Juniper Networks | Driven by Experience™

JUNIPER SUPPORT INSIGHTS SECURITY AND PRIVACY OVERVIEW

Protecting our customers' data is mission critical to Juniper. This document explores how security and privacy are central to Juniper Support Insights.

Table of Contents

Overview

Juniper Support Insights is a cloud solution hosted by Juniper on a private cloud that transforms the Juniper support experience into an intelligent and adaptive customer journey. It leverages operational state data, through the collection of Device Facts (defined below) from Juniper products running the Junos® operating system. This fully-managed solution provides operational dashboards, reports, and data insights that are timely, trusted, accessible, and readily usable. As a cloud-connected solution it is simple to use, secured, and dynamically scalable without overhead for the customer operations team to manage and maintain.

Juniper Support Insights reduces the cost and effort to efficiently operate networks by automating the data collection that powers existing Juniper support and service processes, such as Juniper Networks Technical Assistance Center support and renewals.

A key principle is that only data necessary for the support process and service experience is collected.

Data Security

Juniper Support Insights utilizes three types of information:

- Customer Account Information for setup and report access,
- Device Access Information to enable data collection, and
- Device Facts as input for dashboards and reports relevant to the operational management of deployed Juniper products.

In the interest of supporting data privacy, data security, and efficiency, the scope of data is minimized to the smallest set of data elements needed by Juniper Support Insights. This solution focuses on network device data rather than individuals' personal data. The only personal data processed by Juniper Support Insights is Customer Account Information as described in the following table.

Table 1: Information Processed by Juniper Support Insights

Information Category	Examples	Use Cases
Customer Account Information	Standard credentials for accessing Juniper Support, including Juniper assigned account and site IDs.	Access to the Juniper Support Insights Portal is integrated through the Juniper single sign-on.
Device Access Information	Device IP addresses for network devices and read-only credentials to access Junos network devices. Network device IP addresses and credentials to access any optional bastion (jump) hosts between the Juniper Support Insights collector and the network devices.	Required for allowing the collector to access network devices.
Device Facts	XML formatted output of standard Junos network device 'show' commands, such as "show chassis hardware detail" and "show system commit." Examples include but are not limited to the following: • Serial numbers • Part numbers • Host names • IP addresses • Junos software versions • Hardware versions • Installed memory • Installed flash • Boot versions • Product name and series • Line card types • SFP types • Firmware versions • MAC addresses • CPU utilization • Memory utilization • Alarms	Device Facts contained in the command output are used to create the Juniper Support Insights reports, based on daily periodic collection.

Data Collection Points

Juniper Support Insights has two distinct paths for data collection: the Portal and the Lightweight Collector (LWC). All information collected by the Portal is voluntarily provided by the user. User data provided may include passwords, SSH keys, or passphrases for network devices. By default, passwords, keys, and passphrases are masked in the Portal, and are always transmitted and stored in encrypted form. This data is stored only in Juniper's Enterprise Data Platform (EDP). No copies are stored in the Portal or LWC. Only the customer's Admin User(s) or Juniper account administrator can view this information in unencrypted form.

The LWC is installed on the customer's premises to provide additional security. Device Access Information entered through the Portal is used to connect to network devices and collect device data. Data resides on the LWC transiently and in volatile memory only. No customer data persists in the LWC across a reboot or power cycle, which reduces the scope of information being stored even on the customer's own premises.

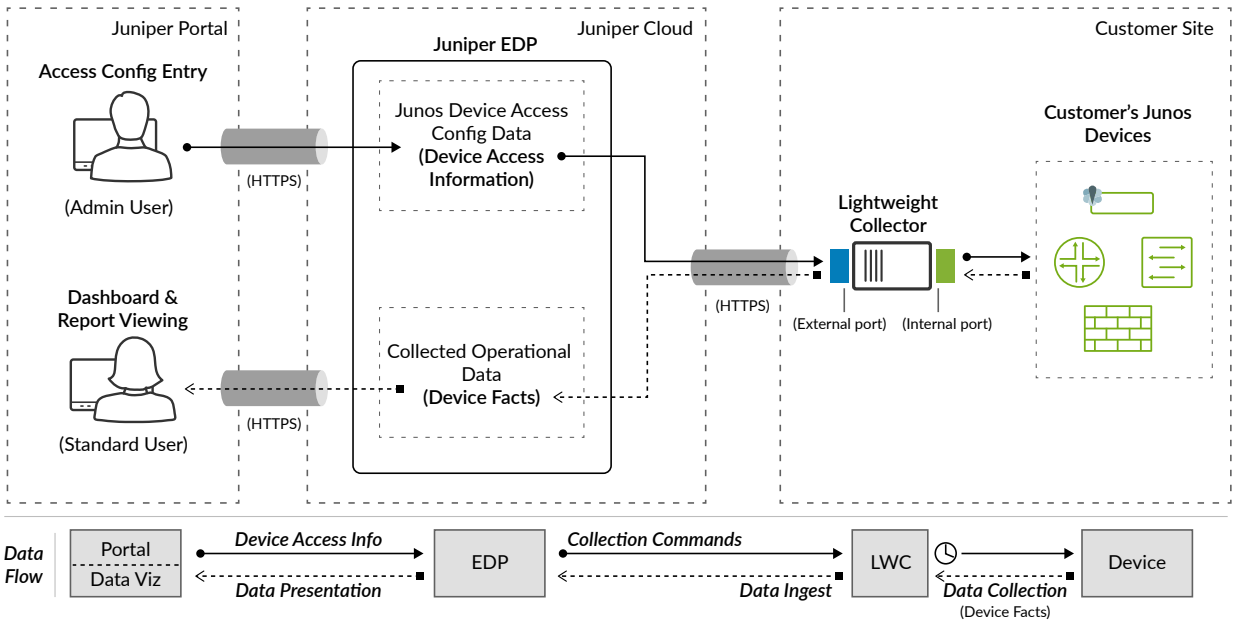

Figure 1: Data Collection

Security Highlights

- All data is encrypted in transit by a TLS connection using MQTT, HTTPS, and WebSocket protocols.
- Juniper EDP is secured within a Virtual Private Cloud.
- Further enablement is achieved by a private link between the EDP and Juniper cloud instance to create a network secured from unauthorized external access.

EDP Access Controls and Restrictions

Access to the Juniper EDP, which stores data collected by Juniper Support Insights, is managed and limited by Juniper's Information Technology organization.

End User Access Controls

End User access control to the Juniper Support Insights Portal is managed using standard Juniper Support accounts and credentials. A user is not required to create an additional access account with Juniper to access Juniper Support Insights. The controls placed on access for Juniper Support Insights directly correspond with the existing controls over how a user views and manages Juniper Support access.

End Users must be registered Juniper Support Users with a user login account. Details of the Juniper standard user registration process and instructions can be found in KB9946: Create New User Account for the Juniper Support Site.

Roles are selected as part of the initial onboarding process and can be updated via service request through the assigned Admin User.

Table 2: Roles and Permissions

Role	Access
Standard User	Standard Users have the ability to access the Juniper Support Insights Portal and view infor-mation such as network device onboarding details. Standard users cannot view keys or passwords for network device access.
Admin User	In addition to Standard User access, Admin Users have the ability to add, update, and delete, network device onboarding data. Only Admin Users have permission to view network device passwords and keys.
Power User (Dashboards and Reports)	In addition to Standard User access, Power Users have the ability to create, update, and de-lete custom dashboards and reports.

Juniper Support Insights LWC and Platform Access Controls

Access is restricted on the Juniper Support Insights LWC and platform. There is no user-accessible interface to the LWC. All user interaction is through the Portal.

The LWC is delivered on Juniper's platform in a limited capacity. Juniper Support Insights is a managed service and does not permit nor need Command Line Interface (CLI) or management access to the platform.

- Juniper limits access to the platform to help prevent vulnerabilities. No management interface is configured.
- Users do not have access to the Junos CLI.
- Only two ports are connected to the platform.
  - The Internal Port is connected to the customer's network devices (represented by the green box in Figure 1).
  - The External Port is connected to the Juniper cloud (represented by the blue box in Figure 1) and does not listen for or accept any inbound connections.
- The LWC initiates connections to the Juniper Cloud through the External Port. No other external connections are allowed.
- The LWC connects to the customer's Junos devices through the Internal Port. Any Junos devices reachable from this port can be configured for Device Facts collection.
- For security of the customer internal network, the LWC prohibits network traffic between the Internal and External Ports. The Internal and External Ports must be configured on separate subnets.

There is no direct access to the customer's on-premises LWC through the Juniper Support Insights Portal for any user, including the Juniper development and support teams. All communication between the on-premises LWC and Juniper Support Insights Portal must be through the Juniper cloud.

Data Privacy

Juniper is committed to helping our customers address global privacy compliance requirements, including, for example and as may be applicable, requirements from the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), by providing information that customers may need regarding the data processing conducted by Juniper Support Insights and by implementing security features within Juniper Support Insights.

As part of our commitment to help customers address their global privacy compliance requirements, Juniper provides information in this document for reference by customers, who are encouraged to consult with their own data protection and privacy compliance counsel regarding any particular laws or regulations that may apply to them and to develop a compliance program that best aligns with their business needs.

Please visit our Privacy Policy for additional information regarding Juniper's data privacy program. Our Customer Data Protection and Privacy Exhibit for Juniper Products and Services (DPA) is our data processing agreement for customers and is available on our website. The Juniper DPA incorporates the European Commission's Standard Contractual Clauses and other provisions applicable to Juniper. The DPA provides customers with greater clarity as to how Juniper will process and store any personal data.

In alignment with the principles and requirements of many data protection laws globally, Juniper Support Insights minimizes the personal data it collects to only Customer Account Information to enable customer users to log into the solution, where such Customer Account Information is sourced from customers' existing Juniper Support services accounts. Further, the Device Facts processed by Juniper Support Insights include only data about network devices, which is collected to generate and provide to customers a set of operation dashboards and reports and to aid the Juniper-customer support and services processes. Devices Facts do not include any information about user devices.

EDP data is currently hosted in a virtual private cloud located in the United States.

Data Retention

Juniper retains data collected in connection with Juniper Support Insights in accordance with the Customer Data Protection and Privacy Exhibit for Juniper Products and Services. Device Facts data are retained for 36 months. Juniper will not retain Device Access Information after an agreement or other ordering document for Juniper Support Insights expires or is terminated.

Information Security Incident Management

Juniper has established both an Incident Response Plan as a formal incident management process and three incident response teams to address cybersecurity incidents: Juniper IT CIRT, Juniper SIRT, and the Crisis Management Team.

The Juniper IT Cybersecurity Incident Response Team (Juniper IT-CIRT) is responsible for detecting cyber security threats, responding to attacks, and mitigating security incidents in order to manage risk, and protect confidential information in support of Juniper's mission and values.

The Juniper Networks Security Incident Response Team (Juniper SIRT) responds to security vulnerabilities regarding a Juniper product.

The Crisis Management Team is a cross-functional team that responds to any sudden and unpredictable event that requires investigation and has the potential to negatively impact Juniper's employees and external stakeholders.

As part of the incident management process, Juniper identifies issues and conducts root cause analysis. Lessons learned are documented to avoid the same issue from occurring again. Based on the criticality of the incident, Juniper has an escalation management process whereby key stakeholders are notified and engaged.

The Crisis Management Team reviews security incidents and determines whether and how to notify external stakeholders regarding such incidents, in coordination with Juniper Executive Leadership and Corporate Communications, when appropriate. During an active security incident, SIRT may communicate with external entities as prescribed by Juniper's internal policies and legal and contractual requirements.

Related Documentation

- Customer Data Protection and Privacy Exhibit for Juniper Products and Services
- Juniper Privacy Policy

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700

Juniper Networks | Driven by Experience™

9040194-001-EN Oct 2021