JUNIPER | Engineering
NETWORKS | Simplicity

Juniper Identity Management Service User Guide

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

YEAR 2000 NOTICE

END USER LICENSE AGREEMENT

Table of Contents

About This Guide

Use this guide to prepare, install, and configure the Juniper Identity Management Service for use with SRX Series devices and with Contrail Service Orchestration (optional) in your network.

1
CHAPTER

Juniper Identity Management Service Overview

Introduction

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.

If your network environment uses Contrail Service Orchestration (CSO) to deploy network services in the Cloud CPE Centralized deployment model, Juniper Identity Management Service supports operation with each CSO to facilitate the handling of firewall security policy decisions between the CSO platform and SRX Series devices by providing domain, group, user, and device identity information from Active Directory domains to each CSO.

Juniper Identity Management Service has the following features:

Centralized User Identity Data Collection

Juniper Identity Management Service provides a scalable service that can take over user identity data collection from Microsoft Active Directories, domain controllers, and Exchange servers, serving as a single, centralized data collection source for SRX Series devices and CSO in your network.

For example, Juniper Identity Management Service can replace the connections from individual SRX Series devices to multiple Active Directory domain controllers with a single connection from the service to each domain controller, eliminating scaling limitations.

Starting in Juniper Identity Management Service Release 1.0, you can configure Juniper Identity Management Service to collect user identity information for up to 100 SRX Series devices.

Starting in Juniper Identity Management Service Release 1.4.0, you can configure Juniper Identity Management Service to collect user identity information for up to 1200 SRX Series devices.

⚠ **CAUTION**: To mitigate brute force attacks, Juniper Identity Management Service only accepts requests from known devices and limits failed login attempts. To further protect against attacks, you should implement strong security business continuity plans, limit the exploitable attack surface, and only allow trusted administrators, networks, and hosts to access Juniper Identity Management Service deployments.

Data Collection from Event Log Sources

Juniper Identity Management Service connects to event log sources to collect user and device status events and provide IP address-to-username mappings to SRX Series devices. For user login events, it collects the domain name and username. For device login events, it collects the domain name and machine name.

An event log source can be a Microsoft Active Directory domain controller or a Microsoft Exchange server. You can configure event log sources for Juniper Identity Management Service that can be a combination of Active Directory domain controllers and Exchange servers.

Starting in Juniper Identity Management Service 1.0, Juniper Identity Management Service supports up to 25 Active Directory domains.

Data Collection from User Information Sources

Juniper Identity Management Service connects to user information sources to collect group information for users and their devices and provide username-to-group mappings to SRX Series devices. The service queries each user information source for its supported domains and selects a source by domain when it needs to initiate user or device information queries. It queries the appropriate user information source each time it receives a login event for a user.

Starting in Juniper Identity Management Service Release 1.0, you can configure up to 100 Active Directories as user information sources for Juniper Identity Management Service.

Data Collection from Syslog Sources

Juniper Identity Management Service connects to syslog sources to collect event data and user information data from an event source such as a DHCP server. The number of syslog entries is limited to 200. You define the IP address and port of the remote syslog server that the JIMS server permits a connect from the remote server. You configure the JIMS server to collect syslog data whenever it detects the occurrence of a logoff event, logon event, or a change in value from the remote server session.

The JIMS server collects data from syslog messages containing username, groups, and/or IP address mappings, and turns those messages into entries in its cache. The JIMS server transmits this information to each SRX Series device for it to use in making policy decisions in the user firewall feature.

Support for Identity-Based Security Policies on SRX Series Devices

Juniper Identity Management Service enables you to apply policies on SRX Series devices (including the vSRX 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 the associated groups (session information), and provides this information to the SRX Series devices, which use the mapping information to generate entries for their authentication tables that you can use to enforce user-based and group-based security policy control. On SRX Series devices, user groups are known as user roles.

Support for Identity-Based Security Policies on CSO

Support for Identity-Based Security Policies on CSO is supported in Juniper Identity Management Service Release 1.1 and later.

Juniper Identity Management Service is available as a standalone product or as an integrated identity management service from within Contrail Service Orchestration (CSO) running Release 3.3 or a later release.

CSO is deployed in the cloud, and the tenant infrastructure includes the tenant premises behind a firewall and cannot directly access Microsoft Active Directory. Juniper Identity Management Service acts as the communication layer between identity servers such as Microsoft Active Directory and the CSO platform. Juniper Identity Management Service assists CSO in defining user firewall policies to filter

traffic on SRX Series devices in a distributed deployment by providing user, device, and group identity information from the Active Directory domains to each CSO.

All communication between Juniper Identity Management Service and CSO is initiated by the JIMS server. Upon startup, or configuring or updating CSO, the JIMS server initiates HTTPS connection to each fully configured CSO.

The information exchange between Juniper Identity Management Service and each fully configured CSO is secure, live, and allows for a full resynchronization at any point in the data collection process.

Templates

Templates are supported in Juniper Identity Management Service Release 1.1 and later.

You can develop one or more templates in Juniper Identity Management Service:

- SRX Series Device Templates—Support the grouping of client configurations to facilitate the configuration of multiple SRX Series devices.

- Data Source Templates—Support the grouping of event or information source configurations to facilitate the configuration of a specific data source.

A template is a way to share common configuration attributes across items within a homogeneous collection without having to re-enter those attributes for each configuration instance (that is IP address). Templates allow configurations to share common data.

A template provides default settings that can be referenced by multiple instances. A special ID provides a single reference that is utilized by multiple configuration items within a type of collection (for example, SRX Series clients, Event Source, or Info Sources).

For example, when using an SRX series device template, you can specify a username and password in a template, and assign that template across all SRX Series devices that require the same login credentials. Utilizing a template allows you to copy the configuration and only re-enter the password for the specific template.

Domain PC Probing

Domain PC probing acts as a supplement to event log reading. When a user logs in to a domain, the event log contains that information. When there is no IP address-to-username mapping from the event log, Juniper Identity Management Service initiates a domain PC probe to the device to get the username and domain of the currently active user. Domain PC probes are also used to determine a device's status after its logged-in state has expired.

Juniper Identity Management Service initiates a domain PC probe:

- When it receives a query from an SRX Series device for a specific IP address when the user is not known.

- When a user's session or a device's session times out after the configured session timeout period. The PC probe helps to determine a logged-in or logged-out state for the user or device.

Note the following usage considerations about domain PC probing:

- Domain PC probing works on Microsoft Windows endpoints only.

- Juniper Identity Management Service creates and maintains sessions for Active Directory domain controllers as well as domain PCs. This might result in the service attempting to send PC probes to the domain controllers. To avoid this behavior, add the IP addresses of the domain controllers as an excluded entry in the IP filter on Juniper Identity Management Service. See "Configuring IP Address Filters" on page 62 for information about IP filtering.

Session Reporting to SRX Series Devices

When reporting to SRX Series devices, Juniper Identity Management Service generates reports that contain records of the IP address, username, and group relationship information collected from the user identity data sources.

Juniper Identity Management Service generates a report:

- When it discovers a new user session.

- When a user session is in the logged-in state and then times out waiting for user group information. In this case, the report does not contain the user group information.

- When it discovers user group information for an active user session.

- When the user session is in the logged-in state and times out waiting for a PC probe response or when a PC probe fails. This results in Juniper Identity Management Service determining a logged-out state for the session.

- In response to individual queries for missing information with reports containing the requested information.

Juniper Identity Management Service keeps a list of reports that are communicated to the SRX Series devices in XML or JavaScript Object Notation (JSON) format, depending on the API utilized by JIMS server-SRX Series device communication.

The service also generates reports for device-only sessions without sending the username in the report when the username is not available. For SRX Series devices running Junos OS Release 15.1X49-D100, 17.4R1, or a later release, you can enforce security policies based on device authentication as well as on user authentication.

After Juniper Identity Management Service generates a report, it sends the report to the SRX Series devices and CSO in your network.

- For SRX Series devices running Junos OS Release 15.1X49-D100, 17.4R1, or a later release, the SRX Series devices can initiate requests for batch reports from the service. A batch report contains multiple records. Based on the information in the report, the SRX Series devices create authentication entries in their authentication tables to enforce security policy control over access to protected corporate resources and the Internet.

- For SRX Series devices running Junos OS Release 12.3X48-D45 or later, the service immediately posts reports to the SRX Series devices when using the legacy Web API function (webapi).

- Starting in Junos OS Release 18.1R1, SRX Series devices supports IPv6 addresses associated with the source identities in security policies. If an IPv4 or IPv6 entry exists, policies matching that entry are applied to the traffic and access is either allowed or denied.

  SRX Series devices search the identity management authentication table for information based on IPv6 addresses. Click the IPv6 **Enabled** checkbox in the JIMS Administrative Interface to generate session reports containing IPv6 addresses.

  Session reports are unique per address. Therefore a user with both an IPv4 and an IPv6 addresses are reported as two distinct sessions to the SRX Series device.

- Prior to Junos OS Release 17.4R1, SRX Series devices only handle sessions with IPv4 addresses. Uncheck the client configuration **IPv6 Enabled** checkbox on JIMS server to avoid sending sessions with IPv6 addresses.

Query Support for SRX Series Devices

Juniper Identity Management Service responds to queries from SRX Series devices with the corresponding IP addresses, usernames, and device names. The service also responds to individual IP address queries with the corresponding usernames and device names.

For SRX Series devices running Junos OS Release 15.1X49-D100, 17.4R1, or a later release, batch queries from individual SRX Series devices can filter information based on a combination of timestamp, domain, and IP address. When SRX Series devices miss data for an existing flow, they can engage a captive portal to get the username. Once the user is authenticated by the captive portal, the SRX Series devices can issue an additional query to Juniper Identity Management Service, specifying the username and IP address to obtain the corresponding group information.

Reports Sent to CSO

Support for Reports Sent to CSO is supported in Juniper Identity Management Service Release 1.1 and later.

When reporting to CSO, Juniper Identity Management Service updates the CSO with a list of reports to be communicated. Juniper Identity Management Service maintains a separate list for each report type: Domains, Groups , Users, and Devices.

When the connection from Juniper Identity Management Service to CSO starts (or restarts), the JIMS server begins to transmit domain or group or user and device reports to CSO.

CSO reports are maintained in a set of active lists for each type of report. If an item being reported changes state (for example, a user changes from enabled to disabled, or a group is deleted), then the old report is replaced with a current report that is transmitted to CSO.

Juniper Identity Management Service renders reports to CSO in JavaScript Object Notation (JSON) format.

Server Certificates for Authentication with SRX Series Devices

Juniper Identity Management Service enables you to select automatically generated server certificates or configure previously imported certificates for server authentication with the SRX Series devices in your network. Specifying a server certificate enables the JIMS server to authenticate with SRX Series devices before communicating with them. This certificate is used for the TLS connection from the SRX Series device to encrypt the data between the SRX and JIMS server.

The server certificate needs to be installed in the following location: `Certificates (Local Computer) / Personal / Certificates`.

Note that the JIMS server automatically creates a self-signed root CA certificate as well as a certificate based on the root CA in the above location that is utilized by default. If that certificate expires, it can be deleted, that triggers the JIMS server to recreate it when the JIMS service is restarted.

The certificate configuration is found on the JIMS Administrative Interface at Settings > General > SRX Client Query Configuration. However, it is not recommended that this be changed unless you really understand certificate management on Windows. Note that JIMS requires certain fields to be set to specific values in the certificate in order to utilize it.

System-Level IP Address, Event, and Group Filtering

Juniper Identity Management Service enables you to specify IP address ranges to include in or exclude from reports the JIMS server sends to SRX Series devices. You can also specify Active Directory user groups to include in the reports. These filters are applied to all the SRX Series devices in your network.For SRX Series devices running Junos OS Release Junos OS Release 15.1X49-D100, 17.4R1, or a later release, you can apply IPv4 address filters. For SRX Series devices running Junos OS Release 18.3R1 or later, the JIMS server supports both IPv4 and IPv6 address filtering for the SRX Series devices in your network.

JIMS supports both IPv6 filter from the SRX Series device 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 JIMS server receives the logon events from the configured event sources. For example: If 192.0.2.1 is added as the exclude IP address in the system-level filter on JIMS server. When a user with 192.0.2.1 logs on the domain controller, JIMS server ignores the session for this user. Thus no entry with 192.0.2.1 is sent to the SRX Series device.

The IPv6 filters used by the SRX Series device query are configured on SRX Series device. The SRX Series device includes or excludes the IP addresses in the batch query that it sends to JIMS server. The JIMS server replies with the entries based on the filters received from the SRX Series device. However, note that the SRX Series devices only apply filter within the context of the system-level filter. For example, If 192.0.2.0/24 is configured on SRX Series device as the include filter. The SRX Series device 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 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 devices 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 the JIMS server sends to SRX Series devices. 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 devices running Junos OS Release 15.1X49-D100, 17.4R1, or a later release, Juniper Identity Management Service applies the filters it receives from individual SRX Series devices. If filtering is also configured on Juniper Identity Management Service, the service first applies its own filters to all the SRX Series devices in your network, and then applies the filters it receives from the individual SRX Series devices.

Connected Network Device Monitoring

You can monitor the status of the network devices connected to the JIMS server, including:

- SRX Series devices

- Contrail Service Orchestration (CSO)

- Event log sources, which can be Microsoft domain controllers or Exchange Servers

- User information sources, which can be Microsoft Active Directories

- System log messages (also called syslog messages) logged by network elements as an event source

- Domain PC probes to user devices

JIMS Logging

For troubleshooting purposes, Juniper Identity Management Service is installed with a default log called jims_*yyyymmdd_nnnnn*.log, which is stored in **\Program Files (x86)\Juniper Networks\Juniper Identity Management Service\logs**. For example, a default log can be called: jims_20180117_00000. The log includes the following event types:

- **System**—Configuration, administration, and system-level events

- **Client**—HTTPS/HTTP GET requests from and HTTPS/HTTP POST submissions to the SRX Series devices or CSO (HTTPS request/submissions only)

- **Event Source**—User and device events generated by external networking devices and received via system log messages (also called syslog messages).

- **Info Source**—Active Directory events

- **PC Probe**—PC probe requests per set of administrative credentials

- **Sessions**—Internal session finite state machine (FSM) transitions and internal cache events for domains, sessions, users, devices, and groups

Logging levels for each component can be set to:

- **None**—No logging

- **Error**—Critical events affecting the entire system

- **Warning**—Unexpected per-transaction events

- **Standard**—Minimal logging for a concise view of transaction flows

- **Detail**—Detailed logging for a broader view of transaction flows

- **Debug**—Most detailed logging level for troubleshooting

Each logging level includes events from the previous levels.

Juniper Identity Management Service also supports the ability to receive remote system log event data and user information data from an event source (such as a DHCP server). You define the IP address and port of the remote syslog server that the JIMS server permits a connect from the remote server. You configure the JIMS server to collect syslog data whenever it detects the occurrence of a logoff event, logon event, or a change in value from the remote server session. The JIMS server transmits this information to each SRX Series device and CSO platform (if your network environment uses CSO) for it to use in making policy decisions in the user firewall feature.

High Availability

JIMS servers can be configured in a primary and secondary (backup) server configuration with SRX Series devices and, if applicable, CSO.

- For SRX Series devices, the SRX sends HTTPS queries to the primary JIMS server and falls back to the secondary server when queries to the primary JIMS server fail. The SRX Series devices probe the primary server and change back to it when the primary server becomes available again.

- For CSO, both the primary and secondary JIMS server poll the CSO at regular intervals. Data is only sent by the JIMS server that is still active. When the CSO platform detects that the primary JIMS server is down (absence of poll), it requests the secondary server to start sending data. If the primary JIMS server comes back online, the secondary server continues to send data until it goes down. At that point, CSO requests the primary JIMS server to restart sending data.

JIMS servers are agnostic as to whether they are being utilized as a primary or secondary service. There is no configuration specified in the JIMS server to make this distinction between usage as a primary or secondary service.

To implement high availability for the authentication table, an SRX Series device requires both a primary and a secondary JIMS server. CSO supports this configuration by supporting two JIMS servers using the same username and password for authentication for a single tenant.

Once authenticated, each JIMS server requests a PING filter configuration. CSO determines which JIMS server is to be the active source of reports (domains, groups and users) and which JIMS server is to be the backup and responds with either an active filter or a backup filter.

It is expected that both JIMS servers are configured to use the same Active Directory to maintain consistent reports from both servers. However, it is possible that the SRX Series device has active connections to both JIMS servers, so the SRX Series device may select a different JIMS server than CSO if there is a fault between the JIMS server and CSO that not exist between the SRX Series device and the JIMS server.

Release History Table

Release	Description
1.0	Starting in Juniper Identity Management Service Release 1.0, you can configure Juniper Identity Management Service to collect user identity information for up to 100 SRX Series devices.
1.0	Starting in Juniper Identity Management Service 1.0, Juniper Identity Management Service supports up to 25 Active Directory domains.
1.0	Starting in Juniper Identity Management Service Release 1.0, you can configure up to 100 Active Directories as user information sources for Juniper Identity Management Service.

How Juniper Identity Management Service Works with SRX Series Devices and CSO

shows how Juniper Identity Management Service works with SRX Series devices and Contrail Service Orchestration (CSO) in your network.

Figure 1: Juniper Identity Management Service Workflow

Step	Description
1.	Juniper Identity Management Service communicates with Microsoft Domain Controllers or Exchange Servers in Active Directory domains to collect event log information. Using the event log information, the service determines the IP addresses of Active Directory and Exchange users and abstracts IP address-to-username mapping information.
2.	Juniper Identity Management Service communicates with Active Directories to identify the groups to which users belong and abstracts username-to-group mapping information.

(Continued)

Step	Description
3.	After Juniper Identity Management Service has the IP address, username, and group relationship information stored in its cache, it generates a report and sends it to the SRX Series devices. Juniper Identity Management Service Works with CSO is supported in JIMS Release 1.1. If your network deployment includes CSO, Juniper Identity Management Service updates the CSO with a list of reports to be communicated. Juniper Identity Management Service maintains a separate list for each report type: Domains, Groups, Users, and Devices.
4.	Each SRX Series device receives the IP address, username, and user group relationship information and generates authentication entries that are used to enforce user-based and group-based security policy control over access to protected corporate resources and the Internet.

Keyboard and Menu Shortcuts

Keyboard and menu shortcuts supported in Juniper Identity Management Service Release 1.1 and later.

Keyboard shortcuts are keys or key combinations that you can use in instead of your mouse to navigate an interface. lists the keyboard shortcuts for the Juniper Identity Management Service Administrative Interface.

Table 1: Keyboard Shortcuts

Press this	To do this
F1	Display the Status tabs.
F2	Display the Data Source tabs.
F3	Display the Clients tabs.
F4	Display the Settings tabs.

Table 1: Keyboard Shortcuts *(Continued)*

Press this	To do this
Tab	Move to the next entry on the selected tab.
Left and right arrows	Move left and right across the displayed tabs.
Shift + Tab	Move back to a tab row.
Control + Home	Refresh the information in the Status tabs.
Control + Insert	Add information in the Data Sources, Clients, and Settings tabs.
Control + Delete	Delete the selected entry in the Data Sources, Clients, and Settings tabs.
Control + F11	Save an entry in the Settings tabs.
Escape	Cancel in the Settings tabs.
Ctrl + C	Copy the information from the selected entry to the clipboard in comma-separated values (CSV) file format.
Shift + Control + C	Copy the information from all entries in a tab's list to the clipboard in comma-separated values (CSV) file format, including the column headers as the first line.
Shift + left arrow	Scroll left in a row.
Shift + right arrow	Scroll right in a row.
Up arrow	Move up one entry.
Down arrow	Move down one entry.

Table 1: Keyboard Shortcuts *(Continued)*

Press this	To do this
Shift + Add button	Add a new entry pre-populated with the information from the currently selected entry. **NOTE**: This key combination works only on the Data Sources and Clients tabs.
Control + Shift + Insert	Add using the contents of the currently selected list item to pre-populate the information in a dialog box.
Control + F	Display the **Find in List** dialog box from any list in the Juniper Identity Management Service Administrative Interface. When a find operation is successful, the row containing the text is selected. The list does not have rows highlighted if the text is not found. The **Find in List** dialog box remains active until it is manually closed. This allows the dialog box to maintain context for a subsequent find. The **Control + F** and **Edit > Find** key sequence starts the search from the beginning of the list for the Next button **[»]** or from the end of the list for the Previous button **[«]**. If you dismiss the list and then decide to resume the find operation from the last point, use **Shift + Control + F** to start from the last row found. By default, the **Find in List** dialog box operates across all columns. You can make a selection from the drop-down list to narrow the search within a specific column. Click the **Exact Match** check box in the **Find in List** dialog box to force an exact match to narrow the search. By default, the check box is unchecked, which means that there is a partial match when searching.
Shift + Control + H	Access the **About Administrative Interface** dialog box.

lists the menu keyboard shortcuts for the Juniper Identity Management Service Administrative Interface.

Table 2: Menu Keyboard Shortcuts

Menu Command	Shortcut Keys	To do this
File > Connect	Control + N	Log in to the JIMS server.

Table 2: Menu Keyboard Shortcuts *(Continued)*

Menu Command	Shortcut Keys	To do this
File > Exit	Control + T	Exit from the JIMS server.
Edit > Find	Control + F	Display the Find in List dialog box from any list in the Juniper Identity Management Service Administrative Interface. By default, the Find in List dialog box operates across all columns. You can make a selection from the drop-down list to narrow the search within a specific column. Refer to Control + F in Table 1 on page 14 for more details.
Edit > Copy	Control + C	Copy the information from all entries in a tab's list to the clipboard in comma-separated values (CSV) file format, including the column headers as the first line.
Edit > Copy All	Shift + Control C	Copy the information from all entries in a tab's list to the clipboard in comma-separated values (CSV) file format.
Help > View Help	Control + H	Launch the Juniper Identity Management Service online help.
Help > About	Shift + Control + H	Access the **About Administrative Interface** dialog box.

Juniper Identity Management Service Configuration Overview

Table 3 on page 18 lists the basic tasks to configure Juniper Identity Management Service.

> **NOTE**: These tasks assume that you already have your SRX Series devices and data sources installed, configured, and operational at your site.

Optionally, if your network environment uses Contrail Service Orchestration (CSO), these tasks assume that you already have CSO installed, configured, and operational at your site.

Table 3: Juniper Identity Management Service Configuration Tasks

Task	Description	Action
Prepare your SRX Series devices	Perform a series of configuration taks to prepare the SRX Series devices in your network to work with Juniper Identity Management Service.	For SRX Series devices running Junos OS Release 15.1X49-D100, 17.4R1, or a later release, follow the instructions for configuring the Advanced Query feature in "Preparing SRX Series Devices Running Junos OS Release 15.1X49-D100, 17.4R1, or Later" on page 21. For SRX Series devices running Junos OS Release 12.3X48-D45 or later, follow the instructions for "Preparing SRX Series Devices Running Junos OS Release 12.3X48-D45 or Later" on page 24.
Prepare your data sources	Perform a series of configuration taks to prepare the data sources in your network to work with Juniper Identity Management Service.	"Data Source Configuration Overview" on page 31
Install Juniper Identity Management Service	Install Juniper Identity Management Service on a Windows server	"System Requirements for Installing Juniper Identity Management Service" on page 36 "Installing Juniper Identity Management Service" on page 39

Table 3: Juniper Identity Management Service Configuration Tasks *(Continued)*

Task	Description	Action
Prepare CSO (optional)	If your network deployment includes CSO, perform a series of configuration taks to prepare CSO in your network to work with Juniper Identity Management Service.	"Preparing CSO Identity Management" on page 51
Login to Juniper Identity Management Service	Log into the JIMS server and perform initial setup activities.	"Logging in to the JIMS Server" on page 42
Configure SRX Series devices as clients of JIMS server	Configure Juniper Identity Management Service to connect to the SRX Series devices in your network.	"Configuring the Connection to an SRX Series Device" on page 55
Configure CSO as client of JIMS server (optional)	If your network deployment includes CSO, configure Juniper Identity Management Service to connect to CSO in your network.	"Configuring the Connection to a CSO Client" on page 61
Configure Juniper Identity Management Service data sources	Configure Juniper Identity Management Service to connect to the data sources in your network.	"JIMS Server Data Source Configuration Overview" on page 69

2

CHAPTER

SRX Series Device Preparation

SRX Series Device Configuration Overview

Before you install and configure Juniper Identity Management Service, prepare the SRX Series devices (including the vSRX Virtual Firewall) in your network to work with the JIMS server by performing a series of configuration tasks.

Table 4 on page 21 lists the Junos OS releases running on the SRX Series devices that are supported by the JIMS server and the required configuration tasks to perform for each supported release.

Table 4: SRX Series Device Configuration Tasks

Junos OS Release	Configuration Tasks
15.1X49-D100, 17.4R1, or a later release	Follow the instructions for "Preparing SRX Series Devices Running Junos OS Release 15.1X49-D100, 17.4R1, or Later" on page 21.
12.3X48-D45 or later	Follow the instructions for "Preparing SRX Series Devices Running Junos OS Release 12.3X48-D45 or Later" on page 24.

Preparing SRX Series Devices Running Junos OS Release 15.1X49-D100, 17.4R1, or Later

To enable SRX Series devices (including the vSRX Virtual Firewall) running Junos OS Release 15.1X49-D100, 17.4R1, or a later release, to work with Juniper Identity Management Service, you must configure the Advanced Query feature on the SRX. This feature enables the SRX Series device to perform an advanced user identities query from the JIMS server to obtain user identity information, and for the SRX Series device to pull information from a range of user identities from the JIMS server.

When you configure the Advanced Query feature, the SRX Series device

- Queries the JIMS server for identity information that it collected.

- Populates its local active directory authentication table with the information that it obtained from the JIMS server.

- Uses its populated local active directory authentication table to authenticate a user or a device requesting access to a protected resource.

The Advanced Query feature also allows you to push authentication entries to the JIMS server for users for whom there are not entries in JIMS but who have successfully authenticated to the SRX Series device through captive portal.

To configure the Advanced Query feature for SRX Series devices:

- Review the Understanding the SRX Series Advanced Query Feature for Obtaining User Identity Information from JIMS topic.

- Use the `identity-management` configuration parameters listed in Table 5 on page 22.

Table 5: SRX Series Device Configuration Tasks

`identity-management` Configuration Statement	Function	Junos OS for SRX Series Documentation Reference
`authentication-entry-timeout`	Configure the time-out for the user identity authentication entries. You configure this parameter as part of the advanced user identity query feature for SRX Series devices.	authentication-entry-timeout (Identity Management Advanced Query)
`batch-query`	Configure the SRX Series device to communicate with the JIMS server to obtain an access token to use to query the server for identity information for an individual user (IP query and user query) or a group of users (batch query). The access token allows the SRX Series device to connect to the JIMS server to query it for this information.	batch-query

Table 5: SRX Series Device Configuration Tasks *(Continued)*

identity-management Configuration Statement	Function	Junos OS for SRX Series Documentation Reference
connection	Configure parameters for connecting SRX Series devices to the JIMS server to obtain user identity and device information. These parameters include the protocol, the IP address of the JIMS server, and the information to authenticate the SRX Series device to the JIMS server. **NOTE**: If you are using more than one JIMS server, you must configure each server separately. The SRX Series device always attempts to connect to the primary server first. If the primary server fails, the SRX Series device falls back to the secondary server. The SRX Series device periodically probes the failed primary server and reverts to it when it is available.	connection (Identity Management Advanced Query)
filter	The advanced user identity query feature enables the SRX Series device to communicate with the JIMS server to obtain user identity information for an individual user (ip-query) or a group of users (batch query). Optionally, you can configure filters to convey to the JIMS server at a more granular level the users for whom you want information, based on their IP addresses.	filter (Identity ManagementAdvanced Query)
invalid-authentication-entry-timeout	Configure an independent timeout value to be assigned to invalid user authentication entries in the SRX Series device authentication table for Windows Active Directory. The invalid authentication entry timeout setting is different from the general authentication entry timeout setting. It allows you to protect invalid user authentication entries in an authentication table from expiring before the user can be validated.	invalid-authentication-entry-timeout (Services User Identification Active Directoryand ClearPass)
ip-query	Used for the IP query function. When this feature is enabled, the SRX Series device queries the JIMS server for user identity information based on the IP address of a user's device.	ip-query (Identity Management Advanced Query)

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

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;
}
```

Preparing SRX Series Devices Running Junos OS Release 12.3X48-D45 or Later

IN THIS SECTION

To prepare SRX Series devices running Junos OS Release 12.3X48-D45 or later to work with Juniper Identity Management Service, perform the following tasks.

Configuring the SRX Series User Query Function to Connect to Juniper Identity Management Service

Configuring the user query function allows an SRX Series device running Junos OS Release 12.3X48-D45 or later to connect automatically to Juniper Identity Management Service to make requests for authentication information for individual users.

The user query function supplements input from Juniper Identity Management Service. For the user query function, the SRX Series device is the HTTPS client and sends HTTPS requests to Juniper Identity Management Service on port 443.

Before you begin, you need the following information:

- The hostname of the JIMS server

- The IP address of the JIMS server

- The port number on the JIMS server for receiving HTTPS requests

- The client ID to obtain an OAuth token from the JIMS server for user queries

- The client secret to obtain an OAuth token from the JIMS server for user queries

To configure the SRX Series device to make individual user queries automatically:

1. Configure Juniper Identity Management Service as the authentication source for user query requests, and configure the JIMS server name and its IP address. The SRX Series device requires this information to contact the server.

   ```
   [edit services user-identification]
   user@host#set authentication-source aruba-clearpass user-query web-server jims address
   192.168.5.10
   ```

2. Configure the port number on the JIMS server to which the SRX Series device sends HTTPS requests.

   ```
   [edit services user-identification]
   user@host#set authentication-source aruba-clearpass user-query web-server jims port 443
   ```

3. Configure the client ID and client secret that the SRX Series device requires to obtain an OAuth access token required for user queries.

```
[edit services user-identification]
user@host#set authentication-source aruba-clearpass user-query client-id client-id
user@host#set authentication-source aruba-clearpass user-query client-secret client-secret
```

The client ID and client secret are required values. They must match the client ID and client secret that you configure later for this SRX Series client on Juniper Identity Management Service.

4. Configure the token API that is used in generating the URL for acquiring an OAuth access token.

```
[edit services user-identification]
user@host#set authentication-source aruba-clearpass user-query token-api "oauth_token/oauth"
```

In this example, the token API is **oauth_token/oauth**. It is combined with the following information to generate the complete URL for acquiring an OAuth access token (https://192.168.5.10/oauth_token/oauth).

- The connection method is HTTPS.

- In this example, the IP address of the JIMS server is 192.168.5.10.

5. Configure the query API to use for querying individual user authentication and identity information.

```
[edit services user-identification]
user@host#set authentication-source aruba-clearpass user-query query-api "user_query/v1/ip/$IP
$"
```

In this example, the query-api is **user_query/v1/ip/IP**. It is combined with the URL **https://192.168.5.10/oauth_token/oauth** resulting in **https://192.168.5.10/oauth_token/oauth/user_query/v1/ip/IP**.

The **IP** variable is replaced with the IP address of the end-user's device for the user whose authentication information the SRX Series device is requesting.

6. Configure the amount of time in seconds to delay before the SRX Series device sends the individual user query. In this example, there is no delay.

```
[edit services user-identification]
user@host#set authentication-source aruba-clearpass user-query delay-query-time 0
```

7. Configure the timeout interval in minutes after which idle entries in the authentication table on the SRX Series device expire. The timeout interval begins from when the user authentication entry is added to the authentication table.

```
[edit services user-identification]
user@host#set authentication-source aruba-clearpass authentication-entry-timeout 240
```

Configuring the SRX Series Web API to Connect to Juniper Identity Management Service

Configuring the SRX Series Web API allows Juniper Identity Management Service to initialize a connection to an SRX Series device running Junos OS Release 12.3X48-D45 or later.

Before you begin, you need the following information:

- Device running on JIMS 1.3 or earlier releases

- A username and password for the Web API daemon account

- The IP address of the JIMS server's data port

- The name of the security zone to allow the Web API at the zone level

To configure the Web API daemon to work with Juniper Identity Management Service:

1. Configure the Web API daemon (webapi) username and password for the account.

    This information is used for the HTTPS certification request.

    ```
    [edit system services]
    user@host#set webapi user username password password
    ```

2. Configure the Web API client address. This is the IP address of the JIMS server's data port.

    The SRX Series device accepts information from this address only.

> **NOTE**: The JIMS server's data port whose address is configured here is the same one that is used for the user query function, if you configure that function.

```
[edit system services]
user@host#set webapi client 192.168.5.10
```

In this example, 192.168.5.10 is the IP address of the JIMS server's data port.

3. Configure the Web API daemon HTTP service port and HTTPS service port.

If you enable the Web API service on the default TCP port 8080 or 8443, you must enable host inbound traffic on that port.

```
[edit system services]
user@host#set webapi http port 8080
user@host#set webapi https port 8443
```

4. Configure the Web API daemon to use the HTTPS default certificate.

```
[edit system services]
user@host#set webapi https default-certificate
```

5. Configure the trace level for the Web API daemon.

The supported trace levels are notice, warn, error, crit, alert, emerg. The default value is error.

```
[edit system services]
user@host#set webapi debug-level alert
```

6. Allow the Web API at the zone level (the zone in this example is called Infra).

```
[edit security zones]
user@host#set security-zone Infra host-inbound-traffic system-services webapi-clear-text
user@host#set security-zone Infra host-inbound-traffic system-services webapi-ssl
```

RELATED DOCUMENTATION

3
CHAPTER

Data Source Preparation

Data Source Configuration Overview

Before you install and configure Juniper Identity Management Service, prepare the data sources in your network by configuring a set of user accounts on the sources with limited permissions. Data sources can be Microsoft Active Directories, Active Directory domain controllers, and Exchange servers. Juniper Identity Management Service requires the username and password of valid user accounts to perform various operations when collecting user identity information from the data sources. Configuring limited permission user accounts minimizes the possibility of security compromises during these operations.

> ⚠️ **CAUTION**: To mitigate brute force attacks, Juniper Identity Management Service only accepts requests from known devices and will limit failed login attempts. To further protect against attacks, you should implement strong security business continuity plans, limit the exploitable attack surface, and only allow trusted administrators, networks, and hosts to access Juniper Identity Management Service deployments.

Perform the configuration tasks in this section on any domain server in the Microsoft Active Directory domain that will be served by Juniper Identity Management Service. If you have multiple Active Directory domains, perform these configuration tasks on a domain server in each of the domains.

On each forest that you have no default trusts to the parent, create three user accounts with limited permissions. For example:

- **JIMS-EventLogRemoteAccess**—Used for event log sources, which can be Microsoft Active Directory domain controllers and Exchange servers

- **JIMS-ADRemoteAccess**—Used for user information sources, which are Microsoft Active Directories

- **JIMS-PC-Probe**—Used for PC probes from Juniper Identity Management Service to domain PCs

To configure data sources, perform these tasks:

- "Configuring User Accounts with Limited Permissions" on page 32

- "Permitting Remote WMI for Domain PC Probes" on page 34

- "Setting Up Windows Firewall to Allow Remote Event Log Management" on page 34

Configuring User Accounts with Limited Permissions

Configuring limited permission user accounts minimizes the possibility of security compromises during communications between Juniper Identity Management Service and its data sources.

To configure limited permission user accounts on the data sources, perform these tasks:

Configuring Limited Permission User Accounts

For each new user account:

1. From the Start menu, select **Active Directory Users and Computers**.
2. Navigate to the forest's Users container.
3. Right-click **Users** and select **New Users**.
4. Specify a descriptive first and middle name and any username or pre-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.

Configuring Properties for Limited Permission User Accounts

To set properties for each new user account:

1. Right-click a user and then select **Properties**.

2. Select the **Remote Control** tab.

3. Clear the **Enable Remote Control** check box.

4. Select **Remote Desktop Services Profile**.

5. Select the **Deny this user's permissions to log onto remote desktop session host server** check box.

6. Select the **Dial-in** tab and select the **Deny Access** check box.

Adding Limited Permission User Accounts to Active Directory Groups

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

1. Select **Built-in** under the forest.

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.

Defining 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. In the Group Policy Manager, select the forest, select **Default Domain Policy**, and right-click **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 each new user account.

5. Select **Deny Logon through Remote Desktop Services**, select **Define these policy settings**, and add each new user account.

6. Select **Deny Logon through Terminal Services**, select **Define these policy settings**, and add each new user account.

7. Select **Deny logon as a batch job**, select **Define these policy settings**, and add each new user account.

8. Select **Deny Logon as a service**, select **Define these policy settings**, and add each new user account.

RELATED DOCUMENTATION

Data Source Configuration Overview | 31

Permitting Remote WMI for Domain PC Probes

To permit remote Windows Management Instrumentation (WMI) for PC probes from Juniper Identity Management Service to domain PCs:

1. In the Group Policy Manager, select the forest, select **Default Domain Policy**, and right-click **Edit**.
2. Select **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security > Inbound rules node**. Note that there are two levels of Windows firewall with advanced security.
3. Right-click and select **New Rule**.
4. Select **Predefined**, select **Windows Management Instrumentation**, select **Next**, select **Allow the connection**, and select **Finish**.

Setting Up Windows Firewall to Allow Remote Event Log Management

To configure Active Directory domain controllers and Exchange servers to allow Juniper Identity Management Service to connect when the host Windows Firewall is enabled:

1. In the Windows Control Panel, select **Security** and select **Windows Firewall with Advanced Security**.
2. Select **Inbound Rules** and in the list, right-click **Remote Event Log Management (RPC)** and select **Enable Rule**.

4

CHAPTER

JIMS Server Installation

System Requirements for Installing Juniper Identity Management Service

This section includes the following topics:

Specifications

Specifications supported in Juniper Identity Management Service Release 1.1 and later.

lists the JIMS server specifications.

Table 6: JIMS Server Specifications

Component	Specifications for JIMS release 1.3.x or earlier	Specifications for JIMS release 1.4.0 or later
Supported Junos OS 12.3X48-D45 or a later release	Yes	Yes
ClearPass Integration	With ClearPass Web API	Without ClearPass Web API
Supported Contrail Service Orchestration (CSO) release	Release 3.3 or a later release	Release 3.3 or a later release
Maximum SRX Series devices	100	Up to 1200

Table 6: JIMS Server Specifications *(Continued)*

Component	Specifications for JIMS release 1.3.x or earlier	Specifications for JIMS release 1.4.0 or later
Maximum CSO platforms	10	10
Maximum event log sources	100	150
Maximum Active Directories	100	100
Maximum domains	25	25
Maximum user entries	500,000	500,000
Maximum syslog sources	200	200

System Requirements

Juniper Identity Management Service can be installed on the following Microsoft Windows platforms:

Specifications for JIMS release 1.3.x or earlier

- Windows Server 2019

- Windows Server 2016

- Windows Server 2012 R2 with Windows Server 2012 R2 Updates (KB2919355 and KB2999226)

Specifications for JIMS release 1.4.0 or later

- Windows Server 2016 or later

- Minimum system requirement for Juniper Identity Management Service—A server with a 4-core, 64-bit compatible 1.4 GHz or higher CPU, a minimum of 16 GB of system memory, and 100 GB of disk space.

- Recommended system requirement for Juniper Identity Management Service to scale up to 1200 SRX Series devices—A server with a 16-core, 64-bit compatible 2.4 GHs or higher CPU, a minimum of 64 GB of system memory and 128 GB of disk space is required.

BEST PRACTICE: Note the following best practices when installing Juniper Identity Management Service on a Microsoft Windows platform:

- Because Juniper Identity Management Service participates in the security infrastructure protecting your network, we recommend using Windows Update regularly and judiciously to obtain the latest Security Updates and other Critical Updates from Microsoft.

- Juniper Identity Management Service requires a server with a 4-core, 64-bit compatible 1.4 GHz or higher CPU, a minimum of 16 GB of system memory, and 100 GB of disk space.

NOTE: Juniper Identity Management Service uses the event log timestamp to decide the order of events, and, therefore, you might experience unexpected side issues if your domain controllers and Active Directories are not synchronized. This is more likely to happen across domains than within domains, which typically time-synchronize with their domain controller. Juniper Identity Management Service uses UTC (GMT) internally, and the time zone should not matter, only the time synchronization. See the Windows Time Service Tools and Settings documentation for Windows Server 2016 or 2012 R2.

Supported Identity Sources

Juniper Identity Management Service supports the following identity sources:

- Microsoft Active Directory on Windows Server 2012 R2 or later

- Microsoft Exchange Server 2010 with Service Pack 3 (SP3) and later

- Syslog

- PC Probe

-
    NOTE: Health mailboxes on Microsoft Exchange servers (users with a prefix of HealthMailBox) are filtered out by default by Juniper Identity Management Service.

Installing Juniper Identity Management Service

Before you begin, you will need the JIMS server's HTTPS server port number to be used to communicate with SRX Series devices and CSO.

You install Juniper Identity Management Service on Microsoft Windows platforms by means of an InstallShield installer that requires Administrator privileges to run.

If your network environment is running Contrail Service Orchestration (Release 3.3 or later), the Juniper Identity Management Service is bundled with CSO and can be downloaded directly from the Identity Management page of the Customer Portal of each tenant.

To install Juniper Identity Management Service:

1. Depending on how you intend to install Juniper Identity Management Service:

    - If you are installing Juniper Identity Management Service from the Juniper Networks Downloads page, locate the JIMS setup file on its Download Software page and click the file.

    - If you are installing Juniper Identity Management Service directly from the CSO platform, access the Identity Management page of the Customer Portal on CSO, and then click **Download JIMS**.

    A message appears at the bottom of your screen asking you what to do with the file.

2. At the bottom of your screen, click **Save** to save the file to your Downloads directory.

3. At the bottom of your screen, click **Run** to run the executable file.

    A message appears asking if you want to allow this application from an unknown publisher to make changes to your device.

4. Click **Yes** to allow InstallShield to install Juniper Identity Management Service on your system.

    The Welcome to the InstallShield Wizard for Juniper Identity Management Service page appears.

    > **NOTE**: If there are installation requirements that have not yet been installed on your system, a message appears alerting you that the installation requires a reboot of your system. Click **No** to continue with the installation and be sure to reboot your system after the installation has completed.

5. Click **Next**.

    The License Agreement page appears.

6. Select the option button for **I accept the terms in the license agreement** and click **Next**.

    The Customer Information page appears.

7. Type a username and a name for your organization and click **Next**.

    The Ports page appears.

8. Type the HTTPS server port number on the JIMS server to be used to communicate with the SRX Series devices. The default value is 443.

9. Click **Next**.

   The Setup Type page appears for selecting a complete or custom installation.

10. Make sure that the option button for the **Complete** setup is selected and click **Next**.

    The Ready to Install the Program page appears.

11. Click **Install**. Juniper Identity Management Service gets installed on your Windows system in **\Program Files (x86)\Juniper Networks\Juniper Identity Management Service**.

    The InstallShield Wizard Completed window appears.

12. Select the check box for **Launch JIMS Administrator** and click **Finish**.

    The Juniper Identity Management Service application page appears. The installation is now complete.

13. If a message appeared earlier alerting you that a system reboot is required, reboot your system now.

5
CHAPTER

JIMS Server Login and Initial Setup

Logging in to the JIMS Server

You log in to the JIMS server over an HTTPS connection using the Juniper Identity Management Service Administrative Interface to perform configuration and monitoring tasks. The administrative interface enables you to configure the server dynamically, making changes to the JIMS server's XML database without service interruption.

Before you begin, you need the username and password for a user in the local Administrator's group, which includes the "Domain Admins" group.

To log in to the JIMS server:

1. From the Windows Start menu, select **Juniper Networks > JIMS Administrative Interface**, right-click on **JIMS Administrative Interface**, and then select **Run as administrator**.

   NOTE: The JIMS Administrative Interface GUI can be accessed only from the server on which the JIMS server is installed and running.

   The Server Logon page appears.

2. Type your username and password for the administrator's group, such as the domain administrator's group.

   NOTE: For your username, you might need to include your domain name in the format: _domain\username_.

   When you get a failure message while logging in to the JIMS server, or adding event or user info sources, you should try using the other form of the username. For example:

   - Pre-2000-domain-name\username, where username is the sAMAccountName in Active Directory.

   - username@fqdn.com, where fqdn.com is the fully qualified domain name of the Active Directory domain.

3. Click **Connect.**

   The Juniper Identity Management Service Administrative Interface is now securely connected to the JIMS server.

4. To reconnect, select **File > Connect** to bring up the Server Logon page.

Configuring SRX Series Device Transport Settings

Support for Configuring SRX Series Device Transport Settings is supported in Juniper Identity Management Service Release 1.1 and later.

In the SRX Client Query Configuration section of the **Settings > General** tab, you can configure the following SRX Series device transport settings to communicate with the JIMS server:

- Server certificate for the JIMS server's HTTPS server that is used to authenticate with SRX Series devices and provide a secure data transfer. You can specify either an automatically generated server certificate or a previously configured certificate. You configure one server certificate to authenticate with all SRX Series devices in your network. This certificate is used for the TLS connection from the SRX Series device to encrypt the data between the SRX and JIMS server.

  The server certificate needs to be installed in the following location: `Certificates (Local Computer) / Personal / Certificates`.

  > **NOTE**: You must also configure a client certificate on the SRX Series devices.

- Transport Layer Security (TLS) HTTPS port used by the JIMS server to communicate with SRX Series devices. TLS ensures that the traffic is encrypted between the JIMS server and the SRX Series devices. By default, the HTTPS port is 443.

  > **NOTE**: The JIMS server communicates with SRX Series devices over TCP sockets. The JIMS server requires that the utilized TCP ports be enabled in the Windows Firewall to allow this communication. During installation, the installer script modifies the firewall settings to allow the correct ports to be enabled. If you subsequently change the ports, you must modify the firewall configuration to allow TCP communication over those sockets.

- You have the option to enable the Debug (HTTP) port. By default, the Debug (HTTP) port is disabled. You have the option to enable the Debug (HTTP) port to allow packet traces to be captured to diagnose communication issues between the SRX Series devices and JIMS server. By default, the Debug port is 8082.

Before you begin, note the following JIMS-SRX Series device transport configuration considerations:

- If using a previously created server certificate, you must import the certificate to the JIMS server using the Microsoft Management Console (mmc) application with the Certificates snap-in. If you import a server certificate, be sure to use the local computer certificate store.

- All SRX Series devices connected to a JIMS server are required to match the port configuration specified in the SRX Client Query Configuration section of the General tab to properly communicate with the JIMS server. Use the **show configuration services user-identification** command to confirm the SRX Service device configuration settings.

- Multiple services running on the same Windows Server instance cannot utilize the same port numbers. If you are unclear as to which port to select, execute the `netstat` command from the Windows Command Prompt to determine if there is a conflict. The same command can also verify that the JIMS server is listening on those particular ports.

- For SRX Series devices running Junos OS Release 18.3R1 or later, the JIMS server supports IPv6 connectivity between the JIMS server and SRX Series devices. By default, the JIMS server listens for IPv4 incoming IP addresses from SRX Series devices on the specified port. Click the **Advanced** button to configure IPv6 connections or IPv6 with dual-stack between the JIMS server and the SRX Series device.

To configure transport configuration settings for communication between the JIMS server and SRX series devices:

1. In the navigation pane, select **Settings** and then select the **General** tab.
2. Click **Edit**.
3. In the SRX Client Query Configuration section, select the automatically generated certificate or an imported certificate from the Certificate drop-down list.
4. To modify the TLS port value to use for communication with SRX Series devices, enter a value in the TLS (HTTPS) Port field. This value must be a valid TCP port number between 1024 and 65,535, and it must match the SRX WebAPI configuration. The default value for the HTTPS port is 443.
5. By default, Debug (HTTP) Port is disabled. If you want to enable it, click the check box and enter the HTTP port number on the SRX Series device to use for communication with the JIMS server. This value must be a valid TCP port number between 1024 and 65,535, and it must match the SRX WebAPI configuration. The default value for the HTTP port is 8082.

   > **NOTE**: For security considerations, we recommend that you specify an HTTPS port rather than an HTTP port. HTTP is supported primarily for debugging purposes.
   >
   > If you enable the Debug (HTTP) port and change the port value, ensure that the corresponding port configuration on the SRX Series devices is modified to match this setting.

6. To configure a more detailed set of HTTPS and HTTP transport communication settings with SRX Series devices, including support for IPv6 connections (SRX Series devices running Junos OS Release 18.3R1 or later), click the **Advanced** button. The Advanced SRX Transport Configuration page appears. From this page you can configure the following advanced communication settings for the TLS (HTTPS) Transport and Debug (HTTP) Transport ports.

- Port—TCP port for handling incoming TLS (HTTPS) or Debug (HTTP) connections. The default value for the HTTPS port is 443 and the default value for the HTTP port is 8082. This value must be a valid TCP port number between 1024 and 65,535

- Max Threads—Maximum number of simultaneous processing threads to handle requests on this port.

- Connections Per Thread—Maximum number of allocated connections per thread open to the server.

- Allow IPv6 Connections—Enables support for *only* IPv6 connections between the JIMS server and SRX Series devices running Junos OS Release 18.3R1 or later.

- Allow Dual-Stack—Enables socket support to allow IPv4 or IPv6 connections from SRX Series devices running Junos OS Release 18.3R1 or later.

  > NOTE: Click the **Allow Dual-Stack** check box *only* if you have clicked the **Allow IPv6 Connections** check box.

- Address—Restricts access by entering a specific IPv6 address in the Address field. This address must match the IPv6 address shown in the output of the `ipconfig` command, entered from a Windows command prompt.

  Entering an IP address in the Address field is optional. By default, the JIMS server listens for all incoming IP addresses on the specified port for IPv4 or IPv6 connections, based on the settings of the Allow IPv6 Connections and Allow Dual-Stack check boxes.

  For example:

  > **ipconfig**

```
Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::64ab:5dbd:f8ed:5284
   IPv4 Address. . . . . . . . . . . : 172.16.1.21
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1ab1:69ff:fe2c:5ed8
                                       172.16.1.252
```

Click **OK** to save the advanced transport configuration settings.

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

Configuring a Session Timeout Period

You configure a timeout period for user and device sessions that are monitored by event log sources, after which the JIMS server will attempts to send a domain PC probe to the device and receive a reply. If the PC probe of the device fails, the JIMS server infers a logout event. The PC probe helps determine a logged-in or logged-out state for the user or device.

> **NOTE**: The setting of the Session Timeout value depends on the time sensitivity of the user firewall policies configured on the SRX Series devices.

An event log source can be a Microsoft Active Directory domain controller or Exchange server.

To configure the session timeout period:

1. In the navigation pane, select **Settings** and then select the **General** tab.
2. Click **Edit**.
3. In the User Session Configuration section of the **Settings > General** tab, enter a session timeout period in the Logoff Time text field. The JIMS server setting applies across all SRX Series devices. This value can be between 1 and 1440 minutes. The default value is 1440 minutes.

   This timer starts after Juniper Identity Management Service sends a report to the SRX Series devices. Any login event, successful PC probe, or user update restarts this timer.

   > **NOTE**: If PC Probe credentials have not been configured, Juniper Identity Management Service considers the user logged out when the session timeout period has expired.

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

Configuring JIMS Logging

Juniper Identity Management Service enables you to configure a log file that can be helpful when troubleshooting problems. The system log file includes logging for the following event types:

- **System**—Configuration, administration, and system-level events

- **Client**—HTTPS GET requests from and HTTPS POST submissions to the SRX Series devices

- **Event Source**—User and device events generated by external networking devices and received via system log messages (also called syslog messages)

- **Info Source**—Active Directory events

- **PC Probe**—PC probe requests per set of administrative credentials

- **Sessions**—Internal session finite state machine (FSM) transitions and internal cache events for domains, sessions, users, devices, and groups

Juniper Identity Management Service is installed with a default log called jims_*yyyymmdd_nnnnn*.log, which is stored in **\Program Files (x86)\Juniper Networks\Juniper Identity Management Service\logs**. For example, a default log can be called: jims_20180117_00000. You can use the default log as is or edit the configuration to adjust the logging levels as needed.

To edit the default log configuration:

1. In the navigation pane, select **Settings** and then select the **Logging** tab.
2. Click **Edit**.
3. Edit the following settings as needed:

    - In the Filename Prefix text field, type a new filename, if needed.

    - In the Directory text field, enter a new pathname of the directory for storing log files by clicking **Select**, navigating to a folder for storing the log files, and then clicking **OK**. By default, log files are stored in **\Program Files (x86)\Juniper Networks\Juniper Identity Management Service\logs**.

    - In the Max size (MB) text field, type the maximum size in MB for a log file before stopping and closing the log file and starting another one. The default value is 0 MB, meaning there is no maximum size.

    - In the File Lifetime (days) text field, type the number of days to keep log files before deleting them. The default value is 30 days.

    - For each system component, select a logging level, which can be set to:

        - **None**—No logging

        - **Error**—Critical events affecting the entire system

        - **Warning**—Unexpected per-transaction events

        - **Standard**—Minimal logging for a concise view of transaction flows

        - **Detail**—Detailed logging for a broader view of transaction flows

- **Debug**—Most detailed logging level for troubleshooting

  Each logging level includes events from the previous levels.

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

6

CHAPTER

CSO Preparation

CSO Configuration Overview

The CSO Configuration Overview is supported in Juniper Identity Management Service Release 1.1 and later.

If your network deployment includes Contrail Service Orchestration (CSO), after you install Juniper Identity Management Service (see "Installing Juniper Identity Management Service" on page 39), prepare CSO in your network to work with the JIMS server.

From the Identity Management page of the Customer Portal of CSO, you define the following configuration settings:

- JIMS-to-CSO authentication credentials to synchronize user and user group updates from the JIMS server to CSO.

- SRX-to-JIMS connection and authentication credentials for the JIMS server to send IP address, username, and group relationship information to SRX Series devices. You can also configure a set of optional advanced settings for authentication timeout, and IP address and domain filters.

Table 7 on page 50 lists the Contrail Service Orchestrator release supported by Juniper Identity Management Service and the required configuration tasks.

Table 7: Contrail Service Orchestrator Tasks

Contrail Service Orchestrator Release	Configuration Tasks
Release 3.3 or a later release	Follow the instructions in "Preparing CSO Identity Management" on page 51.

RELATED DOCUMENTATION

Contrail Service Orchestration User Guide

Firewall Policy Overview

Preparing CSO Identity Management

Preparing CSO Identity Management is supported in Juniper Identity Management Service Release 1.1 and later.

To prepare Contrail Service Orchestration (CSO) to work with Juniper Identity Management Service, perform the following tasks from the CSO Customer Portal.

> **NOTE**: This procedure assumes that you have previously downloaded and installed Juniper Identity Management Service from the Identity Management page of CSO. If you have not yet performed installation, see "Installing Juniper Identity Management Service" on page 39.

Configuring JIMS-to-CSO Authentication Credentials

Configuring authentication credentials allows Juniper Identity Management Service to connect automatically to CSO to make requests for authentication information to synchronize individual users and user group updates. These are the credentials that the HTTPS server on CSO uses to authenticate incoming connections from the JIMS server.

To configure user authentication credentials for a JIMS-to-CSO configuration:

1. Using a Web browser, access the URL for the CSO Customer Portal.

   > **NOTE**: We recommend that you use Google Chrome Version 60 or later to access the CSO Customer Portal.

2. Select **Administration > Identity Management** to access the Identity Management page from the CSO Customer Portal.

3. Click **JIMS-to–CSO Configuration** to access that section of the Identity Management page. The username ID is randomly generated. You cannot change it. You will, however, need to specify a password.

4. In the Password field, enter the password associated with the new user that has the automatically generated user ID. The password must contain one number, one uppercase letter, and one special character.

> **NOTE**: Once you specify a password and save it, you can modify the password by clicking **Change Password**.

5. Click **Save** to save the authentication credentials.

Configuring SRX-to-JIMS Settings

Configuring the SRX Series device to JIMS connection and authentication credentials allows the JIMS server to send IP address, username, and group relationship information to SRX Series devices used as a CPE device in a distributed deployment. You can also configure a set of optional advanced settings for authentication timeout, and IP address and domain filters.

Before you begin, you need the following information:

- The IP address of the JIMS server.

- The imported Certificate Authority (CA) certificate.

- The client ID to obtain an OAuth token from the JIMS server for user queries.

- The client secret to obtain an OAuth token from the JIMS server for user queries.

To configure the SRX-to-JIMS configuration:

1. Click **SRX-to-JIMS Configuration** to access that section of the Identity Management page.

2. In the Identity Servers section of **SRX-to-JIMS Configuration**, under Primary Server, enter the IP address of the primary JIMS server. CSO uses this IP address to contact the JIMS server.

3. Select the server CA certificate that the JIMS server is to use to authenticate with the SRX Series devices and ensure a secure data transfer. You specify one server certificate to authenticate communication with each SRX Series device in your network.

> **NOTE**: Certificates in CSO are populated from **CSO > Administration > Certificates > Import Certificate**.

If you are using a secondary JIMS server, under Secondary Server repeat steps 2 and 3 for the secondary JIMS server.

4. In the Client Credentials section of **SRX-to-JIMS Configuration**, enter the client ID and client secret that CSO requires to obtain an OAuth access token required for user queries.

    The client ID and client secret are required values. They must match the client ID and client secret that you configure later for this CSO platform from Juniper Identity Management Service.

5. In the Advanced Settings section of **SRX-to-JIMS Configuration**, if required, you can configure settings for authentication timeout and IP address and domain filters.

    a. In the Authentication Entry Timeout text field, configure the timeout interval in minutes after which idle entries in the authentication table on CSO expire. The timeout interval begins from when the user authentication entry is added to the authentication table. This value can be between 10 and 1440 minutes, where a value of 0 means no timeout. The default value is 1440 minutes.

    b. In the Filter section of **Advanced Settings**, you have a series of selections to define filtering. You can include or exclude a specific IP address. You also have the option to filter by domain.

6. When completed, click **Save** to save the identity management configuration settings for CSO.

7
CHAPTER

JIMS Client Configuration

JIMS Server Client Configuration Overview

After you prepare the SRX Series devices and CSO platform in your network, you configure the JIMS server to connect to SRX Series devices and CSO and perform related tasks to bring Juniper Identity Management Service to an operational state.

Perform the following tasks:

Configuring the Connection to an SRX Series Device

You can configure Juniper Identity Management Service to serve up to 1200 SRX Series devices.

Before you begin, you need the following information:

- Client ID that the SRX Series device needs to obtain an OAuth token from the JIMS server for user queries. This value must match the client ID configured on the SRX Series device.

- Client secret that the SRX Series devices needs to obtain an OAuth token from the JIMS server for user queries. This value must match the client secret configured on the SRX Series device.

- For an SRX Series device running Junos OS Release 12.3X48-D45 or later, you also need the username and password that the SRX Series device's HTTPS server uses to authenticate incoming connections.

To configure the connection to an SRX Series device:

1. In the navigation pane, select **Clients**. Click the **SRX Clients** tab.
2. In the upper SRX Configured Clients pane, click **Add**. The Add SRX Client Configuration page appears.

> **NOTE**: Values with a light blue background represent default values. These values can be overridden as needed.

3. If you have multiple SRX Series devices that can utilize the same client configuration, from the Templates list select one of the available templates to support the grouping of an SRX client configuration. See "Configuring SRX Series Device Templates" on page 58 for details on creating an SRX client configuration template.

4. Type the IP address of the SRX Series device.

   Starting in JIMS release 1.4.0, when configuring SRX, you can now provide IP address or network address of SRX Series device. You can provide subnet as CIDR or doted decimal format. For example, these are the network addresses 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/255.255.0.0, and so on. If you have multiple SRX Series devices in the same subnet, you can now group them using the subnet input field. If no value is given in the subnet field, the IP address will be treated as a host /32 or /128.

5. Type a description for the SRX Series device.

6. If your environment contains SRX Series devices running Junos OS Release 12.3X48-D45 or later, click the **WebAPI (Legacy)** check box, then click **Configure**. The JIMS to SRX Client Configuration dialog box appears.

> **NOTE**: By default, the JIMS server assumes connectivity to SRX Series devices running Junos OS Release 15.1X49-D100, 17.4R1, or a later release, and uses batch query mode to communicate with SRX Series devices. With batch query mode, the JIMS server sends reports in response to requests from the SRX Series device for batch reports. A batch report contains multiple records. The service also responds to individual queries for missing information with reports containing the requested information.

In the JIMS to SRX Client area of the dialog box, perform the following:

a. Type the username credential that the HTTPS or HTTP server on the SRX Series device uses to authenticate incoming connections.

b. Type the password credential that the HTTPS or HTTP server on the SRX Series device uses to authenticate incoming connections.

c. Type the maximum data rate in entries per second. This is the maximum number of entries (reports) allowed to be sent per second from Juniper Identity Management Service to the SRX Series device. The value can be between 1 and 1,000 entries per second. The default value is 200 entries per second.

d. The Filter check box for preventing device-only reports from being sent to the SRX Series device is selected by default. To enable sending device-only reports, clear the check box.

> **NOTE**: When creating a template, the Filter parameter uses a tri-state check box to allow an indeterminate state in addition to the two provided in the check box (checked and unchecked). This third state is shown as a black square in the check box, and indicates that its state is neither checked nor unchecked. In this case, the black square means that the value is not to be included in the template.

e. In the Protocol and Port on Client area, specify the port number on the SRX Series device to use for communication with the JIMS server.

To use the Secure port, click the **Use TLS** check box to select it and then type the port number in the **Secure Port** text field. This value must be a valid port number between 1024 and 65,535, and it must match the SRX WebAPI configuration. The default value for the Secure port is 8443.

> **NOTE**: When creating a template, the Use TLS parameter uses a tri-state check box to allow an indeterminate state in addition to the two provided in the check box (checked and unchecked). This third state is shown as a black square in the check box, and indicates that its state is neither checked nor unchecked. In this case, the black square means that the value is not to be included in the template.

To use the Debug (HTTP) port, leave the **Use TLS** check box unchecked and then type the port number in the **Debug (HTTP) Port** text field. This value must be a valid port number between 1024 and 65,535, and it must match the SRX WebAPI configuration. The default value for the Debug (HTTP) port is 8080.

> **NOTE**: For security considerations, we recommend that you specify a secure HTTPS port rather than an HTTP port. HTTP is supported primarily for debugging purposes.
>
> If you enable the Debug (HTTP) port and change the port value, ensure that the corresponding port configuration on the SRX Series devices is modified to match this setting.

f. Click **OK** to save the JIMS to SRX Client settings.

7. To allow IPv6-related report information to pass from the JIMS server to SRX Series devices, click the **Enable** check box. Leave the check box unchecked if you do not want IPv6-related report information to pass to SRX Series devices.

Starting in Junos OS Release 18.1R1, the IPv6 Enabled checkbox can be turned **ON** in JIMS server to support IPv6 addresses if they are utilized. SRX Series devices can search the identity management authentication table for information based on IPv6 addresses. Prior to Junos OS Release 18.1R1, the client configuration IPv6 Enable checkbox on JIMS server is **OFF** by default for maximal

compatibility, as it filters all IPv6 addresses to the target. SRX Series devices read only IPv4 addresses. Starting in Junos OS Release 18.1R1 and later, SRX Series device supports the use of IPv6 addresses associated with source identities in security policies. If an IPv4 or IPv6 entry exists, policies matching that entry are applied to the traffic and access is either allowed or denied.

> **NOTE**: When creating a template, the IPv6 Reporting Enable parameter uses a tri-state check box to allow an indeterminate state in addition to the two provided in the check box (checked and unchecked). This third state is shown as a black square in the check box, and indicates that its state is neither checked nor unchecked. In this case, the black square means that the value is not to be included in the template.

8. In the SRX Client to JIMS area, do the following:

    a. Type the client ID that the JIMS server requires from the SRX Series device in the request to obtain an OAuth access token. This value must match the client ID configured on the SRX Series device.

    b. Type the client secret that the JIMS server requires from the SRX Series device in the request to obtain an OAuth access token. This value must match the client secret configured on the SRX Series device.

    c. In the Token Lifetime text field, type the token lifetime period for OAuth access tokens, which can be between 60 and 36,000 seconds. The default value is 1,200 seconds.

9. Click **OK** to save the settings.

Configuring SRX Series Device Templates

IN THIS SECTION

- Creating an SRX Series Device Template | **59**
- Modifying an SRX Series Device Template | **60**
- Selecting a Template for Configuring SRX Clients | **61**

Support for Configuring SRX Series Device Templates is supported in Juniper Identity Management Service Release 1.1 and later.

You can develop one or more templates in Juniper Identity Management Service to support the grouping of client configurations to facilitate the configuration of multiple SRX Series devices. A template is a way to share common configuration attributes across items within a homogeneous collection without having to re-enter those attributes for each configuration instance. Templates allow configurations to share common data.

A template provides default settings that can be referenced to create an instance. A special ID provides a single reference that is utilized by multiple configuration items within a type of collection (for example, SRX Series clients).

For example, you can specify a username and password in a template, and assign that template across all SRX Series devices that require the same login credentials. Utilizing a template allows you to copy the configuration and only re-enter the password for the specific template.

Note the following considerations when using templates:

- The IP address or server name is not included in the template since they would not be common across multiple items.

- It is not necessary that a template contain all attributes; the design works with a subset of attributes, such that the attributes not provided in the template will need to be provided in the configuration that utilizes the template.

NOTE: A template cannot be later applied to an SRX Series client that has been created without a template. The fields in the template will not override the original fields configured for the SRX Series client without a template. If you want to use the template fields, delete the original fields configured for an SRX Series client.

This section includes the following topics:

Creating an SRX Series Device Template

To create an SRX Series device template:

1. In the navigation pane, select **Clients**. Click the **SRX Clients** tab.
2. In the SRX Configured Templates pane (bottom pane), click **Add**. The Add SRX Template Configuration dialog box appears.

   If you want to pre-populate the template information in the Add SRX Template Configuration dialog box with attributes from an existing template, click an existing template in the SRX Configured Templates list to select it, and then hold down the **Shift** key while pressing **Add**. The attribute values

from the selected template appear in the Add SRX Template Configuration dialog box with a yellow background. You will need to enter a name for this new template.

3. Complete the SRX Series device configuration as described in "Configuring the Connection to an SRX Series Device" on page 55.

> **NOTE**: If a template name is already in use in the JIMS server, the background will turn red. If the name is unique, the background will turn green.

Note the following about templates:

- Template fields can be left blank. In this case, the field will need to be defined in the client configuration utilizing the template.

- Check box buttons display a black box if that check box is unused. This behavior is valid for templates if you do not want to specify a default value.

- Once a template has been created with a specific name, that name cannot be modified. The Edit SRX Template Configuration page will display the name as a read-only text field.

- If you want to delete a template, ensure sure that the template is no longer in use before you delete it. You will receive an error from the JIMS server if you attempt to delete a template that is still in use.

4. Click **OK** to save the settings. The new template appears in the SRX Configured Templates list.

Modifying an SRX Series Device Template

To modify an SRX Series device template:

> **NOTE**: Modifying an SRX Series device template also changes the clients that use the template.

1. In the navigation pane, select **Clients**. Click the **SRX Clients** tab.
2. In the SRX Configured Templates pane (bottom pane), click **Edit**. The Edit SRX Template Configuration page appears.

   The attribute values from the selected template appear in the Edit SRX Template Configuration dialog box with a yellow background. If it is a default value, the value appears with a blue background.

3. Modify the SRX Series device configuration as described in "Configuring the Connection to an SRX Series Device" on page 55.

> **NOTE**: Once a template has been created with a specific name, that name cannot be modified. The Edit SRX Template Configuration page will display the name as a read-only text field.

4. Click **OK** to save the settings. The modified template appears in the SRX Configured Templates list.

Selecting a Template for Configuring SRX Clients

To select a template for the configuration of multiple SRX clients:

1. In the navigation pane, select **Clients**. Click the **SRX Clients** tab.
2. In the SRX Configured Clients pane (top pane), click **Add**. The Add SRX Client Configuration dialog box appears.
3. Select an existing template from the Template drop-down list. You can either keep the template values or make modifications.
4. To make modifications to the values from the selected template, see "Configuring the Connection to an SRX Series Device" on page 55.

> **NOTE**: Values with a light blue background represent default values. These values can be overridden as needed.

5. Click **OK** to save the settings. The selected template appears in the SRX Configured Client list.

Configuring the Connection to a CSO Client

Support for Configuring the Connection to a CSO Client is supported in Juniper Identity Management Service Release 1.1 and later.

If your network environment uses Contrail Service Orchestration (CSO), you can configure Juniper Identity Management Service to serve up to 10 CSO platforms. CSO must be running Release 3.3 or a later release.

Configuring a CSO client allows the JIMS server to establish a secure link with CSO. This link is used to push the data that the JIMS server has collected about users and groups within a set of domains to CSO. This data allows administrators using CSO to make policy decisions that can be applied to a set of SRX Series devices that are handling the user firewall policy duties for that same set of domains.

> **NOTE**: The JIMS server provides real-time updates about user sessions (mapping users to IP addresses and devices) to the SRX Series devices simultaneously and independently from CSO. The JIMS server and CSO work together to help improve the policy handling and enforcement on the SRX user firewall.

Before you begin, you need the username and password that the CSO HTTPS server uses to authenticate incoming connections.

To configure the connection to CSO:

1. In the navigation pane, select **Clients**. Click the **Identity Clients** tab.
2. In the upper Contrail Service Orchestration (CSO) Configured Clients pane, click **Add**. The Add Identity Client Configuration page appears.

> **NOTE**: Values with a light blue background represent default values. These values can be overridden as needed.

3. Identity Client IP/Hostname text field, enter the hostname or IP address of the CSO platform.
4. Type a description for the CSO.
5. Type the username and password credentials that the HTTPS server on CSO uses to authenticate incoming connections.
6. Click **OK** to save the settings.

Configuring IP Address Filters

Juniper Identity Management Service enables you to specify IP address ranges to include in or exclude from the reports the JIMS server sends to the SRX Series devices. For SRX Series devices running Junos OS Release Junos OS Release 15.1X49-D100, 17.4R1, or a later release, you can apply an IPv4 address filter. For SRX Series devices running Junos OS Release 18.3R1 or later, the JIMS server supports both IPv4 and IPv6 address filtering for the SRX Series devices in your network.

Configuring an IP filter on Juniper Identity Management Service enables you to apply IPv4 and/or IPv6 filters to all the SRX Series devices in your network. You can set the IP filters to include the IP address ranges that the SRX Series devices require or exclude the ranges that they do not require when collecting user identity information.

You can also use an IP filter to include or exclude domain PCs or network servers, either within an IP address range or with a specific IP address.

> **NOTE**: Juniper Identity Management Service creates and maintains sessions for Active Directory domain controllers as well as domain PCs. This might result in the service attempting to send PC probes to the domain controllers. To avoid this behavior, add the IP addresses of the domain controllers as an excluded entry in the IP filter on Juniper Identity Management Service.

You can configure up to 64 include and exclude IP address ranges.

> **NOTE**: Include filters take precedence over exclude filters for IP address ranges.

To include or exclude an IPv4 address range for SRX Series devices:

1. In the navigation pane, select **Settings** and then select the **IP Filters** tab.
2. To include or exclude an IPv4 address range, in the IPv4 Event Filter area, click **Add**. The IP Configuration page appears.

   Do the following:

   a. Select the **Include** or **Exclude** option button.

   b. Type the IP address range start address and end address. To specify a single IPv4 address, type the same IP address for the IP address range start address and end address.

   c. Click **OK** to save the settings.
3. In the IPv6 event filter area, click **Add** to include or exclude an IPv6 address range for SRX Series devices running Junos OS Release 18.3R1 or later. The IP Configuration page appears.

   > **NOTE**: IPv6 filtering between the JIMS server and SRX Series devices is intended for support in a future Junos OS Release for SRX Series devices.

   Do the following:

   a. Select the **Include** or **Exclude** option button.

   b. Type the IP address range start address and end address. To specify a single IPv6 address, type the same IP address for the IP address range start address and end address.

   c. Click **OK** to save the settings.
4. Click **Save** to save the settings.

Configuring User/Device Event and Group Filters

Group filters on Juniper Identity Management Service enable you to apply filters to all the SRX Series devices in your network. You set the filter to list the specific Active Directory groups to include. You can configure up to 200 Active Directory groups to *include*. Note that a user can only be a member of a maximum of 200 groups because SRX Series devices do not support more than 200 groups per user.

User/Device Event filters on Juniper Identity Management Service enable you to apply a filter in your network to define users or devices to *exclude* from the reports that the JIMS server sends to SRX Series devices. The user filter performs regular expression matching to filter specific users or devices by name. The filter ignores events associated with a particular user or device. You can configure up to 64 users or devices to exclude.

> **NOTE**: The User/Device Event filter uses a regular expression to perform a match, unlike the SRX Group filter which uses a string match. Unfortunately, the JIMS UI does not clarify this difference in the Event/Group Filters tab. For example, entering a name ("user1") would match a prefix (also matching "user11", "user112", and so on). To enter a full string, add a dollar sign suffix ("user1$") to the filter.

To configure an SRX group filter:

1. In the navigation pane, select **Settings** and then select the **Event/Group Filters** tab.
2. To add a filter to include an Active Directory group, in the SRX Group Filter area, click **Add**. The Active Directory Groups page appears.
3. Do the following:

   a. Enter the name of the Active Directory group.

   b. Select the **Any** option button to include a group from any domain, or select the **Specify** option button and specify a domain from the list.

   c. Click **OK** to save the settings.
4. Click **Save** to save the SRX group filter setting.

To configure a User/Device Event filter:

1. In the navigation pane, select **Settings** and then select the **Event/Group Filters** tab.

2. To add a user or device filter to exclude, in the User/Device Event Filter area, click **Add**. The User/Device Event Filter page appears.

3. Do the following:

a. Enter the name of the user or device.

> **NOTE**: Filters are case-insensitive ECMAscript style regular expressions.

b. Select the **Any** option button to exclude a user or device from any domain, or select the **Specify** option button and specify a domain from the list.

c. Click **OK** to save the settings.

4. Click **Save** to save the User/Device Event filter settings.

Configuring JIMS Identity Server

Starting in JIMS release 1.3, a new component, JIMS Identity Server provides an interface between user firewall functionality on SRX Series device and JIMS. From this release forward, we will refer to the existing JIMS service as Classic JIMS. JIMS Identity Server allows SRX Series device to validate domains, groups, users, and devices using Junos OS command-line interface (CLI). JIMS Identity Server runs as an independent process from the Classic JIMS. JIMS Identity Server continues to respond to the policy validation requests from SRX Series device even if the connection to the JIMS is down.

From this release, JIMS Identity Server is the default identity client. By default, JIMS Identity Server uses port 591 for SRX Series device validation requests and port 8008 to connect with Classic JIMS.

At the time of installation or upgrade to JIMS 1.3, if one of the ports for JIMS Identity Server is not available, the installer prompts you to enter non-conflicting ports. At this point, you can either remove the competing service that is using those port(s) or change the remote side (CSO or SRX Series device) configuration port arguments to install.

See *Configure Juniper Identity Management Service to Obtain User Identity Information* for the Junos CLI configuration to configure JIMS Identity Server.

Distinguished Name (DN) Filter for Active directory

Starting in JIMS release 1.3, you can configure JIMS to exclude an entire domain using Distinguished Name (DN) exclusion filter. DN filter includes a list of regular expressions. DN filter applies these regular expressions on the ingress of user information from Active Directory (AD). When JIMS reads any DN from the Active Directory and matches the specified regular expression, JIMS discards the DN and does

not attempt to pursue or await further information about the DN. For example, if a group in domain1.net has a user in domain2.net, and regular expression in the DN filter is .*DC=domain2,DC=net, then JIMS does not attempt to contact an AD about a user in domain2. JIMS is not designed to query users in a universal and global group that JIMS is not directly connected to. Use DN filter to avoid these domains.

There are some side effects of using DN filter. If you are matching at the OU level using DN Filters, and you want to move a user from an OU that is not filtered to an OU that is filtered out, when you move the user, the cached user remains in the first group as the user update will be suppressed by the filter. Future group updates will drop the user from those groups. Restarting the JIMS service will reset the mapping. If you need to regularly filter on OUs and move users, contact Juniper Account Team.

After specifying the DN filter, you need to restart JIMS to let JIMS read all the user information and exclude the domains in the DN filter.

Navigate to **Settings**>**DN Filters** and follow the steps to add, delete, or edit the **DN Filters** regular expression such as .*DC=Domain, DC=com.* :

- To add a DN regular expression in the **DN Filters** area, click **Add**. The Distinguished Name Filter page appears. Enter the regular expression and click **OK**.

- To edit an existing regular expression, select the DN in the list and click **Edit**. The Distinguished Name Filter page appears. Edit the DN regular expression and click **OK**.

- To delete a DN regular expression in the Distinguished Name Filter area, click **Delete**.

Full UPN User Name Support

Starting in JIMS release 1.3, SRX Series devices can get the User Principle Name (UPN) from JIMS using **Pass UPN**. JIMS receives the UPN from Active Directory User Info. The UPN matches the Microsoft Windows security events, syslog, and SRX Series device logins through the captive portal.

By default, JIMS continues to pass the full domain name and sAMAccountName to the SRX Series device and other clients such as CSO. When you select the new option **Pass UPN**, JIMS sends the domain name and includes the full UPN into the username field to the clients, if available. For example, user queries that intend to match usernames now need to match the long form domain \upnprefix@upnsuffix. Now you can use Contrail Service Orchestration (CSO) using **Pass UPN** as SRX Series device reports the username that contains the full UPN.

JIMS does not pass UPN properly when you enable **Pass UPN** in the Windows AD and there are two conflicting users such as jims-dom1.local\user1 has UPN user2@jims-dom1.local and jims-dom1.local \user2 has UPN user1@jims-dom1.local.

Navigate to **Settings**>**General**>**Global Configuration** and select the **Pass UPN (requires JIMS restart)** checkbox to enable this new feature. After selecting the **Pass UPN (requires JIMS restart)** checkbox, you need to restart JIMS to reset and update the state of SRX Series devices and other clients.

8
CHAPTER

JIMS Data Source Configuration

JIMS Server Data Source Configuration Overview

Juniper Identity Management Service provides a scalable service that can take over user identity data collection from Microsoft Active Directories, domain controllers, and Exchange servers, serving as a single, centralized data collection source

After you prepare the data sources in your network, you configure the JIMS server to connect to the data sources and perform related tasks to bring Juniper Identity Management Service to an operational state.

Perform the following tasks:

Configuring the Connection to an Active Directory

You can configure up to 100 Microsoft Active Directories as user information sources for Juniper Identity Management Service.

Before you being, you need the following information:

- The hostname or IP address of the Active Directory

- The username and password that you configured for the limited permission user account for Active Directories

> **NOTE**: If you delete an Active Directory from the JIMS server, the corresponding users and groups will continue to appear in the CSO UI for an additional period of time (approximately two hours). Those users and groups will eventually be removed from the CSO UI.
>
> The users and groups associated with the deleted Active Directory will not be removed until you restart the JIMS server.

To configure a connection to an Active Directory:

1. In the navigation pane, select **Data Sources** and then select the **Info Sources** tab.

2. In the upper Active Directory Sources pane, click **Add**. The Add Active Directory Configuration page appears.

3. If you can utilize the same Active Directory source configuration on multiple data sources, from Templates list select from one of the available templates to support the grouping of an information source configuration. See "Configuring Data Source Templates" on page 76 for details on creating a data source template.

4. In the Add Active Directory Configuration page, do the following:

   a. Type a description of the Active Directory.

   b. Type the hostname or IPv4 address of the Microsoft Active Directory.

   c. Type the username credential (Login ID) for Juniper Identity Management Service to use to authenticate with the Active Directory. This is the username credential that you configured for the limited permission user account for Active Directories.

   d. Type the password credential for Juniper Identity Management Service to use to authenticate with the Active Directory. This is the password credential that you configured for the limited permission user account for Active Directories.

   e. Keep the **Yes** option button selected to specify that the JIMS server uses a Secure Sockets Layer (SSL) connection to communicate with the Active Directory. The default setting is **Yes**. If you select the **No** option button, the JIMS server uses an Active Directory Service Interfaces (ADSI) connection between it and the Active Directory.

   > **NOTE**: The ADSI connection is not encrypted. This option is not recommended.

5. To edit the info source, hold down the **control** key and click the **Edit**, or hold down the **control** key and double-click the entry that you want to edit. You will see the deltas with a white background until you save it.

6. Click **OK** to save the settings.

RELATED DOCUMENTATION

Verifying Connectivity to Active Directories | 97

Configuring the Connection to an Event Log Source

An event log source can be a Microsoft Active Directory domain controller or a Microsoft Exchange server. You can configure up to 100 event log sources for Juniper Identity Management Service that can be a combination of Microsoft Active Directory domain controllers and Exchange servers.

Before you begin, you need the following information:

- The hostname or IP address of the Active Directory domain controller or Exchange server

- The username and password that you configured for the limited permission user account for event log sources

> **NOTE**: Juniper Identity Management Service uses the event log timestamp to decide the order of events, and, therefore, you might experience unexpected side issues if your domain controllers and Active Directories are not synchronized. This is more likely to happen across domains than within domains, which typically time-synchronize with their domain controller. Juniper Identity Management Service uses UTC (GMT) internally, and the time zone should not matter, only the time synchronization. See the Windows Time Service Tools and Settings documentation for Windows Server 2016 or 2012 R2.

To configure the connection to an event log source:

1. In the navigation pane, select **Data Sources** and then select the **Event Sources** tab.
2. In the upper Event Source Configured Data Source pane, click **Add**. The Add Event Source Configuration page appears.
3. If you can utilize the same event source configuration on multiple data sources, from Templates list select from one of the available templates to support the grouping of an event source configuration.
4. In the Add Event Source Configuration page, do the following:

   a. Select either **Domain Controller** or **Exchange Server** from the drop-down list to specify the source type.

   b. Type a description of the source.

   c. Type the hostname or IPv4 address of the Active Directory domain controller or Exchange server.

   d. Type the username credential (Login ID) for Juniper Identity Management Service to use to authenticate with the event log source. This is the username credential that you configured for the limited permission user account for event log sources.

e. Type the password credential for Juniper Identity Management Service to use to authenticate with the event log source. This is the password credential that you configured for the limited permission user account for event log sources.

f. In the Startup Event History Catchup Time text field, type a time period in hours that the JIMS server goes back after a restart and begins collecting event log information from the sources. This value can be between 1 and 10 hours. The default value is 1 hour.

5. Click **OK** to save the settings.

Configuring Administrative Credentials for Domain PC Probes

When Juniper Identity Management Service initiates a domain PC probe of a device in a customer's domain, it needs administrative credentials to gain access to the device. You can configure administrative credentials for up to 10 domain PC probes. For a PC probe to a new IP address, Juniper Identity Management Service tries each set of configured credentials in the order in which they appear in the list.

> **NOTE**: The JIMS server performs a reverse lookup of a domain PC probe to increase performance. When a domain PC probe has administrative credentials in the form username@domain, the JIMS server attempts a reverse lookup by IP address to calculate the Kerberos authenticator name, and will use the same path (for example, \\hostname.domain \ROOT\CIMV2). The JIMS server also uses NTLMLDOMAIN style authority and will not perform a reverse lookup if a domain PC probe has domain\username specified in the credentials.

Before you begin, you need the administrator's username and password that you configured for the limited permission user account for PC probes.

> **NOTE**: Administrative credentials for a PC probe are not domain-specific.

To configure administrative credentials for a domain PC probe:

1. In the navigation pane, select **Data Sources** and then select the **PC Probe** tab.

2. Click **Add**. The PC Probe Configuration page appears.

3. Do the following:

   a. Type a description of the PC probe credentials.

   b. Type the administrator's username credential (Login ID) in the format *username@fqdn*. This is the username credential that you configured for the limited permission user account for PC probes.

   c. Type the administrator's password credential for the domain PC probe. This is the password credential that you configured for the limited permission user account for PC probes.

4. Click **OK**.

   The username (Login ID) and description of the configured set of credentials appears in the PC Probe list. Each added set of credentials appears after the currently selected item in the list. If no item is selected, the set of credentials appears at the bottom of the list.

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

6. To change the order in which a set of credentials appears in the list, select an entry and click the **Up** or **Down** button, and then click the **Save** button. Click the **Cancel** button to change back to the previous order before saving.

RELATED DOCUMENTATION

Verifying Domain PC Probing | **100**

Domain Alias

IN THIS SECTION

- Domain Alias Overview | **74**
- Configure Domain Aliases | **74**

In JIMS, you can create an alias for the JIMS Active Directory domain names. Domain aliases enable you to assign different domain names to your primary domain name.

Domain Alias Overview

An Active Directory forest is the top most logical container in JIMS Active Directory configuration that contains domains, users, and group policies. The domain name is the string appended to hostnames that are not fully qualified. The domain name is the name of a network associated with an organization. For sites in the United States, domain names typically take the form of org-name.org-type. JIMS creates a domain object for each Active Directory forest it connects. The domain object maintains a list of outstanding devices and users.

JIMS maps the domain names to the domain object by mapping the long name (juniper.net) and the short name (juniper) to reference the same domain object.

User Principal Name (UPN) is the name of a user in an e-mail address format. The UPN format is based on Internet RFC 822: Standard for the Format of ARPA Internet Text Messages. In the e-mail address, the UPN is the user account name (UPN prefix) followed by the @ (at sign) and by the DNS domain name (UPN suffix) with which the user is associated. UPN is used to log on to a domain network. The UPN suffix can be the DNS name of any domain in the Active Directory forest or it can be an alternative domain name. The alternative domain name need not be a valid DNS name.

By using the domain aliases, JIMS adds the UPN suffixes as entries to the map.

Benefits

Eliminates the need to manage multiple addresses for a single user using domain alias.

Configure Domain Aliases

Before you begin, you need to configure the connection to an Active Directory. To configure the connection to an Active Directory, see Configuring the Connection to an Active Directory.

To configure domain aliases:

1. In the navigation pane, select **Data Sources** and then select the **Info Sources** tab.

2. In the upper Active Directory Sources pane, hold down the **control** key and click **Add**. The Add Active Directory Configuration page appears.

3. Click the **Advanced** button. The Add Advanced Active Directory Configuration page appears.

4. Click **Add** button. The Domain Alias page appears. Enter a domain alias to associate with the Active Directory server. A domain alias refers to the domain name of the Active Directory.

5. You can edit or delete the added domain alias, as required, using the **Edit** or **Delete** buttons, respectively, on the Add Active Directory Configuration page.

    Restart the JIMS server when domain aliases are added or removed. Failure to do so can lead to inconsistent reports to the SRX Series devices.

6. Select the **Enable** check box to enable the forced domain aliases. Forced domain aliases are the other domain aliases that are not in the list of the domain object.

7. Select the **Disable UPN suffix aliasing** check box to disable the UPN suffix alias.

    We recommend that you do not o disable UPN suffix alias. Disabling the UPN suffix alias causes the JIMS server to ignore the UPN suffix list from the Active Directory while utilizing the additional aliases.

    If you select the **Disable UPN suffix aliasing** check box, you can continue to use the force list.

8. Click **OK** to save the settings. The modified Active Directory configuration appears in the configured list.

    If you modify the domain alias configuration and click **OK**, because of the changes made to the Active Directory configuration, the domain alias portion of the template is merged into the Active Directory configuration. Any subsequent changes to the template does not affect the domain alias configuration.

    After making modifications, if you want to revert the domain alias configuration back to the template, uncheck the **Enable** check box and click **OK**. JIMS reverts the Domain Alias configuration back to the entries from the template.

Configuring Data Source Templates

You can develop one or more templates in Juniper Identity Management Service to support the grouping of events or info source configurations. This grouping facilitates the configuration of a specific data source. A template is a way to share common configuration attributes across items within a homogeneous collection. You need not have to re-enter the attributes for each configuration instance. Templates allow configurations to share common data.

A template provides default setting references to create an instance. A special ID is a single reference that is utilized by multiple configuration items within a type of collection (for example, event source or info source).

For example, you can specify a login ID and password in a data source template (such as for event sources). Assign that template across all SRX Series devices that require the same login credentials. Utilizing a template allows you to copy the configuration and only re-enter the password for the specific template.

Configuration of PC probes in a data source template is not supported.

Consider the following while using templates:

- The IP address or server name is not included in the template.

- It is not necessary that a template contains all attributes. JIMS works with a subset of attributes. The attributes that are not included in the template must be provided in the configuration that utilizes the template.

The fields in the template does not override the original fields configured for the specific data source without a template. Clear the original fields configured for the data source if you want to use the template fields.

This section includes the following topics:

Creating a Data Source Template

To create a data source template for an event or info source configuration:

1. In the navigation pane, select **Data Sources**. Perform one of the following actions:

   - Click the **Event Sources** tab if you want to create an event data source template.

   - Click the **Info Sources** tab if you want to create an Active Directory data source template.

   - Click the **Syslog Sources** tab if you want to create a remote syslog server data source template.

2. In the Configured Templates pane (bottom pane), click **Add**. The Add Template Configuration dialog box appears.

   Cick an existing template in the configured templates list to pre-populate the template information in the **Add Template Configuration** dialog box with attributes. Hold down the **Shift** key while pressing **Add**. The attribute values from the selected template appear in the **Add Template Configuration** dialog box with a yellow background. You can enter a name for the new template.

3. Complete the configuration as described in one of the following topics:

   - "Configuring the Connection to an Event Log Source" on page 71

   - "Configuring the Connection to an Active Directory" on page 69

   - "Configuring JIMS to Receive Remote Syslog Messages" on page 79

   - "Domain Alias" on page 73

   As you are typing in a new template name, if the input matches a template name that is already in use in the JIMS server for the configuration, the background turns red. JIMS does not allow you to save the template.

   If the template name is unique, the background turns green. You can save the template.

   Note the following about templates:

   - Template fields can be left blank. In this case, the field needs to be defined in the client configuration utilizing the template.

   - Check box buttons display a black box if that check box is unused. This behavior is valid for templates if you do not want to specify a default value.

   - Once a template is created with a specific name, that name cannot be modified. The Edit Template Configuration page displays the name as a read-only text field.

   - If you want to delete a template, ensure that the template is no longer in use before you delete it. You receive an error from the JIMS server if you attempt to delete a template that is still in use.

4. Click **OK** to save the settings. The new template appears in the Configured Templates list.

Modifying a Data Source Template

To modify a data source template for an event or info source configuration:

1. In the navigation pane, select **Data Sources**. Perform one of the following actions:

    • Click the **Event Sources** tab if you want to modify an event data source template.

    • Click the **Info Sources** tab if you want to modify an Active Directory data source template.

    • Click the **Syslog Sources** tab if you want to modify a remote syslog server data source template.

2. In the Configured Templates pane (bottom pane), click **Edit**. The Edit Template Configuration page appears.

    The attribute values from the selected template appear in the Edit Template Configuration dialog box with a yellow background. If it is a default value, the value appears with a blue background.

    When you add Active Directory Template and subsequently edit an Active Directory configuration (non-Template), you see the Active Directory configuration attribute value with a white background until you save the configuration.

3. Modify the configuration as described in one of the following topics:

    • "Configuring the Connection to an Event Log Source" on page 71

    • "Configuring the Connection to an Active Directory" on page 69

    • "Configuring JIMS to Receive Remote Syslog Messages" on page 79

    • "Domain Alias" on page 73

4. Click **OK** to save the settings. The modified template appears in the Configured Templates list.

    If you modify the domain alias configuration and click **OK**, because of the changes made to the Active Directory configuration, the domain alias portion of the template is merged into the Active Directory configuration. Any subsequent changes to the template does not affect the domain alias configuration.

Selecting a Template for Configuring a Data Source

To select a template for the configuration of multiple data sources:

1. In the navigation pane, select **Data Sources**. Perform one of the following actions:

    • Click the **Event Sources** tab if you want to select a template an event data source.

    • Click the **Info Sources** tab if you want to select a template for an Active Directory data source.

- Click the **Syslog Sources** tab if you want to select a template for a remote syslog server data source.

2. In the Configured Sources pane (top pane), click **Add**. The Add Source Configuration page appears.

3. Select an existing template from the Template drop-down list. You can either keep the template values or make modifications.

    Once you override the domain aliases, the domain aliases in the template are not used. The aliases configured for the specific Active Directory takes precedence.

    If you do not use any domain aliases for one set of configurations, but still want to use the other template parameters (without change in the original template), you must duplicate the template with a new name and remove the old domain aliases from the new template.

4. To make modification to the values from the selected template, see one of the following topics:

    - "Configuring the Connection to an Event Log Source" on page 71

    - "Configuring the Connection to an Active Directory" on page 69

    - "Configuring JIMS to Receive Remote Syslog Messages" on page 79

    - "Domain Alias" on page 73

5. Click **OK** to save the settings. The selected template appears in the Configured Sources list.

Configuring JIMS to Receive Remote Syslog Messages

Juniper Identity Management Service supports the ability to receive remote system log (also called syslog) event data and user information data from an event source such as a DHCP server. The number of syslog sources is limited to 200. You define the IP address and port of the remote syslog server that the JIMS server permits a connect from the remote server. You configure the JIMS server to collect syslog data whenever it detects the occurrence of begin session events, end session events, per session group mask events, create and begin session events, create user or device only events, modify user or device groups session events from the remote server session.

The JIMS server collects data from syslog messages containing username, device name, domain, groups, and/or IP address mappings, and turns those messages into entries in its cache. The JIMS server transmits this information to each SRX Series device for it to use in making policy decisions in the user firewall feature.

The JIMS server uses the following default ports to support the syslog server:

- Syslog UDP: UDP 514

- Syslog TCP: TCP 514

JIMS server do not open the windows firewall for UDP 514 and TCP 514 ports as they are commonly scanned ports. You must open the port manually to receive messages using the firewall mechanism that is currently installed. By default, windows firewall with Advanced Security is installed on windows.

If a port cannot be allocated on startup, the JIMS server writes errors to the log and sets the failure in the statistics status and continues to execute.

You can configure regular expressions (regex) to define a search pattern within one syslog message. After matching the source address, the JIMS server executes the regex associated with the particular connection, in the specified sequence order.

The JIMS server compares the trigger regex to an incoming syslog message. If the trigger regex matches to an incoming syslog message, JIMS attempts each attribute regex.

Before you begin, you need the hostname or IP address of the remote syslog server.

To configure JIMS to receive remote syslog messages:

1. In the navigation pane, select **Data Sources** and then select the **Syslog Sources** tab.
2. In the upper Syslog Configured Sources pane, click **Add**. The Syslog Server Configuration page appears.
3. In the Syslog Server Configuration box, do the following:

    a. Type the remote syslog server IP address.

    b. Type a description of the remote syslog server.

4. Click OK, and configure the remote syslog to send at least one type of (low-volume) syslog message. JIMS does not process these values until triggers are saved but lets you test your regex against incoming values. See step 6.
5. To parse the received syslog messages by using a regex to define a search pattern, click **Add**. The **Add Syslog Regular Expression Builder** dialog appears.

    You can configure a regex to define required data to collect from syslog messages that contain username, domain, group, and/or IP address mappings. Regexes compiles the resulting object cached in the JIMS server cache for processing. Syslog events tie together IP address information with user or device information (similar to that of an Event Log), and ties the user to a group list.

    To modify an existing regex, click the expression in the list and then click **Edit**.

    a. Type a description of the regex to be used.

    b. Specify the type of the regex processing.

    c. Specify which actions the trigger match tells the JIMS server to do:

    - **Begin Session**—Use **Begin Session** when you have the user or device in a Active Directory domain, or (in combination with **Create User/Device Only**, below) the user or device is sourced

from another syslog message. The message links the IP address to the existing user or device. This trigger requires IP address (IPv4 or IPv6) of the user, domain, and one of user name or device name. If the domain matches Active Directory domain, JIMS uses Active Directory domain user name or device name and return groups associated with it. If the domain matches a domain created by syslog **Create User/Device Only** trigger, JIMS begins that session and return the groups created by **Create User/Device Only** with it.

- **End Session**—Logoff whichever user is on a particular IP address. This trigger requires you to specify IP address (IPv4 or IPv6) of the user. If you specify both IPv4 and IPv6 addressees, JIMS ends two sessions, the user with IPv4 and the user with IPv6 address. The user entry or device entry for the IP address on SRX Series device is removed once the logoff message strike the **End Session** trigger.

- **Per Session Group Mask**—This trigger requires you to specify an IPv4 or IPv6 address of the session to update a set of user or device groups to be forced added or masked to/from the session. This trigger is typically used when you have usernames or devices in the Active Directory, but JIMS receive a message representing a transient state for the user.

  For modal groups security alerts – for example, if you receive a message that a device has an out of date antivirus, you should specify the triggers as:

  - First trigger: Uses forced to add the device into a group such as posture-unhealthy.

  - Second trigger: Detects that the problem is re-mediated and removes the device from group such as posture-unhealthy.

- **Create User/Device Only**—This trigger requires to you specify a domain name, user and user group names, and the device and device group names. JIMS does not associate an IP address with the user. This trigger is used when the user or device group information are sourced from a different syslog stream than the session stream.

- **Modify Groups by name**—This trigger requires you to specify a domain name, user with group names, and device with device group names to modify the groups for the named user or device. JIMS updates the groups for that user as appropriate if you specify domain and user, and user or device add groups, user or device remove groups.

- **Modify Groups by IP**—This trigger requires you to specify an IP address (IPv4 or IPv6) of the user, user with group names, and device with device group names to modify the groups for the named user or device. JIMS looksup the current user or device associated with the session, and modifies their groups if you specify IP address.

- **Create and Begin**—Use **Create and Begin** when the user or device data (that is groups) is sourced from the matched syslog message. This trigger requires user and user groups, device and device groups, or all of the four. This trigger creates a user or device, or updates an existing user or device with the specified groups. This trigger is mostly used when there is no Active Directory. Set the domain that matches either a device name or username. If a domain

is created by syslog, JIMS marks this domain as not active. Users in domains created by syslog never results in an Active Directory query, even if an Active Directory is added subsequently. JIMS creates two sessions if both IPv4 and IPv6 address are set.

d. Specify the regex that you want to use as a trigger to parse the received syslog messages. If the regex is marked as required and does not match, and there is no default, then the trigger fails. The regex processing continues to the next trigger. JIMS uses the default value if the attribute match of the regex is blank.

To match all incoming syslog messages, create a regular expression with .*. You can use this regular expression temporarily, with **Test** button, to verify all matched syslog messages. You can pick source_name and set that to (.*). This regular expression says - match whole syslog messages and assign it to a source_name. Then, click the **Test** button. JIMS gives you the first 10 syslog messages by default of the whole syslog messages that matchs the trigger. You can modify the **Return Count** value from 1 to 200 to test those many syslog messages that matchs the trigger.

If the source_name is configured and parsed, and it is from ClearPass, the syslog message in SRX Series device is displayed as **ClearPass**.

If source_name is not configured, the sylog message in SRX Series device is displayed as **JIMS - Syslog**. JIMS use the default value if the source_name matching fails. The syslog message in SRX Series device is displayed as **Unknown** if the source_name matching fails and the default value is null.

You can test the syslog messages that match the trigger from the current time to the required past time duration by:

*   Enabling the **Start time** check box.

*   Selecting the desired option from the drop-down list and enter the value mentioned below.

    Table 8 on page 82 contains the options from the drop-down list with range and default values.

    Table 8: Start-Time-Duration-Range-Default-Values

Duration	Range	Default
mins—Duration in minutes from which JIMS extracts the syslog massages from the current time to last specified value to test.	1 minute through 10,080 minutes	120 minutes
hours—Duration in hours from which JIMS extracts the syslog massages from the current time to last specified value to test.	1 hour through 168 hours	2 hours

Table 8: Start-Time-Duration-Range-Default-Values *(Continued)*

Duration	Range	Default
days—Duration in days from which JIMS extracts the syslog massages from the current time to last specified value to test.	1 day through 30 days	1 day

- Enter the required number of minutes, hours or days in the **last** field.

You can filter the trigger expressions of the syslog entries to test from the syslog server by enabling the **Match Server IP** check box. Enabling the **Match Server IP** check box ensures only syslog entries from the designated syslog server are tested against the trigger and regular expressions. You can test only one trigger at a time.

e. Click **Add** to create a regex that defines how to extract a specific attribute from the string. The Regex Attribute Editor appears. After the trigger regex is met, the JIMS server attempts to match the attribute regexes.

To modify an existing attribute expression, click the expression in the list and then click **Edit**.

- **Attribute**—Select from the list of attributes: devicegroups, devicename, domain, groups, IP, IPv4, IPv6, mac_address, session_device_forced_groups, session_device_masked_groups, session_user_forced_groups, session_user_masked_groups, source_name, timestamp, and username.

  - **Timestamp**—The default timestamp value is specified as **+/-<hours>**, which is added to the timestamp before being sent to the cache. You must use the default timestamp value when the remote syslog server is sending messages that reflect the localtime instead of Zulu or GMT time.

    In addition to the regular expression, timestamps take a format string instead of a default.

    - If the first character of the format is **+** or **-**, JIMS interpret the string as adding or subtracting some number of hours from the matched time. This is used when the syslog message contains local time instead of Zulu or GMT time.

    - To facilitate processing other date or time formats, the default can have a format string as specified in https://en.cppreference.com/w/cpp/io/manip/get_time. You can also add to match the regular expression to **get_time**, along with the format string, and utilize the output of that regular expression.

      Below are the few examples:

```
Timestamp in message :
```

```
2019-10-23T15:17:05.702+08:00.
RE: (\d{4}-\d\d-\d\dT\d\d:\d\d:\d\d\.\d+[+-]\d\d\:\d\d).
Format: %Y-%m-%dT%H:%M:%S
Output timestamp to SRX:2019-10-23T07:17:05.702000Z


Timestamp in message:
2019-10-23 16:09:39.555 +08:00.
RE: (\d{4}-\d\d-\d\d\s+\d\d:\d\d:\d\d\.\d+\s+[+-]\d\d\:\d\d).
Format: %Y-%m-%d %H:%M:%S
Output timestamp to SRX:2019-10-23T08:09:39.555000Z


Timestamp in message:
2019-10-24T14:42:39 IST.
RE: (\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d)\s+IST.
Format: -5.5%Y-%m-%dT%H:%M:%S
Output timestamp to SRX:2019-10-24T09:12:39.000000Z
```

JIMS supports the following additional formatting.

- .####—JIMS interpret this as deci-seconds, centi-seconds, milli-seconds, or micro-seconds, as appropriate (rounded to milli-seconds).

- +/-<hours>—Represent a time offset, such as +2.5. Representing 2 and a half hours ahead of GMT.

The above characters must match the above regular expression.

The string representations of time zone such as EST, PST, or GMT are ignored. To match these, you can utilize multiple regular expressions with the prefix pattern referenced above.

While replaying logs during JIMS server restart, the user firewall is transiently in a previous state before JIMS server reaches the end of the replay, by which time the current state is synchronized. Using the correct timestamp parsing in syslog session, creating and updating messages limits the practical effects, as older events are discarded.

Session attributes should have an IPv4 or IPv6 address set in the message to overwrites the user or device groups regardless of source. Forced groups are always added unless they conflict with the global group filter. Masked groups are always removed. Following are the attributes that are used to modify Active Directories users:

- session_user_forced_groups

- session_user_masked_groups

- session_device_forced_groups

- session_device_masked_groups

To match a list of groups, we support extending the regular expression used during group matching to include the following mechanism `<originalRE>!!!<subRE>`.

For example:

Regular expression: groups: ([^"]*)"!!!\|?([^|,]*)\|?\,?

This mean to take the value after groups: between the quotes, then serially run the regular expression \|?([^|,]*)\|?\,?—means, ignore 0 or 1 vertical bars, match all characters up to a comma, ignore 0 or 1 vertical bars and ignore the comma, then continue to do the same for the rest of the string.

This turn a list as `group1,|group2|,|group three|` into the following internal groups

`group1`

`group2`

`group three`

Group defaults are specified as comma separated. So, a default of `groupa,groupb,groupc` is handled as three separate groups.

Following attributes modify the internal syslog generated users. You must not use these attributes to modify Active Directory users:

- user_added_groups

- user_removed_groups

- device_added_groups

- device_removed_groups

- **Required for Trigger Match**—Click the check box if the selected attribute is required in the regular attribute expression. If the regex is marked as required and does not match, and there is no default, then the trigger fails. The regex processing continues to the next trigger. JIMS uses the default value if the attribute match of the regex is blank.

- **Expression**—Enter the expression in the Regular Expression field.

- **Default**—To modify the attribute value, enter a value in the Default text field.

Do not add additional characters in the regrex while you copy-pasting the regrex. A common occurrence is an incorrect space character or tab character, at the beginning or at the end of the regrex. If the regrex is not matching properly, highlight the entire string and verify the content.

Click **OK** to save the attribute expression as part of the regex.

f. Click **OK** to save the syslog regex.

6. Click **OK** to save the settings.

Use Case # 1: Configuring JIMS to Receive Remote Syslog Messages and Verifying the Syslog Messages from SRX Series Device

IN THIS SECTION

This configuration example provides step-by-step instructions on receiving the ClearPass messages on Juniper Identity Management Service, how to configure the Juniper Identity Management Service to receive and parse ClearPass syslog messages, and verifying syslog messages on SRX Series device.

Requirements

This example uses the following hardware and software components:

- SRX5600 Series device running Junos OS Release 18.3R3 or later.

- SRX5600 Series device must be configured as a client.

- Syslog source: ClearPass on C3000V platform, IP address: 192.0.2.1

- Juniper Identity Management Service, Release 1.2.0 or later

Overview and Topology

Juniper Identity Management Service support the ability to receive remote system log (also called syslog) event and user information data from an event source such as a ClearPass server. JIMS uses port 514 for both tcp and udp to receive syslog messages. JIMS server collects data from syslog messages and transmits the information to each SRX Series device for it to use in making policy decisions in the user firewall.

Figure 2: Juniper Identity Management Service Syslog Configuration
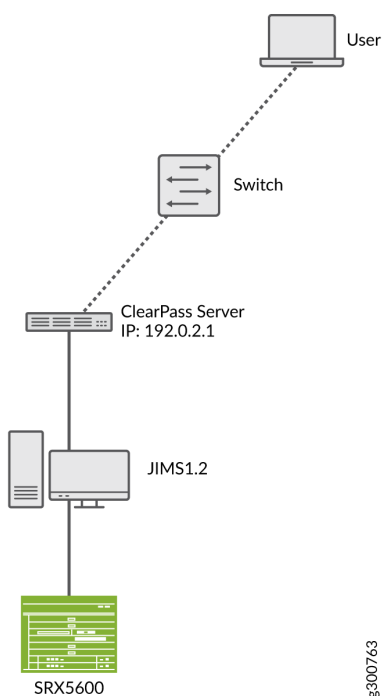
Logon and Logoff messages from ClearPass Server to Juniper Identity Management Service

```
ClearPass server sends the below logon message to Juniper Identity Management Service when user
logon:
<143>Nov 11 2019 10:56:49.567 CST 10.208.164.25 LEEF:1.0|Aruba Networks|ClearPass|6.7.0.101814|
3009|messageId=189694-1-0    Auth.Roles=[Employee]|[Guest]|[User Authenticated]
Radius.Username=test3529    Endpoint.Roles=[Employee]|[Guest]|[User Authenticated]
Endpoint.Username=test3529    Endpoint.Hostname=huashengmi    Endpoint.IP-Address=60.0.13.201
Endpoint.MAC-Address=5f823c000dc9    Endpoint.System-Posture-Token=UNKNOWN
src=10.208.164.25    devTimeFormat=MMM dd yyyy HH:mm:ss.SSS z    cat=Insight Logs
```

```
ClearPass server sends the below logoff message to Juniper Identity Management Service when user
logoff:
<143>Nov 11 2019 13:33:32.840 CST 10.208.164.25 LEEF:1.0|Aruba Networks|ClearPass|6.7.0.101814|
3006|messageId=793838-1-0    RADIUS.Acct-Username=test3529    RADIUS.Acct-Framed-IP-
Address=60.0.13.201    RADIUS.Acct-Timestamp=2019-11-11 13:33:13.325+08    RADIUS.Acct-Status-
Type=Stop    Common.Roles=[Employee], [Guest], [User Authenticated]    RADIUS.Auth-
Source=Local:localhost    src=10.208.164.25    devTimeFormat=MMM dd yyyy HH:mm:ss.SSS z
cat=Session Logs
```

For more information on ClearPass configuration, see ClearPass Configuration Manual

Configuration

IN THIS SECTION

- Configure Juniper Identity Management Service to Receive and Parse ClearPass Syslog Messages | 88

Configure Juniper Identity Management Service to Receive and Parse ClearPass Syslog Messages

Step-by-Step Procedure

The tasks required to configure Juniper Identity Management Service include:

1. In the navigation pane, select **Data Sources** and then select the **Syslog Sources** tab.

2. In the upper Syslog Configured Sources pane, click **Add**. The Syslog Server Configuration page appears.

3. In the Syslog Server Configuration box, type the remote syslog server IP address as 192.0.2.1

4. Click **Add** to parse the received syslog messages by using a regex to define a search pattern. The **Add Syslog Regular Expression Builder** dialog appears.

5. Define the syslog regex for this source for logon messages:

   - Specify the type of the regex processing.as **Create and Begin**

   - Specify which actions the trigger match will tell the JIMS server to do as **.*Endpoint.IP-Address=.***

- To create a regex that defines how to extract a specific attribute from the string, click **Add**. The **Regex Attribute Editor** appears. Specify the attributes as:

  - IP-address: Endpoint.IP-Address=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})

  - username: Endpoint.Username=([^]+?)\t

  - groups: Auth.Roles=(\[.*\])!!!\[(.*?)\]

  - domain: default: cppm.com

  - devicename: Endpoint.Hostname=([^]+?)\t

  - devicegroups:Endpoint.Roles=(\[.*\])!!!\[(.*?)\]

  - timestamp: <.+>(.*)\s+CST format: -8%b %d %Y %H:%M:%S

6. Repeat step 4 to define the syslog regex for this source for logoff messages:

  - Specify the type of the regex processing.as **End Session**

  - Specify which actions the trigger match will tell the JIMS server to do as **.*RADIUS.Acct-Status-Type=Stop.***

  - Click **Add** to create a regex that defines how to extract a specific attribute from the string. The **Regex Attribute Editor** appears. Specify the attributes as:

    - IP-Address: Acct-Framed-IP-Address=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\t

    - Timestamp: RADIUS.Acct-Timestamp=(\d{4}-\d{2}-\d{2}\s+\d{2}:\d{2}:\d{2}\.\d+[+-]\d\d) format: %Y-%m-%d %H:%M:%S

Verification

IN THIS SECTION

Verify the User or Device Entries are Generated Along with Logon Syslog Message on SRX5600 Series Device

Purpose

Verify the user or device entries are generated along with logon syslog message on SRX5600 Series device

Action

On the SRX5600 device, use the `show services user-identification authentication-table ip-address 60.0.13.201` CLI command.

```
user@host> show services user-identification authentication-table ip-address 60.0.13.201
node0:
--------------------------------------------------------------------------
Logical System: root-logical-system

Domain: cppm.com
  Source-ip: 60.0.13.201
    Username: test3529
    Groups:posture-healthy, employee, user authenticated, guest
    Groups referenced by policy:employee, user authenticated, guest
    State: Valid
    Source: JIMS - Syslog
    Access start date: 2019-11-11
    Access start time: 10:57:49
    Last updated timestamp: 2019-11-11 02:56:49
Age time: 0
```

On the SRX5600 device, use the `show services user-identification device-information table ip-address 60.0.13.201` CLI command.

```
user@host> show services user-identification device-information table ip-address 60.0.13.201
node0:
--------------------------------------------------------------------------
Domain: cppm.com
  Source IP: 60.0.13.201
    Device ID: huashengmi$
```

```
    Device-Groups: employee, guest, user authenticated
    Referred by: N/A
```

Meaning

The output displays that user and device entry are generated along with the logon message.

Verify the User or Device Entries are Removed Along with Logoff Syslog Message on SRX5600 Series Device

Purpose

Verify the user or device entries are removed along with logoff syslog message on SRX5600 Series device

Action

On the SRX5600 device, use the `show services user-identification authentication-table ip-address 60.0.13.201` CLI command.

```
user@host> show services user-identification authentication-table ip-address 60.0.13.201
node0:
------------------------------------------------------------------------
warning: "This IP address isn't in authentication table."
```

On the SRX5600 device, use the `show services user-identification device-information table ip-address 60.0.13.201` CLI command.

```
user@host> show services user-identification device-information table ip-address 60.0.13.201
node0:
------------------------------------------------------------------------
warning: "This IP address isn't in device-identity table."
```

Meaning

The output displays that SRX5600 Series device user and device entries are removed along with the logoff message.

RELATED DOCUMENTATION

9
CHAPTER

JIMS Configuration Verification
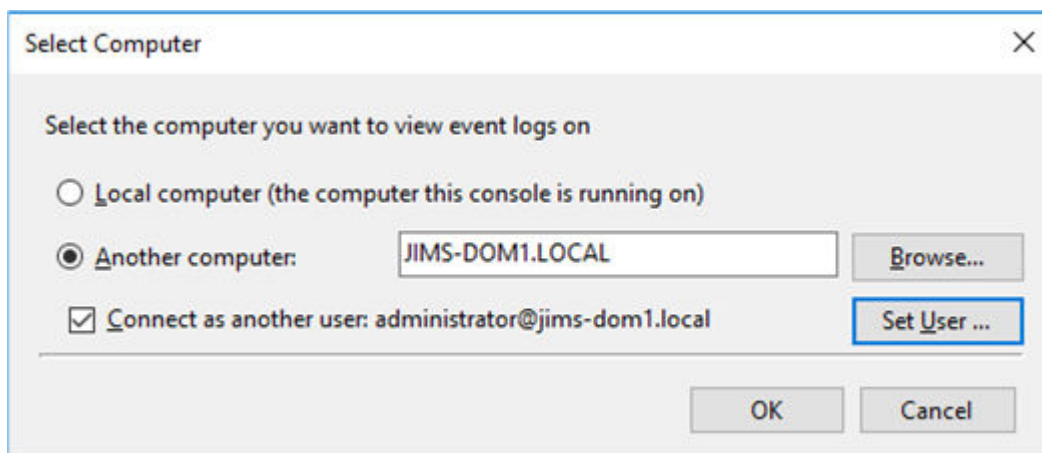
Verifying Connectivity to Event Log Sources

Before you begin, you need the following information:

- The hostname or IP address of the Active Directory domain controller or Exchange server that you want to verify connectivity with

- The username and password of a user on the server

To verify that the connections to event log sources are working properly:

1. From the Windows Start menu, click **Windows Administrative Tools** and from the list of tools, select **Event Viewer**.

2. On the Event Viewer page, select **Action > Connect to Another Computer**.

   The Select Computer page appears.

3. Make sure the option button for **Another Computer** is selected and type the hostname or IP address of the Active Directory domain controller or Exchange server that you want to verify connectivity with.

4. Select the check box for **Connect as another user**, and click **Set User**.

5. On the Select a user page, select a username, type a password, and click **OK**.

6. On the Select Computer page, click **OK**.

7. On the Event Viewer page, in the navigation frame, expand the Windows Logs folder and select **Security**.

   The Event Viewer window now shows the Security pane.
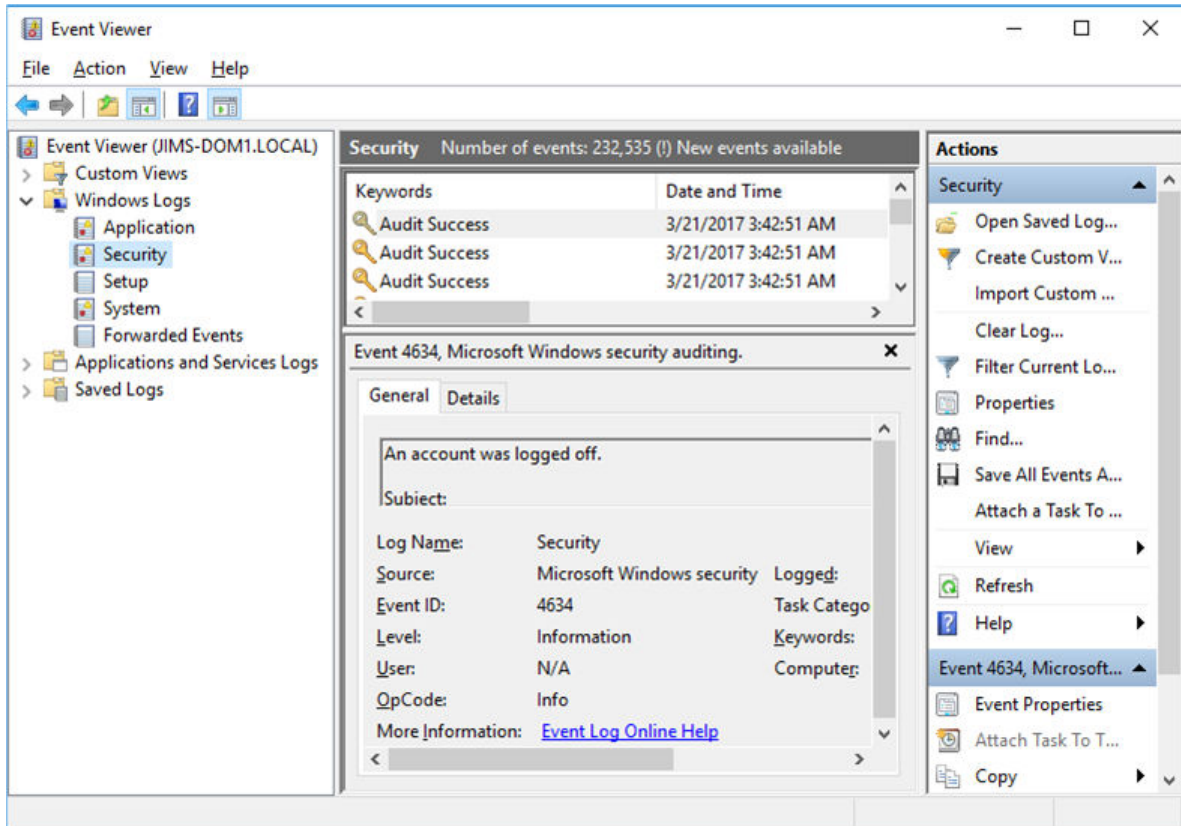
If you see security events, Juniper Identity Management Service is receiving this information as well. If you do not see security events, there is a credentials or connectivity issue or issue with security event logging. See "Troubleshooting the JIMS Event Sources" on page 96 to enable security event logging.

We monitor the logon events of a user when the user on a PC logs on to the domain controller. This happens periodically at the rate of the group policy refresh interval, which is configured by the group policy located at Computer Configuration\Administrative Templates\System\Group Policy and User Configuration\Administrative Templates\System\Group Policy.

RELATED DOCUMENTATION

Troubleshooting the JIMS Event Sources

If you see Juniper Identity Management Service not receiving the event log sources:

1. Check for correct credentials or connectivity issues.
2. If the credentials or connectivity is correct, check filter for the following events in the **Event Viewer** page on the domain controller:

    - Event Id logon (4624)

    - Event Id Kerberos authentication request (4768)

    - Event Id Kerberos service request (4769)

    - Event Id Kerberos service renewed (4770)

To enable the security event logging:

1. From the Windows Start menu, click **Windows Administrative Tools** and from the list of tools, select **Event Viewer**.

2. On the Event Viewer page, select **Action > Create Custom View**.

    The Create Custom View page appears.

3. On the Create Custom View page, select **Filter** tab.

4. On the Filter tab, select **Windows Logs > Security** from the drop-down list of event logs and type 4624, 4768, 4769, and 4770 separating with commas in the Includes/Excludes Event IDs text field.

5. On the Create Custom View page, click **OK** tab.

6. On the Event Viewer page, in the navigation frame, expand the Windows Logs folder and select **Security** to see the security events in the security pane.

    If you see security events, Juniper Identity Management Service is receiving this information as well

RELATED DOCUMENTATION

Configuring the Connection to an Event Log Source | **71**

Verifying Connectivity to Event Log Sources | **94**

Audit Kerberos Authentication Service

4624(S): An account was successfully logged on.

4768(S, F): A Kerberos authentication ticket (TGT) was requested.

> 4769(S, F): A Kerberos service ticket was requested.
>
> 4770(S): A Kerberos service ticket was renewed.

Verifying Connectivity to Active Directories

Before you begin, you need the following information:

- The hostname and port number of the Active Directory domain controller

- The username and password for the domain controller

You can verify that the connections to Active Directories are working properly using a Windows tool called Ldp.exe. Ldp.exe is a Lightweight Directory Access Protocol (LDAP) tool that enables you to connect to and bind with LDAP-compatible directories such as an Active Directory.

To verify connectivity to an Active Directory using Ldp.exe:

1. From a JIMS server or an Active Directory domain controller, open a command shell and type:

    Ldp.exe

    The Ldp GUI Tool page appears.

2. On the Ldp GUI Tool page, select **Connection > Connect**.

    The Connect page appears.
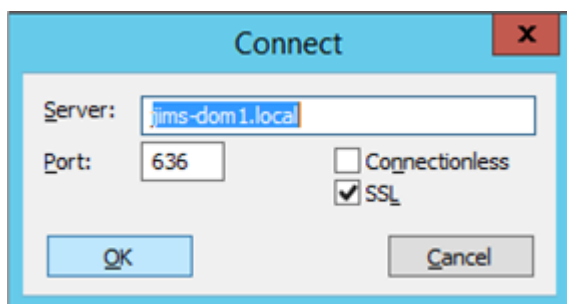
3. To connect with an Active Directory domain controller, enter the hostname of the domain controller, enter the port number, select the **SSL** check box, and click **OK**.

4. Select **Connection > Bind**.

    The Bind page appears.
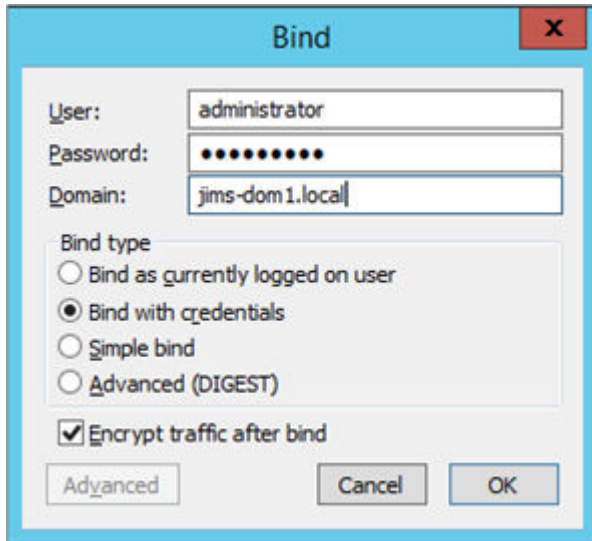
5. Type the username, password, and domain information and select the option button for **Bind with credentials** to bind with the credentials configured in Juniper Identity Management Service.

6. If this was successful (no errors were returned in the right-hand panel), select **View > Tree** from the Ldp GUI Tool page.

   The Tree View page appears.

7. Specify an empty Base Domain Name value (enter no value) and click **OK**.

   A page similar to the following appears:
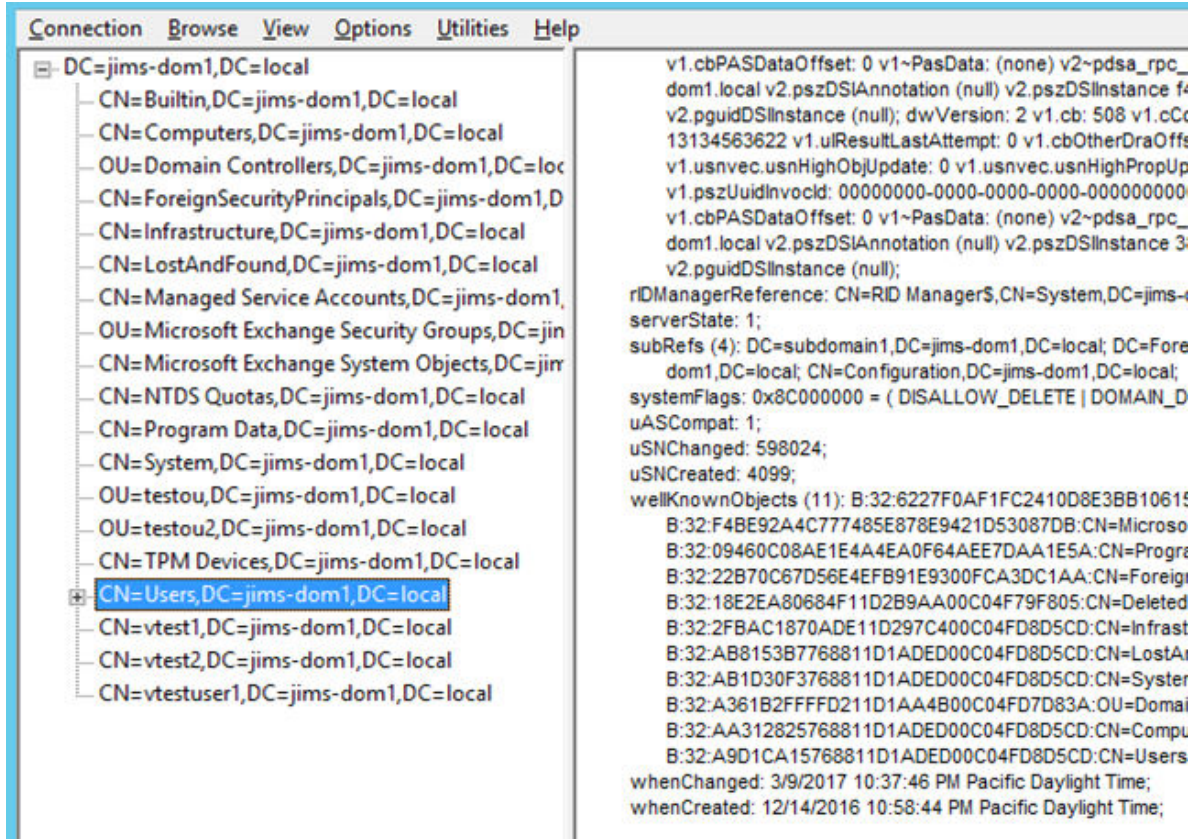
8. Double-click **CN=Users** (CN stands for Common Name) and then select a user.

   You should see output similar to the output in the lower-right of the window as shown in the following figure:

   If you can see the user information, Juniper Identity Management Service is receiving this information as well.

Verifying Domain PC Probing

Before you begin, you need the following information:

- The IP address of the domain PC

- The username for the domain PC in the format *user@domain* or *domain\user*

- The password for the domain PC

To verify that domain PC probing is working properly:
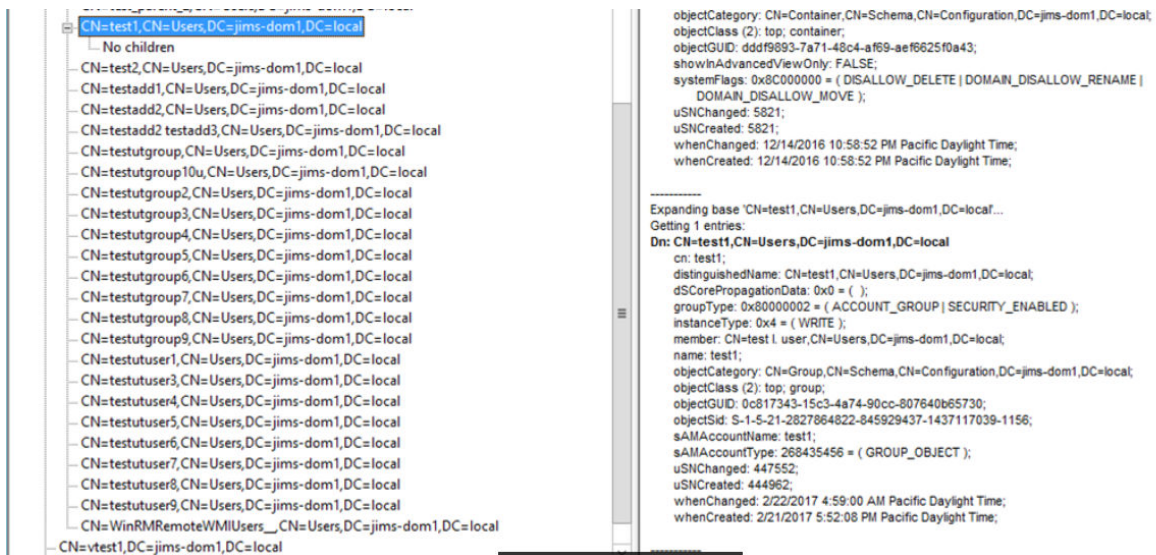
- Invoke the Windows Management Instrumentation Command-line (WMIC) and at the prompt, type:

  `C:\cic\v2\srv\products\cic\cwd>wmic /node:`*"client_ip_address"* `/user:`*"user@domain"* `/password:`*"password"*
  `computersystem get name`

  or

  `C:\cic\v2\srv\products\cic\cwd>wmic /node:`*"client_ip_address"* `/user:`*"domain\user"* `/password:`*"password"*
  `computersystem get name`

  `C:\cic\v2\srv\products\cic\cwd>wmic /node:`*"client_ip_address"* `/user:`*"user@domain"* `/password:`*"password"*
  `computersystem get username`

  or

  `C:\cic\v2\srv\products\cic\cwd>wmic /node:`*"client_ip_address"* `/user:`*"domain\user"* `/password:`*"password"*
  `computersystem get username`

  The command `computersystem get name` returns the machine name and `computersystem get username` returns the logged on user upon a successful PC probe

  If you get this result, the PC probe configured on Juniper Identity Management Service with the same credentials should work properly.

Verifying the User Query Connection from an SRX Series Device

Before you begin, you need the following information:

- The port number on the JIMS server for receiving HTTPS requests (by default, port 443)

- The client ID to obtain an OAuth token from the JIMS server for user queries

- The client secret to obtain an OAuth token from the JIMS server for user queries

To verify that the Web API connection and user queries and responses between the SRX Series device and Juniper Identity Management Service are working properly:

1. If there are no entries in the authentication table and the status of the Query State on Juniper Identity Management Service is Inactive, do the following:

   - Check if traffic is allowed between Juniper Identity Management Service and the SRX Series device on the configured port (by default, port 443).

   - Check the client ID and client secret for OAuth authentication configured on the SRX Series device and on Juniper Identity Management Service and verify that these values match.

   - Perform a packet capture on the JIMS server.

   - Switch to the HTTP protocol to view cleartext messages.

2. If the status of the Query State on Juniper Identity Management Service is Active, display in the trace log any error messages generated by the user query function using the following commands:

```
[edit services user-identification]
user@host#set services user-identification authentication-source aruba-clearpass traceoptions
file cp_query
user@host#set services user-identification authentication-source aruba-clearpass traceoptions
file size 5m
user@host#set services user-identification authentication-source aruba-clearpass traceoptions
level all
user@host#set services user-identification authentication-source aruba-clearpass traceoptions
flag all
```

The SRX Series device creates a new log named cp_query under **/var/log**. Check for an XML post similar to the following:

```
May 12 09:24:49 uid_set_query_url: query url: https://192.168.5.10/user_query/v1/ip/
192.168.8.30
May 12 09:24:49 uid_set_http_header: set HTTP header "Authorization:Bearer
FGDfuanyhlhDhlbuvsoapO6q7VkdvZN8hamxYgk"
May 12 09:24:49 CURLINFO (query for 192.168.8.30): Added 192.168.5.10:443:192.168.5.10 to DNS
cache
May 12 09:24:49 CURLINFO (query for 192.168.8.30): Found bundle for host 192.168.5.10:
0x868f0c0
May 12 09:24:49 CURLINFO (query for 192.168.8.30): Re-using existing connection! (#7) with
host 192.168.5.10
May 12 09:24:49 CURLINFO (query for 192.168.8.30): Connected to 192.168.5.10 (192.168.5.10)
port 443 (#7)
May 12 09:24:49 uid_query_write_data_cb: saved curl data: {
    "source": "Aruba ClearPass",
    "ip": "192.168.8.30",
    "user": "peter",
    "domain": "TME.JNPR.LOCAL",
    "roles": [
        "Administrators",
        "Domain Admins",
        "Domain Users",
        "Denied RODC Password Replication Group",
        "Users"
],
"spt": "Healthy",
"updated_at": "2017-05-12T16:14:56.202000Z",
"is_online": true,
"end-user-attribute": {
    "device-identity": {
        "value": "FGU-TMEWIN7-06$",
May 12 09:24:49 CURLINFO (query for 192.168.8.30): Connection #7 to host 192.168.5.10 left
intact
```

Juniper Identity Management Service replies in JavaScript Object Notation (JSON) format. Look for any error messages in the output.

3. When you are done, disable the trace logging.

Configuring the SRX Series User Query Function to Connect to Juniper Identity Management Service | **25**

Verifying the Web API Connection from an SRX Series Device

Before you begin, you need the following information:

- The HTTPS port number (default value is 8443) or HTTP port number (default value is 8080) on the SRX Series device

- The username and password that the HTTPS or HTTP server on the SRX Series device uses to authenticate incoming connections

To verify that the Web API connection and data communications between an SRX Series device and Juniper Identity Management Service are working properly:

1. Verify that users are in the Valid state by checking the user authentication tables on the SRX Series device:

   ```
   user@host>show services user-identification authentication-table authentication-source aruba-
   clearpass all
   user@host>show services user-identification authentication-table authentication-source aruba-
   clearpass all extensive
   ```

   These commands display the entire ClearPass authentication table contents. In this scenario, the ClearPass authentication table's user entries include authentication and identity information that the SRX Series device obtains from Juniper Identity Management Service.

2. If there are no entries in the authentication table and the status of the Web API connection on Juniper Identity Management Service is Connect Failed, do the following:

   - Check if traffic is allowed between Juniper Identity Management Service and the SRX Series device on the configured ports (by default, HTTPS port 8443 and HTTP port 8080).

   - Check the configured user credentials.

   - Perform a packet capture on Juniper Identity Management Server.

   - Switch to the HTTP protocol to view cleartext messages.

3. If the status of the Web API connection on the JIMS server is Connected, enable debugging by using the following commands:

```
[edit services user-identification]
user@host#set system services webapi debug-log api-log
user@host#set system services webapi debug-level info
```

The SRX Series device creates a new log named api_log under **/var/log**. Check for an XML post similar to the following:

```
2017/05/12 18:39:08 [info] 99992#0: 99992#0: <?xml version="1.0" encoding="UTF-8">
<userfw-entries>
    <userfw-entry>
        <source>Aruba ClearPass</source>
        <timestamp>2017-05-12T01:38:38.850000Z</timestamp>
        <operation>logon</logon>
        <IP>192.168.8.29></IP>
        <domain>domain_name</domain>
        <user>pete</user>
        <role-list>
            <role>Domain Admins</role>
            <role>Administrators</role>
            <role>Denied RODC Password Replication Group</role>
            <role>Domain Users</role>
            <role>juniper</role>
            </role-list>
        <posture>Healthy</posture>
        <end-user-attribute>
            <device-identity>
                <value>FGU-TMEWIN7-06$</value>
            </device-identity>
        </end-user-attibute>
        </userfw-entry>
    </userfw-entries>
```

This is the HTTPS POST message from Juniper Identity Management Service to the SRX Series device. Following this post is the parsing of XML data by the SRX Series device. Look for any error messages in the data.

4. When you are done, disable debug logging.

Verifying the Syslog Messages from an SRX Series Device

Before you begin, you need the following information:

- Define the IP address and port of the JIMS syslog server listens to.

- Configure the JIMS server to collect syslog data whenever it detects the occurrence of a logoff event, logon event, or a change in value from the remote server session.

- SRX Series device

To verify that JIMS can receive the message from a remote syslog client over a UDP and TCP connection:

JIMS supports three types of syslog messages- logon, logoff and modify.

1. Verify that the syslog message is parsed as logon message. If the syslog message is parsed as a logon message, a logon entry is sent to SRX Series device which is verified by checking the user firewall authentication entry which is generated on SRX Series device:

   ```
   user@host> show services user-identification authentication-table ip-address 192.0.2.10
   ```

   The SRX Series device displays an output similar to the following:

   ```
   Logical System: root-logical-system
   Domain: win2012.test.com
     Source-ip: 192.0.2.10
       Username: ad-user1
       Groups:posture-healthy, users, domain users, ad-group1
       State: Valid
       Source: JIMS - Active Directory
       Access start date: 2018-10-26
       Access start time: 16:26:57
   ```

```
        Last updated timestamp: 2018-10-26 08:21:29
        Age time: 60
```

2. If the syslog message is parsed as a logoff message, the correspondent authentication entry is deleted from the SRX series device.

3. If the syslog message is parsed as a modify message, the authentication entry can be updated from the SRX Series device.

RELATED DOCUMENTATION

Configuring JIMS to Receive Remote Syslog Messages | **79**

10
CHAPTER

JIMS Configuration Import and Export

Configuring Administration Interface Options

From the Options dialog box, you can configure the following Administration Interface settings:

- File logging log level and log path. The File Logging settings are for logging errors that might popup in dialog boxes when using the Administrative Interface. The File Logging settings are independent of the settings specified in the Logging tab that define the log from. See "Configuring JIMS Logging" on page 46.

To specify a default folder path that is used when performing an import or export of a configuration file:

1. In the navigation pane, select **File > Options**. The Administrative Interface Configuration dialog box appears.

2. From the Export/Import Settings section of the dialog box, in the Default Path field click **Browse** to access the Browse For Folder dialog box. Navigate to the location that you want to use as the default path for configuration file exporting and importing.

    The default path location is written to the windows registry under the following key: `HKEY_CURRENT_USER \Software\Juniper Networks\Juniper® Identity Management Service\Workspace\Administrative Interface Configuration`. This action preserves the folder path to ensure the same whenever you restart the JIMS Administrative Interface.

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

To specify the GUI logging log level and path:

1. In the navigation pane, select **File > Options**. The Administrative Interface Configuration dialog box appears.

2. From the File Logging section of the dialog box, make the following selections:

    - Log Level—Select a logging level, which can be set to:

        - **None**—No logging (disabled).

        - **Error**—Critical events affecting the entire system (log only errors).

        - **Warning**—Unexpected per-transaction events (log errors and warnings).

        - **Debug**—Most detailed logging level for troubleshooting (log errors, warnings, and additional debug data that may be available).

    - Log Path—Specify the base folder for the logs. Click **Choose** to access the Browser for Folder dialog box. Select the folder to use for file logging.

        Following is the log filename format `jims_admin_yyyy-mm-dd.log` (for example, `jims_admin_2018-08-01.log`).

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

Exporting or Backing Up a JIMS Server Configuration

Juniper Identity Management Service supports exporting an existing JIMS server configuration as a file that can be imported into another JIMS server. You can save the configuration to a file in a configurable default path. As an alternative to exporting the JIMS server configuration to another JIMS server, you can backup the configuration file and save it locally on the same JIMS server.

You must not save the password associated with a JIMS server configuration unless you are planning on importing the configuration file to the same JIMS server. Password encryption is specific to each JIMS server, and is saved if you backup the configuration file to the same JIMS server. If you attempt to import the configuration with passwords from a different server, you must reenter the each password.

To export a JIMS server configuration to a file:

1. In the navigation pane, select **File > Export**. The Export Configuration to File dialog box appears. The File text field lists the path to the last folder location previously specified. The configuration file includes a default file name that reflects the content of the exported configuration. The default configuration file name also includes the current date and time.

   The default filename is based on the local date and time. The prefix is selected as either `backup_` or `export_` depending on whether the **Include Passwords** check box is checked or unchecked.

2. Click the **Advanced** button to export the required partial configuration. The configuration chooser dialog box appears to choose the partial configuration from the subset.

   If you export a configuration and use the **Advanced** button, only the partial configuration that you choose is written to the saved XML configuration. If you subsequently import a partial configuration, only the partial configuration from the original subset is overwritten.

3. To backup the configuration file to the same JIMS server, click the **Include Passwords** check box.

   Ensure that the **Include Passwords** check box is unchecked if you import the exported configuration on another JIMS server. Password encryption is specific to each JIMS server and decrypted correctly if you restore the configuration file to the same JIMS server on which the backup is made.

4. Click **Change** to access the Save As dialog box to select a different configuration file location or to create a new folder. Navigate to a location where you want to save the JIMS server configuration file, or create a new folder. The File Name text field lists the path to the last folder location previously specified.

   You have the option to specify a default folder path as a configuration file Export/Import setting. See .

   Hold down the control key while clicking the **Advanced** button to export the configuration that contains only templates or base configuration. We do not recommend this option because a subsequent import replaces the configuration with only the templates.

It is recommended that you export a full configuration first to be able to repair the error configuration.

5. Click **OK** to export or backup the configuration file.

Importing a JIMS Server Configuration

Juniper Identity Management Service supports importing of an existing JIMS server configuration to the same JIMS server or to another JIMS server. Note that when importing the configuration file on a different server, you are prompted for a list of new passwords.

To import a JIMS server configuration file:

1. In the navigation pane, select **File > Import**. The Import dialog box appears with the path to the last folder location that was previously specified.

2. To select a different configuration file location, click **Browse** to access the Open dialog box. Navigate to the location where you saved the exported configuration file.

   You can specify a default folder path as a configuration file Export/Import setting. See "Configuring Administration Interface Options" on page 108.

3. Click the **Advanced** button to import the required partial configuration. The configuration chooser dialog box appears to choose the partial configuration from the subset. If you choose the partial configuration, the following warning message is displayed on the configuration chooser dialog box.

   `You are choosing to import a partial configuration, only those elements will be overwritten.`

   If you import a full configuration and use the **Advanced** button, only the partial configuration that you choose is overwritten. If you import a partial configuration, only the chosen partial configuration from the subset is overwritten.

   You must click the **Accept Warning** check box at the bottom of the dialog box to click **OK** for import process to start.

   > ⚠ **WARNING:** When you import the partial configuration, JIMS clears all the user directory settings and templates and replace them with whatever is specified. JIMS do not overwrite your event sources but overwrite all the user directory entries.

4. Once the file is selected for import, the **Add Passwords** button appears at the bottom left side of the Import dialog box if the configuration file is exported without passwords, or if it is exported to a different JIMS server.

a. Click **Add Passwords**. The Import - Add Missing Passwords dialog box appears to enter passwords for all configuration items that require a password. The table lists each entry by Index, Type, Data Type, Data, Username, Password, and Template.

Configuration items that require passwords appear with a light red background, and the Password column indicates that the password is `missing`. Once the password is assigned, the background turns to light green and the Password column changes from `missing` to `OK`.

The Status box shows the current state of the configuration.

The status of the last assign operation is reflected in the status text at the bottom of the dialog box.

- Success- In-memory working configuration is updated.

- Total–Total number of passwords in the configuration.

- Fixed–Count of passwords that are now OK

- Remaining–Count of passwords that still need to be assigned

The green progress bar shows the amount of progress made towards assigning the missing passwords.

b. Under the Current Password List Entry section of the dialog box, type a password for the currently selected item.

c. Click **Assign**. The assigned password is encrypted and saved in the in-memory working configuration. The current selection moves to the next index in the missing password list if password assignment was successful.

d. Once all missing passwords are assigned, click **OK**. You return to the main Import dialog box.

The **OK** button is grayed out until all missing passwords are assigned.

5. Click **OK** to start the import process using the configuration with the newly added or updated passwords.

11
CHAPTER

Network Device Monitoring

Network Device Monitoring Overview

Juniper Identity Management Service enables you to monitor system-level status and the status of the following network devices connected to Juniper Identity Management Service:

- SRX Series devices

- Event log sources, which can be Microsoft Active Directory domain controllers or Exchange servers

- User information sources, which can be Microsoft Active Directories

- PC probes to domain PCs

Viewing a System-Level Status Summary

To view a summary of the system-level status of Juniper Identity Management Service and the network devices connected to the server, in the navigation pane, select **Status** and then select the **Summary** tab.

Click **Refresh** to update the information in the status fields.

> **NOTE**: The system-level status summary displays a timestamp from the last refresh at the top of the screen.

contains the field definitions for a system-level status summary.

Table 9: System Status Summary Field Definitions

Field	Definitions
JIMS Service State	The state of Juniper Identity Management Service, which can be: • Start Pending • Continue Pending • Running • Pause Pending • Paused • Stop Pending • Stopped
Process ID	The process ID of Juniper Identity Management Service.
Admin Connection State	The state of the connection between the Juniper Identity Management Service application and the JIMS server, which can be: • Connecting • Connected • Connection Failed • Service Unknown
Port	The port number of the JIMS server.
Server	The IPv4 address of the JIMS server.
JIMS Server	
Started	The date and time the server was started.
Uptime	The time the server has been running.

Table 9: System Status Summary Field Definitions *(Continued)*

Field	Definitions
Active	
Clients [JIMS Release 1.0 only]	The number of connected SRX Series devices.
Users	The number of active users.
Groups	The number of groups.
Event Sources [JIMS Release 1.0 only]	The number of connected event log sources, which can be Active Directory domain controllers and Exchange servers.
Devices	The number of active devices.
Domains	The number of domains.
Sessions	The number of active sessions.
Reports	The number of generated reports.
Configured Clients	
SRX	The number of connected SRX Series devices.
CSO	The number of connected CSO platforms.
Configured Sources	
Event	The number of connected event log sources, which can be Active Directory domain controllers and Exchange servers.

Table 9: System Status Summary Field Definitions *(Continued)*

Field	Definitions
Info	The number of connected Active Directories.
Syslog	The number of connected syslog server sources.
PC Probe	The number of configured sets of PC probe credentials.

Viewing System-Level Status

To view system-level status of connected network devices, in the navigation pane, select **Status** and then select the **System** tab.

Click **Refresh** to update the information in the status fields.

NOTE: The system-level status displays a timestamp from the last refresh at the top of the screen.

Table 10 on page 116 contains the field definitions for system-level status.

Table 10: System Status Field Definitions

Category	Attribute	Definition
Overview	Sessions	The number of currently logged-in users that triggered an event.
	Users	The number of currently logged-in devices that resulted in the generation of data.
	Devices	The number of currently logged-in devices.

Table 10: System Status Field Definitions *(Continued)*

Category	Attribute	Definition
	Reports	The number of reports sent to the SRX Series devices.
	Domain names	The number of domains within which authentication is occurring.
	Groups	The number of groups within which authentication is occurring.
Session Data	Event Users	The number of currently logged-in users that triggered an event.
	Event Devices	The number of currently logged-in devices that resulted in the generation of data.
Session States	Init	The number of sessions in the Init state.
	Incomplete	The number of sessions in the Incomplete state.
	Reported	The number of sessions in the Reported state.
Pending Requests	Directory	The number of pending requests that have been sent to or are waiting to be sent to the connected Active Directories.
	PC Probe	The number of pending domain PC probes to user devices.
	Batch Context	The number of pending batch queries from the SRX Series devices to Juniper Identity Management Service.
Client Reports	User	The number of currently logged-in users.
	Device	The number of currently logged-in devices.
	Group	The number of groups within which authentication is occurring.

Table 10: System Status Field Definitions *(Continued)*

Category	Attribute	Definition
	Domains	The number of domains within which authentication is occurring.
Cumulative		
PC Probe	Success	The number of successful PC probes.
	Total	The number of attempted PC probes.
	No Credentials	The number of unsuccessful PC probes caused by no credentials being configured for PC probes.
User Events	On	The number of currently logged-in users.
	Discarded	The number of discarded events.
	Info	The number of Information events.
Device Events	On	The number of currently logged-in devices.
	Discarded	The number of discarded events.
	Info	The number of Information events.
SRX Query	Reports	The number of reports received per SRX Series device.
	Requests	The number of query requests for reports per SRX Series device.
	Errors	The number of query errors.
SRX WebAPI	Pushes	The number of pushed SRX Series device reports.

Table 10: System Status Field Definitions *(Continued)*

Category	Attribute	Definition
	Online Reports	The number of SRX Series device login reports, including retries.
	Errors	The number of SRX Series devicepush errors.
	Offline Reports	The number of SRX Series device logout reports, including retries.
CSO Clients	Pushes	The number of pushed CSO reports.
	Online Reports	The number of CSO login reports, including retries.
	Errors	The number of CSO push errors.
	Offline Reports	The number of CSO logout reports, including retries.
Directory Data	Success	The number of requests handled successfully.
	Updates	The number of user updates.
	Polls	The number of polls.
	Misses	The number of requests not handled because no handler was found.
	Group Updates	The number of group updates.
Event Reader	Events	The number of events.
	Polls	The number of polls.

Viewing SRX Series Device Status

To view the status of the SRX Series devices connected to the JIMS server, in the navigation pane, select **Status** and then select the **Clients** tab. Double-clicking an entry in the list brings up a page displaying detailed status for that specific SRX Series device.

Click **Refresh** to update the information in the status fields.

> **NOTE**: The SRX Series client status displays a timestamp from the last refresh at the top of the screen.

contains the field definitions for SRX Series client status and contains the field definitions for SRX Series detailed client status.

Table 11: SRX Series Client Status Field Definitions

Field	Definition
IP Address	The IP address of the SRX Series device.
Description	A description of the SRX Series device.
Query State	The state of the Query connection between Juniper Identity Management Service and the SRX Series device, which can be: • Active • Inactive • Batch Active • Batch Inactive This is the connection used when the SRX Series device is running Junos OS Release 15.1X49-D100, 17.4R1, or a later release.
Requests	The number of queries sent from the SRX Series device.

Table 11: SRX Series Client Status Field Definitions *(Continued)*

Field	Definition
Reports	The number of reports sent from Juniper Identity Management Service in response to queries from the SRX Series device.
Errors	The number of errors detected while processing queries from the SRX Series device.
Last Error	The last error detected while processing queries from the SRX Series device. This can be either an HTTP status value (3 digits) or a Windows status code.
WebAPI Connection	The state of the Web API connection between Juniper Identity Management Service and the SRX Series device, which can be: • Inactive • Session Open • Connect • Connected • Session Open Failed • Connect Failed • Not Configured This is the connection used when the SRX Series device is running Junos OS Release 12.3X48-D45 or later.

Table 11: SRX Series Client Status Field Definitions *(Continued)*

Field	Definition
State	The last state of the Web API push, which can be: • Inactive • Pending • Request Open • Request Sent • Write Data • Data Written • Receive Response • Response Received • Retry • Auth Retry • Open Failed • Open Request Failed • Send Request Failed • Write Data Failed • Receive Response Failed • Failed
Pushes	The number of times a set of reports was pushed from Juniper Identity Management Service to the SRX Series device.
Last Status	The last HTTPS response status of the push from Juniper Identity Management Service to the SRX Series device.

Table 11: SRX Series Client Status Field Definitions *(Continued)*

Field	Definition
Errors	The number of errors encountered during pushes from Juniper Identity Management Service to the SRX Series device.
Last Error	The last error detected while pushing reports from Juniper Identity Management Service to the SRX Series device.

Table 12: SRX Series Client Detailed Status Field Definitions

Category	Attribute	Definition
SRX Client	Description	A description of the SRX Series device.
	IP Address	The IP address of the SRX Series device.
	ID	Client ID that the SRX Series device needs to obtain an OAuth token from the JIMS server for user queries.
	Work	The total number of Work objects scheduled for the SRX Series device.
	Active	The number of active Work objects for the SRX Series device.
	Pended	The number of pending Work objects for the SRX Series device.
Query	Requests	The number of query requests for reports by the SRX Series device.
	Reports	The number of reports sent to the SRX Series device based on the query.
	Time	Timestamp of the query from the SRX Series device.
	State	The state of the query connection between Juniper Identity Management Service and the SRX Series device, as shown in Table 11 on page 120.

Table 12: SRX Series Client Detailed Status Field Definitions *(Continued)*

Category	Attribute	Definition
	Status	The status of the query connection between Juniper Identity Management Service and the SRX Series device.
	Pings	Total number of ping transmitted to check the connection.
	Bytes Sent	Total number of bytes transmitted.
Query Last Error	Time	Timestamp of the last error detected while processing queries from the SRX Series device.
	Status	Log on or log off operation.
	Errors	The last error detected while processing queries from the SRX Series device. This can be either an HTTP status value (3 digits) or a Windows status code.
Queries By Type	IP (V1)	Queries for existing IP flow from IP address on interface V1.
	IP (V2)	Queries for existing IP flow from IP address on interface V2.
	User	Queries from active users.
	Batch	Pending batch queries from the SRX Series devices to Juniper Identity Management Service, listed by type.
Errors By Type	IP (V1)	Error codes for existing IP flow from IP address on interface V1.
	IP (V2)	Error codes for existing IP flow from IP address on interface V2.
	User	Active users with errors.

Table 12: SRX Series Client Detailed Status Field Definitions *(Continued)*

Category	Attribute	Definition
	Batch	Pending batch queries with an error from the SRX Series device to Juniper Identity Management Service, listed by error type.
Web API	Connection	The HTTPS port number (default value is 8443) or HTTP port number (default value is 8080) on the SRX Series device.
	Time	The timestamp when the Web API established a connection with the Juniper Identity Management Service.
	State	The state of the Web API connection between Juniper Identity Management Service and the SRX Series device, as shown in Table 11 on page 120.
	Status	The status of the Web API query connection between Juniper Identity Management Service and the SRX Series device.
WebAPI Last Error	Time	The time of the last error detected while pushing reports from Juniper Identity Management Service to the SRX Series device.
	Status	The status of WebAP connection.
	Errors	The number of SRX Series device push errors.
WebAPI Reports	Online	The number of SRX Series device login reports, including retries.
	Offline	The number of SRX Series device logout reports, including retries.
	Device Excluded	The number of SRX Series devices excluded from the report.
	Bytes Sent	Total number of bytes transmitted in the Web API reports.
Filtered	Address	Filtered IPv4 address range (start address and end address).

Table 12: SRX Series Client Detailed Status Field Definitions *(Continued)*

Category	Attribute	Definition
	Domain	Filtered SRX Series device batch query count by domain.
	Begin Time	The begin time of the filtered query.
	End Time	The begin time of the filtered query.
	IPv6	Filtered IPv6 address range (start address and end address).

Viewing CSO Client Status

Support for Viewing CSO Client Status is supported in Juniper Identity Management Service Release 1.1 and later.

To view the status of the Client Service Orchestration (CSO) connected to the JIMS server, in the navigation pane, select **Status** and then select the **Clients** tab. Double-clicking an entry in the list brings up a page displaying detailed status for the CSO client.

Click **Refresh** to update the information in the status fields.

> **NOTE**: The CSO status displays a timestamp from the last refresh at the top of the screen.

contains the field definitions for CSO status and contains the field definitions for CSO client detailed status.

Table 13: CSO Client Status Field Definitions

Field	Definition
Contrail Server	The host name or the IP address of the CSO platform.

Table 13: CSO Client Status Field Definitions *(Continued)*

Field	Definition
Description	A description of the CSO platform.
Connection State	The state of the connection between Juniper Identity Management Service and CSO, which can be: • Active • Inactive • Batch Active • Batch Inactive

Table 13: CSO Client Status Field Definitions *(Continued)*

Field	Definition
State	The last state of the push, which can be: • Inactive • Pending • Request Open • Request Sent • Write Data • Data Written • Receive Response • Response Received • Retry • Auth Retry • Open Failed • Open Request Failed • Send Request Failed • Write Data Failed • Receive Response Failed • Failed
Pushes	The number of times a set of reports was pushed from Juniper Identity Management Service to CSO.
Re-Auths	The number of times a re-authentication occurred between the Juniper Identity Management Service and CSO.

Table 13: CSO Client Status Field Definitions *(Continued)*

Field	Definition
Last Status	The last HTTPS response status of the push from Juniper Identity Management Service to CSO.
Errors	The number of errors encountered during pushes from Juniper Identity Management Service to CSO.
Last Error	The last error detected while pushing reports from Juniper Identity Management Service to CSO.

Table 14: CSO Client Detailed Status Field Definitions

Category	Attribute	Definition
CSO Client	Description	A description of the CSO platform.
	IP Address	The IP address of the CSO platform.
	ID	Client ID that the SRX Series device needs to obtain an OAuth token from the JIMS server for user queries.
	Work	The total number of Work objects scheduled for the CSO platform.
	Active	The number of active Work objects for the CSO platform.
	Pended	The number of pending Work objects for the CSO platform.
Contrail	Connection	The HTTPS port number (default value is 8443) of the CSO platform.
	Time	The timestamp when the CSO platform established a connection with the Juniper Identity Management Service.

Table 14: CSO Client Detailed Status Field Definitions *(Continued)*

Category	Attribute	Definition
	State	State for the CSO platform, which can include: • Last successfully transmitted Report (or NULL) • Statistics • Last HTTP code • Last error
	Status	Periodic status update to aid in error handling.
	Re-Authentications	The number of times a re-authentication occurred between the Juniper Identity Management Service and the CSO platform.
Last Error	Time	Timestamp of the last error detected while processing queries from the CSO platform.
	Status	Log on or log off operation.
	Errors	The last error detected while processing queries from the CSO platform.
Reports	Online	The number of CSO login reports, including retries.
	Offline	The number of CSO logout reports, including retries.
	Bytes Sent	Total number of bytes transmitted in the JSON reports.
Filtered	Domain	Filtered CSO batch query count by domain.
	User	Filtered CSO batch query count by user.

Viewing Event Log Source Status

To view the status of the event log sources connected to the JIMS server, in the navigation pane, select **Status** and then select the **Event Sources** tab.

Click **Refresh** to update the information in the status fields.

> **NOTE**: The event log source status displays a timestamp from the last refresh at the top of the screen.

At startup, JIMS will wait up to 900 seconds (or more in some cases) for user data sources to complete the learning mode before JIMS proceeds to read events. After the timeout has completed, JIMS will process events even if it has not completed the initial learning operation.

Table 15 on page 131 contains the field definitions for event log source status.

Table 15: Event Log Source Status Field Definitions

Field	Definition
Server	The IPv4 address of the event log source.
Source Type	The type of event log source, which can be a Microsoft Active Directory domain controller or Exchange server.
Description	A description of the event log source.
State	The last state of the event log source, which can be: • Init • Idle • Learning • Polling • Restarting • Shutting Down

Table 15: Event Log Source Status Field Definitions *(Continued)*

Field	Definition
Errors	The number of event errors.
Polls	The number of polls.
Events	The number of events.

Release History Table

Release	Description
1.2.0	At startup, JIMS will wait up to 900 seconds (or more in some cases) for user data sources to complete the learning mode before JIMS proceeds to read events.

Viewing Active Directory Status

To view the status of the Active Directories connected to the JIMS server, in the navigation pane, select **Status** and then select the **Info Sources** tab.

Click **Refresh** to update the information in the status fields.

> **NOTE**: The info sources status displays a timestamp from the last refresh at the top of the screen.

contains the field definitions for Active Directory status.

Table 16: Active Directory Status Field Definitions

Field	Definition
Server	The IPv4 address of the Active Directory.

Table 16: Active Directory Status Field Definitions *(Continued)*

Field	Definition
Source Type	The source type, which can be a Microsoft Active Directory.
Description	A description of the Active Directory.
State	The last state of the Active Directory, which can be: • Idle • Learning • Polling • Restarting • Reconnecting • Shutting Down
Errors	The number of errors.
Requests	The number of requests.
Success	The number of requests handled successfully.
Polls	The number of polls.
Updates	The number of user updates.

Viewing Domain PC Probe Status

To view the status of the domain PC probes initiated by Juniper Identity Management Service, in the navigation pane, select **Status** and then select the **PC Probe** tab.

Click **Refresh** to update the information in the status fields.

> **NOTE**: The domain PC probe status displays a timestamp from the last refresh at the top of the
> screen.

contains the field definitions for domain PC probe status.

Table 17: Domain PC Probe Status Field Definitions

Field	Definition
Sequence	The sequence number of the set of administrative credentials.
Username	The username credential (Login ID) in the set of administrative credentials used to initiate the PC probe to a domain PC.
Description	A description of the set of administrative credentials.
Total Probes	The number of attempted PC probes to domain PCs.
Success	The number of successful PC probes to domain PCs.

Viewing Syslog Source Status

To view the status of the collected system message log data, in the navigation pane, select **Status** and then select the **Syslog Sources** tab.

The JIMS server drops syslog messages from unknown sources.

- Click **Refresh** to update the information in the status fields. The syslog sources status displays a timestamp from the last refresh at the top of the screen.

contains the field definitions for syslog source status.

Table 18: Syslog Remote Status Field Definitions

Field	Definition
Server IP	The IPv4 address of the remote syslog source.
Source Type	The syslog event source trigger type (logon, logoff, modify).
Description	A description of the remote syslog source.
State	The last state of the remote syslog source, which can be: • Init • Idle • Learning • Polling • Restarting • Shutting Down
Errors	The number of remote syslog source errors.
Requests	The number of remote syslog source requests.
Events	The number of remote syslog source events. Syslog events work similar to both Event Log events and User info – they tie together IP information with user or device information as an Event Log does, and ties the user to a group list.

12

CHAPTER

Juniper Identity Management Service
License Attributions

Juniper Identity Management Service License Attributions

Support for Juniper Identity Management Service License Attributions is supported in Juniper Identity Management Service Release 1.1 and later.

Juniper Identity Management Service uses OpenSSL version 1.0.2-r, which is licensed under the OpenSSL license as well as the original SSLeay license.

OpenSSL License

Copyright © 1998-2017 The OpenSSL Project All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public License.]

Juniper Identity Management Service uses 'zlib', a general purpose compression library, copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler. This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.]

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Juniper Identity Management Service uses JSON for Modern C++ 2.11, which is licensed under the MIT License MIT License Copyright (c) 2013-2018 Niels Lohmann

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR