JUNIPER NETWORKS | Engineering Simplicity

Juniper Identity Management Service User Guide

Published
2025-04-25

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

Juniper Identity Management Service User Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide | v

About This Guide | vi

1 JIMS Overview

Overview | 2

Benefits of JIMS | 2

2 How JIMS works

JIMS Architecture, Workflow and Functionalities | 4

JIMS Workflow | 4

JIMS Architecture | 6

3 How to Install JIMS

JIMS Specifications and Installation | 10

Specifications | 10

Install JIMS | 11

4 JIMS Administrative User Interface

JIMS Administrative User Interface and Configuration | 14

JIMS User Interface Menu | 14

5 Configurations of JIMS Use Cases

Prerequisites – Security Hardening | 24

Set up JIMS – Identity Aware Network | 24

Configure Limited-Permission User Accounts | 25

Add Limited Permission User Accounts to Active Directory Groups | 25

Define Group Policies for Limited Permission User Accounts | 25

Customer Managed Devices (On-Premises) Deployment | 26

JIMS Server | 26

Directory Services | 27

Identity Producers | 27

Add Event Source | 28

Add PC Probe | 28

Add Syslog Source | 28

Filters | 29

Settings | 30

Logging | 30

General | 31

Enforcement Points | 31

Add Enforcement Points in JIMS UI | 31

Configure JIMS in Junos | 32

Juniper Secure Edge Deployments | 36

Configuration of Juniper Secure Edge Deployments | 36

Add Directory Services | 37

About This Guide

Juniper® Identity Management Service (JIMS) is a standalone Windows service application that collects and maintains a large database of user, device, and group information from Active Directory domains or syslog sources, enabling SRX Series Service Gateways (including the vSRX Virtual Firewall) to rapidly identify thousands of users in a large, distributed enterprise. SRX Series Service Gateways can create, manage, and refine firewall rules that are based on user identity rather than IP address, query Juniper Identity Management Service, obtain the proper user identity information, and then enforce the appropriate security policy decisions to permit or deny access to protected corporate resources and the Internet.

Use this guide to prepare, install, and configure the Juniper Identity Management Service (JIMS) for use in your network.

About This Guide

Juniper® Identity Management Service (JIMS) is a standalone Windows service application that collects and maintains a large database of user, device, and group information from Active Directory domains or syslog sources, enabling SRX Series Service Gateways (including the vSRX Virtual Firewall) to rapidly identify thousands of users in a large, distributed enterprise. SRX Series Service Gateways can create, manage, and refine firewall rules that are based on user identity rather than IP address, query Juniper Identity Management Service, obtain the proper user identity information, and then enforce the appropriate security policy decisions to permit or deny access to protected corporate resources and the Internet.

Use this guide to prepare, install, and configure the Juniper Identity Management Service (JIMS) for use in your network.

1
CHAPTER

JIMS Overview

IN THIS CHAPTER

- Overview | 2

Overview

SUMMARY

Read this section to know about Juniper® Identity Management Service (JIMS) and its benefits.

IN THIS SECTION

- Benefits of JIMS | 2

Juniper® Identity Management Service (JIMS) is a standalone Microsoft Windows service application that enables you to define identity-aware firewall policies instead of classic IP-based firewall policies.

JIMS ensures that the users and devices can access the required resources when they move between different IP networks without the need to statically map a MAC address on a device to one or more IP addresses. JIMS uses automated updates to enable the access to resources. JIMS allows SRX firewall to automatically map ip-addresses to user or devices based on group membership, this reduces the workload on administrators and improves the end-user experience.

Benefits of JIMS

Juniper Identity Management Service (JIMS) constantly monitors Microsoft Active Directory activity to track changes related to users, devices, and groups and automatically maps these together.

1. End-user experience—JIMS simplifies the daily end-user experience using automated correlation between end-users [username] or devices and current ip-address assignment. This ensures easy and controlled access to resources independent of the location as there is no further need to map ip-addresses to users and their devices.
2. Reduces complexity and load—JIMS aggregates and reduces the load on your identity management system by serving as a middleware between identity management system and all your SRX Series Firewalls.
3. Reduced administrative tasks—JIMS allows administrators to control the access to firewall policies using group memberships instead of statistically defining policies based on ip-addresses or subnets. This also ensures that only authorized users and devices are granted access and restricted access is provided based on privileges. This cleans up the firewall policies without the need to continually remove old ip-address assignment to users or devices.

2

CHAPTER

How JIMS works

IN THIS CHAPTER

- JIMS Architecture, Workflow and Functionalities | 4

JIMS Architecture, Workflow and Functionalities

SUMMARY

Read this section to learn about the JIMS workflow, architecture, and functionalities.

IN THIS SECTION

- JIMS Workflow | 4
- JIMS Architecture | 6

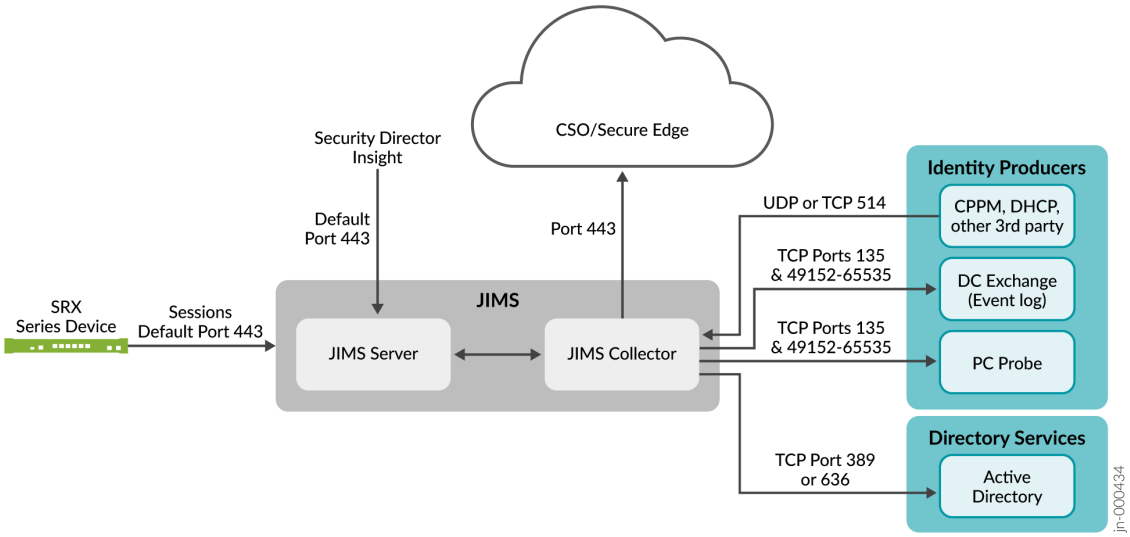
JIMS Workflow

Juniper Identity Management Service (JIMS) enables you to apply policies on the SRX Series Firewalls (including Juniper Networks® vSRX Virtual Firewall Virtual Firewall) based on user identity information such as usernames and user groups in addition to IP addresses. The service maps IP addresses to users and devices based on groups membership and provides this mapping information to the SRX Series Firewalls. (User groups for the SRX Series Firewalls are also known as user roles.) SRX Series Firewalls use the mapping information to generate entries for their authentication tables that you can use to enforce user/device-based security policy control based on group membership.

To support identity-aware firewall policies, JIMS performs these steps:

1. Communicates with Microsoft Active Directory to retrieve the username-to-group mapping information and uses this information to identify the group to which each user belongs.
2. Communicates with the Microsoft Domain Controllers or Microsoft Exchange Servers in the Active Directory domains to collect event log information, which contains the IP address-to-username mapping information. The service uses the mapping information to determine the IP addresses of users in Active Directory and Exchange Servers.
3. Stores IP address, username, and group-relationship information in its cache. The service then generates a report using the stored information and makes it available to the enforcement points (SRX Series Firewalls).
4. Generates authentication entries which are used to enforce device and user-based or group-based access control applied in the rule base for the SRX Series firewalls.

Figure 1: JIMS Architecture



The JIMS collector uses the Active Directory to monitor state changes of users, devices, and group memberships and collects this information. After each instance of data collection, the collector automatically sends this data to the JIMS server. This data is required to update the enforcement points.

The JIMS collector performs the following actions:

- It connects to:
  - Directory services (Microsoft Active Directory) using Lightweight Directory Access Protocol (LDAP) over (TCP port 389) or LDAP over Secure Sockets Layer (LDAPS) over (TCP port 636).
  - Identity providers (Microsoft Domain Controllers or Exchange Server) using Microsoft Remote Procedure Call (RPC) over (TCP port 135 and dynamic ports 49152 through 65535).

    NOTE: Microsoft Exchange Server is also known as Exchange Server.

  - Identity providers (ClearPass Policy Manager or CPPM, Dynamic Host Configuration Protocol or DHCP, and syslog server) using internal communication. The syslog server listens to TCP and UDP ports 514 for incoming syslog messages.
  - An identity provider (PC probe) using internal communication. PC probe sends outbound Windows Management Instrumentation (WMI) request to devices using TCP port 135 and dynamic ports 49152 through 65535.
- Sends data to JIMS servers using Transport Layer Security (TLS) over TCP port 443. (TCP ports are configurable.)

Enforcement points (SRX Series Firewalls) use TLS over TCP ports 443 and 591 (default port) to send queries to the JIMS server.

JIMS Architecture

IN THIS SECTION

- JIMS Service Types | 6
- JIMS Server | 6
- JIMS Collector | 6

JIMS Service Types

The JIMS consists of two services:

- Collector—Maps users and devices to IP addresses.
- Server—Serves the enforcement points with the mapping information.

Currently, these two services run on the same server as a single application.

JIMS Server

The JIMS server provides all your enforcement points (SRX Series firewalls) with high-scale identity data without consuming unnecessary CPU cycles on your directory services. The server provides the identity information in a JIMS report that includes user, device, IP address, and group mapping information. Each SRX Series Firewall uses this information to make policy decisions in the user firewall feature.

JIMS Collector

The JIMS collector communicates with your Active Directory to collect user, device, and group membership information. The collector also maps each active user and device to an IP address.

The collector can also connect to a syslog server and act on incoming data from a different system of interest, such as network access control (NAC), Dynamic Host Configuration Protocol (DHCP), VPN gateways, or a captive portal to record login and logout events .

Identity Data Collection

JIMS is scalable and can take over user identity data collection from Microsoft Active Directory, Domain Controllers, Microsoft Exchange Servers, and syslog servers. JIMS serves as a single centralized data collection source for the SRX Series Firewalls.

The service generates reports that contain the IP address, username, device, and group relationship information that the service collects from the user-identity data sources.

JIMS uses the following directory services and identity producers to collect identity data.

- **Directory Services—Data Collection from Microsoft Active Directory**

  JIMS communicates with each Active Directory to collect group information for users and devices. The service queries each configured Active Directory for user and device information. It queries the appropriate user information source each time it receives a login event for a user.

- **Identity Producers—Data Collection from Event Log Sources**

  JIMS connects to event log sources to collect user and device status events and provides IP address-to-username mapping information to the SRX Series Firewalls. For user login events, JIMS collects the domain name, username, and IP address. For device login events, JIMS collects the domain name, machine name, and IP address.

  Event log sources can be one or more Active Directory Domain Controllers or one or more Exchange Servers. JIMS gives you the option to configure event log sources that can be a combination of the Active Directory Domain Controllers and Exchange Servers.

- **Identity Producers—Data Collection from Syslog Sources**

  JIMS allows syslog clients to send event data such as user and device information from an event source such as a DHCP server. You have to define the IP address and port of the remote syslog client to which the JIMS server permits a connection. You must configure the JIMS server to collect syslog data whenever it detects a logout event, login event, or a change in data value. The JIMS collector extracts the device, username, and IP address information from the syslog messages and maps this information to group memberships. The collector then turns the mapping information into JIMS reports.

- **Identity Producers—Data Collection Using Domain PC Probing**

  PC Probe

  To initiate a domain PC probe of a device in a customer's domain, JIMS needs administrative credentials to access the device. For a PC probe to a new IP address, JIMS uses each set of configured credentials in the order in which they appear in the list.

  Domain PC probing acts as a supplement to event log reading. When a user is logged in to a domain, the event log contains all the information that JIMS requires. When IP address-to-username mapping

information is not available from the event log, JIMS initiates a domain PC probe to the device to get the username and domain of the current active user. You can use domain PC probes to also determine a device status after its logged-in state has expired. When using a PC probe, you should ensure that your firewall blocks outgoing PC probe requests to the Internet and potentially spoofed IP addresses by blocking outbound Windows Management Instrumentation (WMI) packets from your JIMS servers.

Enforcement Points

When a previous batch query fails to retrieve IP address-to-username mapping information, enforcement points (SRX Series firewalls) again send batch queries (reports) or IP queries to extract information about users, devices, and group membership from the JIMS server. When the JIMS server does not have the IP address about which an endpoint has queried, the server requests the JIMS collector for this data. The JIMS collector queries the Domain Controller and the Exchange Server for the corresponding record. When such a record does not exist, JIMS performs a PC probe to the IP address. You can run a PC probe only on Microsoft Windows.

3

CHAPTER

How to Install JIMS

IN THIS CHAPTER

- JIMS Specifications and Installation | **10**

JIMS Specifications and Installation

SUMMARY

Read this section to know about the system requirements and configurations to install JIMS. You can also learn how to install JIMS on the client machine.

IN THIS SECTION

- Specifications | **10**
- Install JIMS | **11**

Specifications

Table 1: JIMS Specifications

Component	OS and Kernel Versions
Supported Junos OS software releases	12.3X48-D45 or a later release
Supported Contrail Service Orchestration (CSO) release	Release 3.3 or a later release
Support for Juniper Secure Edge	Release 1.6.0
Maximum SRX Series Firewalls	Up to 1200
Maximum CSO platforms	10
Maximum event log sources	100
Maximum Active Directories	100
Maximum domains	25
Maximum user entries	500,000
Maximum syslog sources	200

Table 1: JIMS Specifications *(Continued)*

Component	OS and Kernel Versions
Supported platforms	Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 with Windows Server 2012 R2 Updates (KB2919355 and KB2999226)
Supported Identity Sources	Microsoft Active Directory on Windows Server 2012 R2 or later, Microsoft Exchange Server 2010 with Service Pack 3 (SP3)

Install JIMS

NOTE: You need administrative privileges to install JIMS.

1. Download the Juniper Identity Management Service installer from the Downloads page.
2. Unzip the installer and certificate without modifying the target directory.
3. Start the installation by running the installer.
4. Click **Yes** to allow InstallShield to install JIMS on your system. The Welcome to the InstallShield Wizard for the Juniper Identity Management Service page appears.

   If the installation requirements are not available in your system, a message alerts you that the installation requires a system reboot. Click **No** to continue with the installation and reboot your system after the installation has been completed.
5. Click **Next**.

   The License Agreement page appears.
6. Review the license agreement and select **I accept** to proceed.
7. Type the username and your organization name and click **Next**.
   The Ports page appears.
8. Type the JIMS server's HTTPS server port number that the enforcement points use to communicate with JIMS. The default value is 443.
9. Click **Next**.
   You see the Setup Type page, which gives you the option to select a complete or custom installation.
10. Select the **Complete setup** option and click **Next**.
    The Ready to Install the Program page appears.

11. Click **Install**. The JIMS application is installed by default in the location *C:\Program Files (x86)\Juniper Networks*.
12. Select the **Launch JIMS Administrator** check box and click **Finish**.
    The Juniper Identity Management Service application page appears. The installation is now complete.
13. In an earlier step if you had seen a message alerting you that a reboot is mandatory, then reboot your system now.

4

CHAPTER

JIMS Administrative User Interface

IN THIS CHAPTER

- JIMS Administrative User Interface and Configuration | **14**

JIMS Administrative User Interface and Configuration

SUMMARY

Read this section to know about the JIMS administrative interface and its configuration options.

IN THIS SECTION

- JIMS User Interface Menu | 14

JIMS User Interface Menu

IN THIS SECTION

- Monitor | 15
- JIMS Server | 17
- Directory services | 17
- Identity Producers | 18
- Enforcement Points | 18
- Filters | 20
- Settings | 21

JIMS user interface consists of three menu.

The below illustration captures the JIMS UI.

Figure 2: JIMS UI Screen

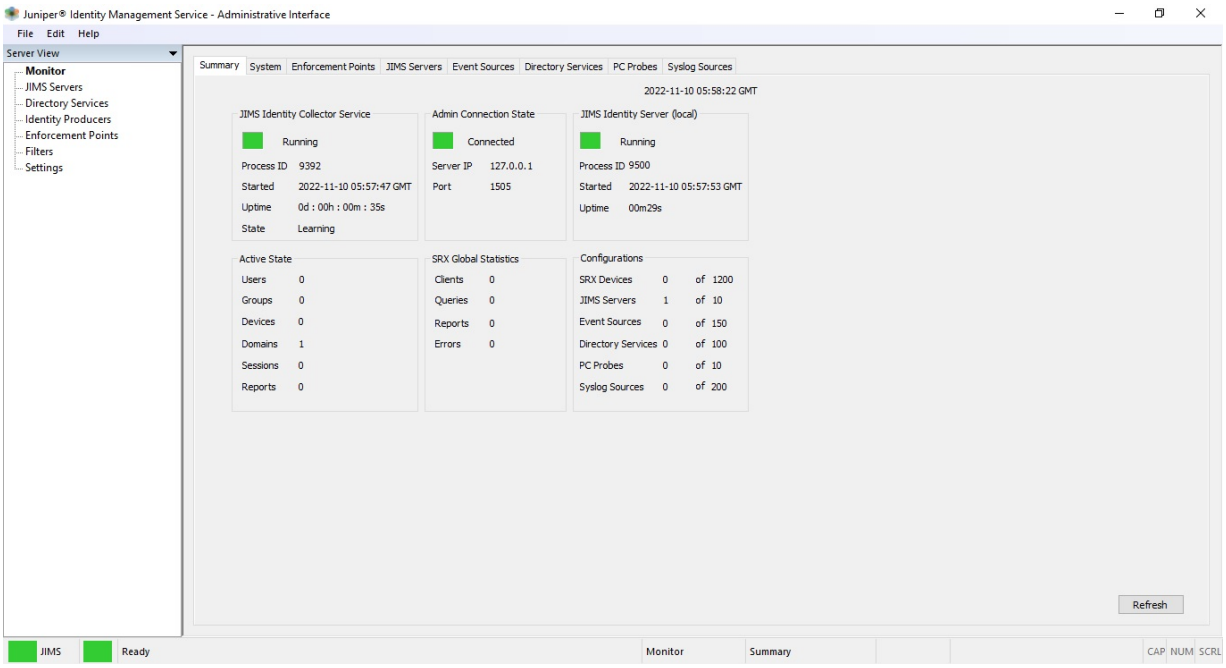


Table 2:

Menu	Description
File	Allows you to import and export the configuration data related to the JIMS. You can use the File menu to connect the JIMS collector to Juniper Secure Edge and reconnect to a lost connection of the UI.
Edit	Allows you to copy and search content from the user interface with table/list view.
Help	Allows you to find the documentation and information about JIMS such as Version, Build and other Copyright information like Trademark Notice, All Rights Reserved, Attributions and Terms of Licensing.

The other UI options are listed below.

Monitor

The Monitor menu offers several tabs with different information related to state, events and so on. The Date and Time on the top bar show date and time in GMT format.

The **Monitor** menu consists of 8 tabs:

Table 3:

Menu	Description
Summary	• **JIMS Collector Service** shows status, process-id, start time and uptime of the process. • **Admin Connection State** shows the current connect port and IP. The current release/version of JIMS allows you to run as admin only on the same server. • **Active State** shows the number of objects collected from the Active Directory for each type. • **SRX Global Statistics** shows the total number of connected enforcement points (clients), and the total number of queries requested from these enforcement points. It also shows the total number of reports that the JIMS server has provided to these enforcement points and the number of errors that occurred. • **Configurations** shows the number of configured objects versus maximum supported.
System	Lists all the systems configured.
Enforcement Points	Lists all configured Enforcement Points with device specific statistics. For a more detailed explanation and configuration steps, see "Enforcement Points" on page 18
JIMS Servers	Lists all configured JIMS Server with specific statistics. For a more detailed explanation and configuration steps, see "JIMS Server" on page 17

Table 3: *(Continued)*

Menu	Description
Event Sources	Lists all configured Event Sources with specific statistics. For a more detailed explanation and configuration steps, see "Directory services" on page 17
Directory Services	Lists all configured Directory Services with specific statistics. For a more detailed explanation and configuration steps, see "JIMS Server" on page 17
PC Probes	Lists all configured username and the order of execution including probe statistics. For a more detailed explanation and configuration steps, see "Identity Producers" on page 18
Syslog Sources	Lists all configured Syslog clients sending data to JIMS with specific statistics. For a more detailed explanation and configuration steps, see "Identity Producers" on page 18

JIMS Server

When JIMS is installed, it automatically configures the local JIMS server. If you use Contrail® Service Orchestration (CSO) or Juniper® Secure Edge these need to be configured manually.

For the configuration steps, see "JIMS Server" on page 26

Directory services

You must configure at least one directory server for JIMS Collector to collect users, devices, and group memberships. Currently, only Active Directory is supported.

If you plan to use multiple directory server with the same credentials, you can create a template to reduce the input for each directory server.

For the configuration steps, see "Directory Services" on page 27

Identity Producers

You can configure Identity Producers to gather user and device status events. JIMS uses this information to provide IP address-to-username mappings. JIMS also provides device names with domain names to the enforcement points (SRX Series Firewalls).

The identity producers offers many tabs that are listed below.

Event Sources are used to collect the username and associated IP-address. This creates an IP_address-to-username mapping as well as a device name with a domain name from a Microsoft Domain Controller or Microsoft Exchange Server. You can navigate to event sources from **Server View** > **Identity Producers**

If you plan to use multiple Event Sources with the same credentials, you can create a template to reduce the input for each event source server.

For the configuration steps, see "Add Event Source" on page 28

PC Probes are a complement to event sources and Syslog events for all the Windows devices connected in the domain. When the event source that is missing a domain and username is associated with an IP address, the pc probe initiates a WMI call to the specific device to collect the missing information. The WMI information contains sensitive data. Ensure that the JIMS Collector does not send WMI probes to untrusted networks. You can navigate to pc probes from **Server View** > **Identity Providers**

For the configuration steps, see "Add PC Probe" on page 28

Syslog Sources are used to collect user and device mapping from an IP from other systems such as a VPN concentrator, network access control (NAC) system, a wireless access controller and so on. You can navigate to syslog sources from **Server View** > **Identity Producers**

Syslog is used as a regular expression (regex), instead of a template offered by other functions. Syslog uses a base configuration that is specific to each syslog client type. You can use an already created base configuration for Juniper® Secure Connect to log the users that are active at logon and logoff events.

NOTE: When configuring a Regex expression, make sure the result will not contain any of the following characters: /\ [ ] : ; | = , + * ? < > @ "

For the configuration steps, see "Add Syslog Source" on page 28

Enforcement Points

You must configure enforcement points. Otherwise, the SRX Series Firewalls cannot pull user, device, and group information to enforce identity aware policies (user firewall).

If you have many SRX Series Firewalls with the same client id and client secret, you can create a template to reduce the input for each SRX Series Firewall.

For the configuration steps, see "Add Enforcement Points in JIMS UI" on page 31

JIMS with SRX Series Firewall

Juniper Identity Management Service (JIMS) is a Windows service application designed to collect and manage user, device, and group information from Active Directory domains.

For using the Juniper Identity Management Service, your enforcement points (SRX Series Firewalls and NFXs) are required to be configured properly to get identity information from JIMS.

The enforcement points use the primary JIMS server until the connection declares the server as lost. Periodically, the enforcement point probes the failed primary server and reverts to it once it becomes available again without any user intervention.

The connection to the JIMS server should only use HTTPS transport, which encrypts the communication between the enforcement point and the JIMS server. Both the enforcement points and JIMS server authenticate the connection using a client ID and client secret, which generates an access token. This access token must be present in each query to the JIMS server.

There are two methods for obtaining user identity information from JIMS:

- **Batch queries:**

  SRX sends a batch query message to JIMS every 5 seconds by default to obtain available identity information.

- **IP queries:**

  When SRX is missing information about a specific IP-address, it can send an ip-query to JIMS which then returns its status for that specific ip-address. If JIMS does not contain an entry for the specified IP address, SRX will threat this IP as it is an unknown-user.

In the SRX, it's possible to define filters which can be used to filter out identity information known to JIMS. You can either subscribe to certain domains and or include or exclude information related to certain ip-prefixes defined by address-book entries or address-sets. Changes to these filters will only take place during the next batch query.

You can select up to xxx address-book/sets entries for include or exclude filters, and the total number of xxx address-book entries is combined by both sets and books.

You can add a maximum of 25 domains to the filter list. Each address-set can include x number of address book entries, if address-sets are included in an address-set, `set services user-identification identity-management filter`

You can refresh the user identity information in your identity management authentication table obtained from JIMS. Identity information will be update during the next batch query, `clear services user-identification authentication-table authentication-source identity-management`

To search user identity information and validate the authentication source to grant access to the device, use `run show services user-identification authentication-table authentication-source all`

The following configuration illustrates a basic JIMS server configuration on an SRX Series Firewall:

`root@srx1#` **show services user-identification identity-management**

```
authentication-entry-timeout 120;
invalid-authentication-entry-timeout 10;
connection {
    connect-method https;
    port 443;
    primary {
        address 70.0.0.250;
        client-id abcd;
        client-secret "$9$86jLdsaJDkmTUj"; ## SECRET-DATA
    }
    secondary {
        address 70.0.0.251;
        client-id otest;
        client-secret "$9$W0K8-woaUH.5GD"; ## SECRET-DATA
    }
}
batch-query {
    items-per-batch 500;
    query-interval 5;
}
```

For detailed configuration steps, see "Configuration of JIMS with SRX Series Firewall" on page 32

Filters

JIMS enables you to specify the IP address ranges to include in or exclude from reports that the JIMS server sends to the SRX Series Firewalls. You can also specify Active Directory user groups to include in the reports. These filters are applied to all the SRX Series Firewalls in your network. You can also apply the IPv4 address filters in the later release versions.

JIMS supports both an IPv6 filter from the SRX Series Firewall query and a system-level IPv6 filter. The system-level filter works to filter the IP addresses from the event sources. The system-level IP filters are

configured through the JIMS Administrative Interface. JIMS server includes or excludes the IP sessions when the JIMS server receives the logon events from the configured event sources.

For example, let us consider that 192.x.x.x is added as the exclude IP address in the system-level filter on the JIMS server. When a user with 192.x.x.x logs on to the domain controller, JIMS server ignores the session for this user. Thus, no entry with 192.x.x.x is sent to the SRX Series Firewall.

The IPv6 filters used by the SRX Series Firewall query are configured on the SRX Series Firewall. The SRX Series Firewall includes or excludes the IP addresses in the batch query that it sends to the JIMS server. The JIMS server replies with the entries based on the filters received from the SRX Series Firewall. However, note that the SRX Series Firewalls only apply filters within the context of the system-level filter. For example, If 192.0.2.0/24 is configured on the SRX Series Firewall as the include filter, the SRX Series Firewall sends the query with 192.0.2.0/24 as the include subnet to JIMS sever. JIMS server replies with the entries within this subnet only, although the JIMS server holds lots of entries other than 192.0.2.0/24.

In addition, the JIMS server allows you to filter by:

- Groups—You define the Active Directory user groups to include in reports. Group filters are applied to all the SRX Series Firewalls in your network.
- User/Device Event—Event filters on the JIMS server enable you to apply a filter in your network to define users or devices to exclude from reports that the JIMS server sends to SRX Series Firewalls. The User/Device event filter performs regular expression matching to filter specific users or devices by name. The filter ignores events associated with a particular user or device.

For SRX Series Firewalls running Junos OS Release, JIMS applies the filters that it receives from individual SRX Series Firewalls. If you configure the filters for JIMS, the service first applies its own filters to all the SRX Series Firewalls in your network, and then applies the filters that it receives from the individual SRX Series Firewalls.

For detailed configuration steps, see " Add Filters" on page 29

Settings

The **Settings** menu consists of two tabs:

- General
- Logging

Settings on the server view allows you to change the configured values of ports used by JIMS. You can also change the digital certificate that is used for the JIMS local server. Navigate to **General** from **Server View** > **Settings**

For detailed configuration steps, see " Configure the General section" on page 30

The Logging menu item on the server view allows you to change the log levels. Change the log levels only if Juniper advises changing logs for troubleshooting. Navigate to **Logging** from **Server View** > **Settings**

For detailed configuration steps, see "Configure the Logging section" on page 31

5

CHAPTER

Configurations of JIMS Use Cases

IN THIS CHAPTER

- Prerequisites – Security Hardening | **24**
- Customer Managed Devices (On-Premises) Deployment | **26**
- Juniper Secure Edge Deployments | **36**

Prerequisites – Security Hardening

SUMMARY

This section explains how to restrict access for system accounts with JIMS.

IN THIS SECTION

- Set up JIMS – Identity Aware Network | **24**
- Configure Limited-Permission User Accounts | **25**
- Add Limited Permission User Accounts to Active Directory Groups | **25**
- Define Group Policies for Limited Permission User Accounts | **25**

Prepare Deployment

Define the servers on which you want to install JIMS. Create service accounts to enable JIMS to read from the defined directory services and identity producers. If you use PC probe, you must create a service account for it.

Set up JIMS – Identity Aware Network

Follow the below steps to set up JIMS to offer an identity aware network:

1. Define service accounts and enforcement point credentials.
2. Install JIMS.
3. Configure JIMS to connect to all your Active Directory services.
4. Configure JIMS to use the identity producers of your choice.
5. Configure the required integrations such as Juniper Secure Edge or Security Director Cloud and so on.
6. Enroll all your SRX Series Firewalls into JIMS.

Configure Limited-Permission User Accounts

Follow these steps for a new user account:

1. From the Start menu, select **Active Directory Users and Computers**.
2. Navigate to the Users container in the forest.
3. Right-click **Users** and select **New Users**.
4. Specify a descriptive first and middle name or any Windows 2000 username.
5. Specify a password according to your organization's password policy.
6. Clear the **User must change password at next login** check box.
7. Select the **User cannot change password** check box.
8. Select the **Password never expires** check box.

Add Limited Permission User Accounts to Active Directory Groups

To add each new user account to an Active Directory group:

1. Select the **Built-in** option.
2. Select the **Event Log Readers** group and add the **JIMS-EventLogRemoteAccess** account.
3. Select the **Distributed COM Users** group and add the **JIMS-PC-Probe** account.
4. Select the **Remote Management Users** group and add the **JIMS-PC-Probe** account.
5. Select the **Domain Admins** group and add the **JIMS-PC-Probe** account.

Define Group Policies for Limited Permission User Accounts

To define group policies for each new user account:

1. From the **Start** menu, select **Group Policy Management**.
2. On the **Group Policy Manager** tab/window, select the **forest** and **Default Domain Policy**. Right-click **Default Domain Policy** and select **Edit**.
3. Select **Computer Configuration**> **Policies**> **Windows Settings**> **Security Settings** >**Local Policies**> **User Rights Assignment**.
4. Select **Deny Logon locally**, select **Define these policy settings**, and add the new user account.
5. Select **Deny Logon through Remote Desktop Services**, select **Define these policy settings**., and add the new user account.

6. Select **Deny Logon through Terminal Services**, select **Define these policy settings**, and add the new user account.
7. Select **Deny logon as a batch job**, select **Define these policy settings**, and add the new user account.
8. Select **Deny Logon as a service**, select **Define these policy settings**, and add the new user account

.

Customer Managed Devices (On-Premises) Deployment

IN THIS SECTION

- JIMS Server | 26
- Directory Services | 27
- Identity Producers | 27
- Filters | 29
- Settings | 30
- Enforcement Points | 31

NOTE: “Configuration of Juniper Secure Edge Deployments” and “Add Directory Services” are mandatory for customers using both On-Premises and Secure Edge deployments.

JIMS Server

The JIMS Server is configured by default for localhost connection. Once it is configured, you can only edit the **JIMS Server port** and **Max Data Rate** for the server.

A new JIMS server can also be configured. To add a new JIMS Server, follow the below steps:

1. Click **Add** to add a new JIMS Server.

2. Enter the IP address or the fully qualified domain name (FQDN) of the server.
3. Give a description.
4. Enter the **Username** and **Password** for authentication purposes.
5. Select the **JIMS Server Type** from the drop-down menu.
6. Deselect TLS only if you perform troubleshooting.
7. The identity **JIMS Server Port** and **Max Data Rate** are automatically configured by JIMS. You can either change to a certificate signed by your organization or use the default certificate provided by JIMS.

Directory Services

You must configure at least one directory server for JIMS Collector to collect users, devices, and group memberships. Currently, only Active Directory is supported.

If you plan to use multiple Directory Server with the same credentials, you could create a template to reduce the input for each directory server.

To add a new Directory Server:

1. Click **Add** to add a new Directory Server.
2. Optionally use an already created template to pre-configure the credentials.
3. The source is selected by default.
4. Provide a **Description**.
5. Enter the **Server Hostname or IP Address** of the server.
6. Enter the **Login ID**) and **Password** for authentication purposes.
7. Select **TLS Connection** if you like to encrypt communication between JIMS and the Directory Server.

Identity Producers

IN THIS SECTION

- Add Event Source | **28**
- Add PC Probe | **28**
- Add Syslog Source | **28**

You can configure Identity Producers to gather user and device status events. JIMS uses this information to provide IP address-to-username mappings. JIMS also provides device names with domain names to the enforcement points (SRX Series Firewalls).

The identity producers have 3 tabs/options. Select the appropriate option for your deployment based on the information provided in the "Identity Producers" on page 18 section.

Add Event Source

To add a new event source:

1. Click **Add** to add a new Event Sources.
2. Use an existing template to pre-configure the credentials.
3. Select the type of source from the drop-down menu:
   - Domain Controller
   - Exchange Server
   - Windows Event Collector (WEC)
4. If you select **Windows Event Collector (WEC)**, enter the **Channel Path** from which logs should be collected.
5. Provide an optional description.
6. Enter the **Server Hostname** or **IP Address** of the server.
7. Enter the **Login ID** and **Password**. Use the dedicated service account created with limited privileges.
8. Enter **Startup Event History Catchup Time** to ensure JIMS collects historical event logs before the system begins active monitoring.

Add PC Probe

To add a new PC probe:

1. Click **Add** to add a new PC Probes.
2. Enter the **Login ID** and **Password**. This is the newly created service account with limited privileges.
3. Provide an optional description.
4. After you provide the details, you can move the order of usernames in the sequence you want them executed.

Add Syslog Source

To add a new syslog source:

1. Click **Add** to add a new Syslog Source.
2. Optionally, select a pre-existing **Base Configuration** to inherit predefined settings.

3. **Enter** the IP address or Fully Qualified Domain Name (FQDN) of the Syslog client (server sending the logs).
4. Provide an optional description.
5. Click **Add** to define your matching regular expressions.
6. Navigate to the **Regular Expression Sequences** section. On the right-hand side, you will see **Add**, **Edit**, and **Delete** buttons.
7. **Click Add** to define a new Regular Expression Sequence. A pop-up window titled **Add Regular Expression Builder** will appear.
8. In the pop-up window, fill in the following details:
   a. **Description**: A brief explanation of the sequence.
   b. **ID**: Auto-generated, starting with 1 by default.
   c. **Type**: Select the type of sequence from the drop-down menu:
      - **Begin Session**
      - **End Session**
   d. **Regular Attribute Categories**: Specify applicable attribute categories relevant to the pattern.
   e. **Trigger Match Expression**: Define the regex pattern that should trigger a match.
   f. **Return Count***(optional)*: Set the number of times this expression should return a match.
   g. **Starting Time (in minutes)***(optional)*: Specify the time window to begin evaluating matches.
   h. **Match Source IP**: Enable or disable the checkbox based on whether you want to match the source IP in your expression.
9. After completing the fields, click **Add** to save the sequence.
10. Click **OK** to populate the **Regular Expression Sequences** table with your newly defined sequence(s). Once configured, the Regular Expression Sequences will be associated with the selected Syslog Source and used for matching incoming log messages accordingly.

Filters

The JIMS server allows you to filter by:

- **IP Filters**—Allows you to **include or exclude** traffic from the specified IP ranges in reports. The Include IP filters will only include those IP ranges while sending updates to SRX, similarly Exclude IP filters will exclude the IP ranges from its update to SRX. Requires input for **IP Range Start** and **IP Range End**.

- **User/Device Filters**—Designed to **exclude specific users or devices** from reports. You can specify usernames or device identifiers to filter out unwanted data. Helps in refining the visibility of events by omitting irrelevant or known sources.
- **Group Filters**—Acts as **Include Filters**, applied to all **SRX Series Firewalls** across your network. For improved matching, a **Domain** can also be added alongside the group specification.
- **DN Filters**—Used to **exclude** entries based on **Distinguished Names (DN)**. Ideal for filtering out specific organizational units or user paths from directories.

> **NOTE**: Supports the use of regular expressions for more accurate and flexible matching for User/Device Filters, Group Filters and DN Filters.

Settings

IN THIS SECTION

- Logging | 30
- General | 31

The **Settings** menu consists of two tabs:

Logging

In the **Logging** section, enter the following details:

1. Enter the Filename Prefix.
2. Click on **Select** to choose the required **Directory**.
3. Enter the **File Size**.

> **NOTE**: The acceptable file size range is 1 to 2000 MB.

4. Enter the **File Lifetime**.

> **NOTE**: The acceptable file lifetime range is 1 to 30 days.

General

In the **General** section, enter the following details:

1. Under **Administrative Interface Configuration**, enter the **TLS (https) Port**.
2. Under **User session Configuration**, enter the **Logoff Time**.

   NOTE: The acceptable logoff time frame should fall within 1 to 1440 minutes.

3. Under the **Global Configuration** section (which requires a JIMS restart), enter the **Syslog Initial Timespan (minutes)**. Choose the appropriate options: **Pass UPN**, **Permit Compound Usernames** and **Trust Other Domains** based on your requirements.

Enforcement Points

IN THIS SECTION

- Add Enforcement Points in JIMS UI | 31
- Configure JIMS in Junos | 32

Add Enforcement Points in JIMS UI

You must configure the Enforcement Points (SRX/NFX devices), otherwise, it cannot pull user, device, and group information to enforce identity-aware policies (user Firewall).

If you have many Enforcement Points with the same client id and client secret, you can create a template to reduce the input for each of them.

To add a new Enforcement Point:

1. Click **Add**.
2. Optionally use an already created template to pre-configure the credentials.
3. Enter the **SRX IP Address**.
4. If you have several Enforcement Points within a subnet, you can enter a matching **Subnet** that covers all of them.
5. Provide an optional description.

6. Enable the IPv6 reporting as IPv6 as it is used in your organization. This adds duplicated records in the auth table on the Enforcement Point.
7. Enter the **Client ID** and **Client Secret** used for this device.
8. The **Token Lifetime** is enforced. This lifetime can be changed/adjusted.

Configure JIMS in Junos

IN THIS SECTION

- Configuration of JIMS with SRX Series Firewall | **32**
- Configuration of the Device Identity Authentication Source (End-User-Profile) | **34**
- Configuration of the Firewall Policy to Match the Source Identity. | **35**

Configuration of JIMS with SRX Series Firewall

Use the following steps to configure JIMS with SRX Series Firewall:

1. Configure the FQDN/IP address of the primary/secondary JIMS server.

```
[edit services user-identification]
user@host# set identity-management connection primary address [fqdn/ip-address]
user@host# set identity-management connection secondary address [fqdn/ip-address]
```

2. Configure the client ID and client secret that the SRX Series device provides to the JIMS primary/secondary server as part of its authentication.

```
[edit services user-identification]
user@host# set identity-management connection primary client-id [client-id]
user@host# set identity-management connection primary client-secret [client-secret]
user@host# set identity-management connection secondary client-id [client-id]
user@host# set identity-management connection secondary client-secret [client-secret]
```

3. Optionally, configure the source-ip or routing instance that should be used to reach JIMS servers.

```
[edit services user-identification]
user@host# set identity-management connection primary source [ip-address]
user@host# set identity-management connection primary routing-instance [routing-instance-name]
```

NOTE: You can also configure the enforcement point to validate the certificate of the JIMS server, to do so, see advanced section.

4. Configure the maximum number of user identity items that the device accepts in one batch in response to the query.

```
[edit services user-identification]
user@host# set identity-management batch-query items-per-batch [number-of-items-per-batch]
```

5. Configure the interval in seconds after which the device issues a query request for newly generated user identities.

```
[edit services user-identification]
user@host# set identity-management batch-query query-interval [query-interval]
```

6. Configure active directory domains of interest to the SRX Series Firewall. You can specify up to twenty domain names for the filter.

```
[edit services user-identification]
user@host# set identity-management filter domain [domain-name]
```

7. Configure the address book name to include the IP filter.

```
[edit services user-identification]
user@host# set identity-management filter include-ip address-book [address-book-name]
```

8. To configure the referenced address set, trace option file name, trace file size, level of debugging output, and the trace identity management for all modules, use the below commands appropriately:

```
[edit services user-identification]
user@host# set identity-management filter include-ip address-set [address-set]
user@host# set identity-management traceoptions file [file-name]
user@host# set identity-management traceoptions file [file-size]
user@host# set identity-management traceoptions level all
user@host# set identity-management traceoptions flag all
```

Configuration of the Device Identity Authentication Source (End-User-Profile)

Specify the device identity authentication source and the security policy. The device obtains the device identity information for authenticated devices from the authentication source. The device searches the device identity authentication table for a device match when traffic issuing from a user's device arrives at the device. If it finds a match, the device searches for a matching security policy. If it finds a matching security policy, the security policy's action is applied to the traffic.

Use the following steps to configure device identity authentication source:

1. Specify the device identity authentication source.

```
[edit services user-identification]
user@host# set device-information authentication-source network-access-controller
```

2. Configure the device identity profile and domain name to which the device belongs.

```
[edit services user-identification]
user@host# set device-information end-user-profile profile-name [profile-name] domain-name
[domain-name]
```

3. Configure the profile name attribute device identity string.

```
[edit services user-identification]
user@host# set device-information end-user-profile profile-name [profile-name] attribute
device-identity string [string-value]
```

Configuration of the Firewall Policy to Match the Source Identity.

Use the following steps to configure one or more firewall policies that control access based on identity.

1. Create a source or destination address for a security policy and configure the application/service to match the policy.

```
[edit security]
user@host# set policies from-zone untrust to-zone trust policy name match source-address any
user@host# set policies from-zone untrust to-zone trust policy name match destination-address
any
user@host# set policies from-zone untrust to-zone trust policy name match application any
```

2. Define a username or a role (group) name that the JIMS sends to the device. **For Example:** "jims-dom1.local\user1".

```
[edit security]
user@host# set policies from-zone untrust to-zone trust policy name match source-identity
username or group
```

3. Permit the packet if the policy matches.

```
[edit security]
user@host# set policies from-zone untrust to-zone trust policy name then permit
```

4. To configure the session initiation time and session close time use the below commands:

```
[edit security]
user@host# set policies from-zone untrust to-zone trust policy name then log session-init
user@host# set policies from-zone untrust to-zone trust policy name then log session-close
```

It is recommended to have a policy or a captive portal that could authenticate users if they are not already logged on to the Active Directory. Ensure that the captive portal is configured to use the below example:

```
[edit security policies from-zone LAN to-zone FINANCE policy FinanceAUTH]
user@host# set match source-address any
user@host# set match destination-address Payroll
user@host# set match application any
```

```
user@host# set match source-identity unauthenticated-user
user@host# set match source-identity unknown-user
user@host# set then permit firewall-authentication user-firewall web-redirect
user@host# set then permit firewall-authentication user-firewall web-redirect-to-https
user@host# set then log session-init
user@host# set then log session-close
```

Juniper Secure Edge Deployments

IN THIS SECTION

- Configuration of Juniper Secure Edge Deployments | 36

Configuration of Juniper Secure Edge Deployments

IN THIS SECTION

- Add Directory Services | 37

NOTE: If you plan to use both Secure Edge and On-Premises deployment, kindly follow the on-premises deployment instructions first.

If you use Juniper Secure Edge services with JIMS, in the Secure Edge management interface you must generate the JIMS configuration file and download it to your local JIMS server. To do so, navigate to **Secure Edge** > **Identity** > **JIMS** > **Onboard**.

On the local JIMS server, import the JIMS configuration file into JIMS using the JIMS administrative UI. To do so, navigate to **File** > **Juniper Secure Edge Connect**. This will automatically import the settings for Secure Edge.

If you use the on-premises enforcement points, you can configure them as described in chapter "Configuration of Customer Managed Devices (On-Premises) Deployment" on page 26.

Add Directory Services

You must configure at least one directory server for JIMS Collector to collect users, devices, and group memberships. Currently, only Active Directory is supported.

If you plan to use multiple Directory Server with the same credentials, you could create a template to reduce the input for each directory server.

To add a new Directory Server:

1. Click **Add** to add a new Directory Server.
2. Optionally use an already created template to pre-configure the credentials.
3. Enter the IP-address or FQDN of the server.
4. Give a description.
5. Enter the username (Login ID) and password for authentication purposes.
6. Choose **SSL Connection** if the Directory Server is on a different host.
   Select and configure your active directory for LDAPS or TLS communication.