



6.

**NOTE**: Before configuring collection rules for device groups, ensure that a device group already exists for the account.

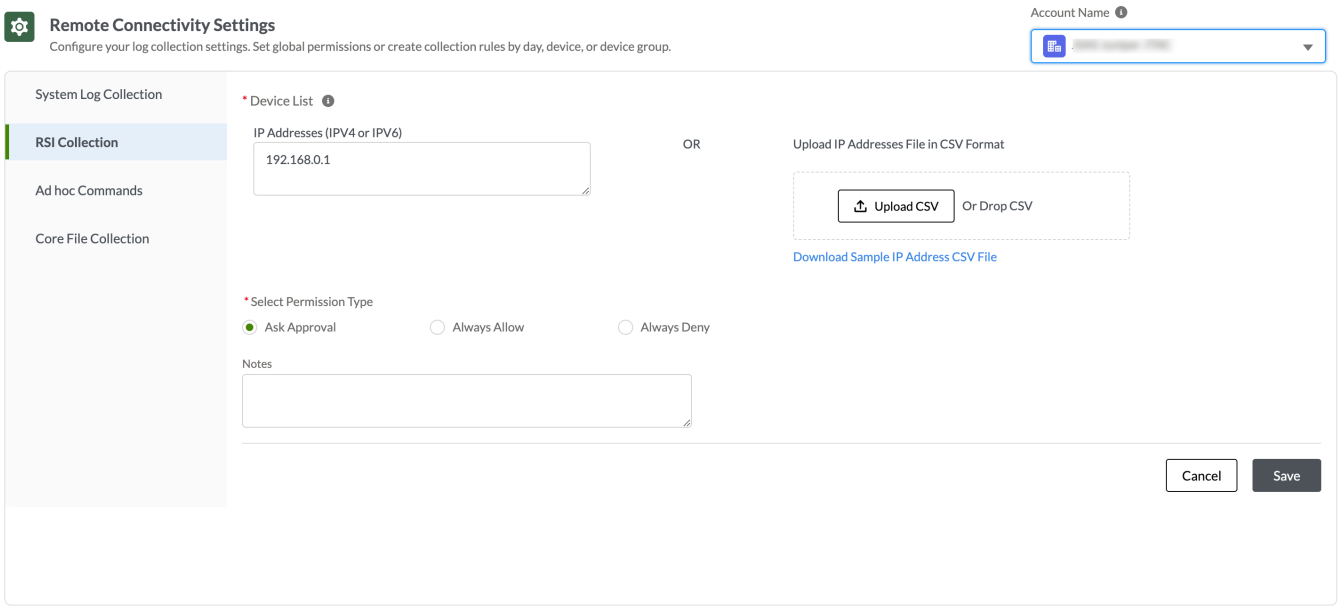
To create separate collection rules for specific device groups, click **Add** in the Device Group Rules section. The Device Group Rules Settings page opens.

You can configure the collection rule for a specific device group, and click **Save** to save the rule and return to the Remote Connectivity RSI Collection Settings page.



7. To create separate collection rules for individual devices, click **Add** in the Device List Rules section. The Device List Rules Settings page opens.

   You can configure the collection rule for individual devices, and click **Save** to save the rule and return to the Remote Connectivity RSI Collection Settings page.




# Step 3: Keep Going

**IN THIS SECTION**



Congratulations! Your JSI solution is now up and running. Here are some of the things you can do next.

## What's Next?

| If you want to | Then |
|---|---|
| Onboard additional devices or edit the existing onboarded devices. | Onboard additional devices by following the procedure explained here: "Onboard Devices" on page 15 |
| View the operational dashboards and reports. | See "View Operational Dashboards and Reports" on page 17 |
| Manage your notifications and email subscriptions. | Log into the Juniper Support Portal, navigate to **My Settings** and select **Insights** to manage your notifications and email subscriptions. |
| Get help with JSI. | Check for solutions in the FAQs: Juniper Support Insights and Knowledge Base (KB) articles.<br><br>If FAQ or KB articles do not address your issues, contact Juniper Customer Care. |

## General Information

| If you want to | Then |
|---|---|
| See all documentation available for Juniper Support Insights (JSI) | Visit the JSI Documentation page in the Juniper TechLibrary |
| Find more in-depth information about installing the Lightweight Collector (LWC) | See the LWC Platform Hardware Guide |

## Learn with Videos

Our video library continues to grow! We've created many, many videos that demonstrate how to do everything from install your hardware to configure advanced Junos OS network features. Here are some great video and training resources that will help you expand your knowledge of Junos OS.

| If you want to | Then |
| --- | --- |
| Get short and concise tips and instructions that provide quick answers, clarity, and insight into specific features and functions of Juniper technologies | See Learning with Juniper on the Juniper Networks main YouTube page |
| View a list of the many free technical trainings we offer at Juniper | Visit the Getting Started page on the Juniper Learning Portal |