SRC PE Software Release Notes

Release 4.0.0
September 2011
Revision 12

These release notes cover Release 4.0.0 of the Juniper Networks Session and Resource Control (SRC) portfolio. The SRC software runs on C Series Controllers. If the information in these release notes differs from the information found in the published documentation set, follow these release notes.

Contents

Release Overview

If the information in your current release notes differs from the information found in the other documentation sources, follow the *SRC PE Release Notes*.

Before You Start

Before you use your new software, read these *Release Notes* in their entirety, especially the section *Known Problems and Limitations*. You need the following documentation to fully understand all the features available in Release 4.0.0:

- These *SRC 4.0.0 Release Notes*, which describe the changes between Releases 3.2.0 and 4.0.0.
- The 4.0.0 SRC Policy Engine (SRC PE) software documentation set, which provides detailed information about features available in Release 4.0.x.

If the information in your current release notes differs from the information found in the other documentation sources, follow the *Release Notes*.

Documentation

The 4.0.x SRC PE core documentation set consists of several manuals and is available only in electronic format. Refer to the following table to help you decide which document to use.

Task	Related Documentation
Install the C Series Controller.	*C Series Controllers C3000 and C5000 Hardware Guide* *C Series Controllers C2000 and C4000 Hardware Guide*
Get up and running quickly.	*C3000 and C5000 Quick Start Guide* *C2000 and C4000 Quick Start Guide*
Learn about the general operation of the SRC software.	*SRC PE Getting Started Guide*
Perform basic configuration of a C Series Controller.	*SRC PE Getting Started Guide*
Use the SRC CLI.	*SRC PE CLI User Guide*
Use the License Manager and directory events.	*SRC PE Getting Started Guide*
Use the SAE, Juniper Networks routers, NIC, ACP, SSR, and SIC.	*SRC PE Network Guide*
Use the SNMP agent and logging utilities.	*SRC PE Monitoring and Troubleshooting Guide*
Integrate external network devices into the SRC network.	*SRC PE Network Guide*
Work with SRC services and policies.	*SRC PE Services and Policies Guide*

Task	Related Documentation
Work with SRC subscribers and subscriptions.	*SRC PE Subscribers and Subscriptions Guide*
Use the enterprise portals.	*SRC Sample Applications Guide*
Use the residential portal.	*SRC Sample Applications Guide*
Use the C-Web interface to configure the SRC software.	*SRC PE C-Web Interface Configuration Guide*
Get specific information about commands and statements for: • CLI and system • Juniper Networks database • SAE • Network Information Collector (NIC) • Session State Registrar (SSR) • Subscriber Information Collector (SIC) • SNMP agent • SRC Admission Control Plug-In (SRC ACP)	*SRC PE CLI Command Reference, Volume 1*
Get specific information about commands and statements for: • Services • Policies • Subscribers • Redirect server • External Subscriber Monitor • Dynamic Service Activator • IP Multimedia Subsystem (IMS) • Diameter application	*SRC PE CLI Command Reference, Volume 2*

The entire documentation set, including the release notes, in PDF format is available on the Juniper Networks Web site:

http://www.juniper.net/techpubs/software/management/src/

SRC Software

The SRC software for C Series Controllers is preinstalled on the device and available on the USB storage device supplied with the platform.

You can also download the SRC software and the product release notes from the Juniper Networks Web site at:

https://www.juniper.net/support/csc/swdist-erx/src.html

Release Highlights

Highlights include the following product enhancements:

NOTE: The SRC software runs on the C Series Controllers—a range of hardware platforms. The SRC 4.0.0 software contains the features found in the SRC 3.2.0 release plus the features listed in this section. The SRC 4.0.0 software may contain references to Release 7.6.0, which refers to the SAE version.

C Series Controllers

- Support for C3000 and C5000 Controllers

  There are two C Series Controller models: the C3000 model and the C5000 model. Each model is composed of four hard drives, three fan modules, redundant power supplies, one USB port, a console management port, and four Ethernet ports.

  - The C3000 Controller is designed to support up to 200,000 concurrent sessions.
  - The C5000 Controller is designed to support up to 400,000 concurrent sessions.

Dynamic Service Activator/Web Services Gateway

- Activation of Video Services

  A Web service SOAP/XML interface between a video server and the video server policy manager allows the video server to dynamically request resources on the operator's access network. It provides operations for requesting, releasing, and querying network resources.

  Dynamic Service Activator has a Web service interface that supports two new types of video services based on the set-top box:

  - On-demand video services
  - Personalized video services

  Each of the supported operations for these video services is implemented as a method in the Dynamic Service Activator Web service interface.

- Multiple Network Paths

  Dynamic Service Activator has new methods that ask for additional information to support requests from the external API that require information about network paths. These new methods are: subscribers-activateService, subscribers-deactivateService, subscribers-login, subscribers-logout, subscribers-modifyService, subscribers-read, subscribers-readSubscriber, and subscribers-readSubscription.

  These methods account for the possibility that a subscriber's IP address might not have a one-to-one relationship with a subscriber session. For example, to apply policies to MX Series routers that support the packet-triggered subscribers and policy control (PTSP) feature, the external API needs to multiplex requests for a single subscriber because the subscriber's single IP address might be used for multiple sessions to direct subscriber traffic on different paths.

- Document Literal Implementation of Dynamic Service Activator

There is now an implementation of Dynamic Service Activator that uses the document literal encoding style (DSA2). This interface is compatible with clients who do not properly support complex data types such as the activation attribute arrays, such as .NET clients.

License Management

- License Management System

  Server licenses for the SRC software must be obtained from the Juniper Networks License Management System. The server license is used in production environments and is managed by the SRC license server. The versions for the license server and the SAE must match.

  To obtain a server license, you must log into the Juniper Networks License Management System at http://www.juniper.net/generate_license and provide the following information:

  - Authorization code provided with your order
  - Serial number of your device on side of the unit
  - Hostname of the license server

NIC

- Configuration Scenarios

  There are configuration scenarios to support new Dynamic Service Activator features:

  - OnePopMixedIp—For activation of video services (assigned IP subscribers)
  - OnePopServiceNode—For multiple network paths (service node support)

  The following table provides information about the NIC configuration scenario and its agents:

Configuration Scenario	Name of NIC Configuration Scenario to Use	Type of Resolution	Agent Name
For scenarios in which there are static subscribers and DHCP subscribers	OnePopMixedIp	IP pool to interface	PoolInterface, StaticPoolInterface
		Virtual routers to SAEs	VrSaeId
For scenarios in which an IP address can have more than one managed subscriber session	OnePopServiceNode	IP addresses to SAEs	IpSaeId, IpSaeIdSsr

PTSP

- Packet-Triggered Subscribers and Policy Control (PTSP) Support

The Juniper Networks MX Series Ethernet Services Router supports the PTSP feature. MX Series routers that support PTSP are called service nodes because they can offer subscriber and service management even though they do not terminate subscriber signaling. When the service node is in the SRC environment, the SRC software supports the MX Series router by providing subscriber awareness. To support service nodes, the SRC software:

- Collects and dispatches subscribers' RADIUS accounting events that are generated by a subscriber management device such as a gateway GSN (GGSN).
- Creates an IP edge attachment session and stores it.
- Manages profile and policies for IP address sessions (PTSP sessions).
- Sends start, interim, and stop accounting records based on interaction with the MX Series router.

- PTSP Driver

  The PTSP feature allows dynamic policy and profile changes to be applied on a per-subscriber basis. The PTSP in the MX Series router signals the SRC policy manager when a new IP address flow is detected or when an existing flow is idle, and allows the policy manager to dynamically apply new policies associated with the IP address flow. The PTSP driver receives IP address notifications from the MX Series router and dynamically activates, modifies, or deactivates policies for existing subscriber sessions.

SAE

- PTSP Support

  The Juniper Networks MX Series Ethernet Services Router supports the packet-triggered subscribers and policy control (PTSP) feature. The SRC software allows the SAE to receive information about the subscribers connecting through IP edge devices attached to the managed MX Series routers that support PTSP (service nodes). The SAE can obtain information about the IP edge attachment sessions, including:

  - VPN ID associated with the virtual router for edge devices

    

    NOTE: **NIC and Dynamic Service Activator do not support use with VPN ID for service node subscriber sessions.**

  - Subscriber identity information from the SSR database

  The SAE uses the information to create interface or subscriber classification contexts and apply policy rules to the new parameters.

- SSR Reader Plug-In

  The SAE can obtain subscriber information from the Session State Registrar (SSR) database. The SSR reader authentication plug-in obtains information about the IP edge attachment sessions from the SSR to set the values for the plug-in attributes. The SSR reader plug-in can be used by a specific virtual router or for all virtual routers.

  - For a specific virtual router, configure the **authentication-plug-in** option at the **shared network device *name* virtual-router** hierarchy level.
  - For all virtual routers, configure the default plug-in used for subscribers assigned to a virtual router that does not specify an authentication plug-in with the **default-vr-authentication** option at the **shared sae configuration plug-ins event-publishers** hierarchy level.
  - For all virtual routers, configure the plug-in used for subscribers who log in through a specific device type with the **device-type-authentication *device-type* [*plug-ins*...]** option at the **shared sae configuration plug-ins event-publishers** hierarchy level.

- Calling-Station-Id AVP

  The SAE can obtain the Calling-Station-Id RADIUS AVP from the router running JUNOSe Software. The Calling-Station-Id AVP is used for customer premises equipment to further identify subscribers. The router reports the Calling-Station-Id to the SAE, which makes this information available for plug-ins, interface classification, subscriber classification, and the remote API.

- Idle Timeout for Specified Traffic Direction

  You can now specify an idle timeout interval for the input or output traffic direction, after which the SAE deactivates the service. At the **services global service** or **services scope *name* service** hierarchy level, you can use the **idle-timeout-input** option for the input traffic direction and the **idle-timeout-output** option for the output traffic direction. The **idle-timeout** option specifies the minimum time the service session is idle in both directions before the SAE deactivates it. The **idle-timeout-input** and the **idle-timeout-output** options can be specified together, but these options cannot be specified if the **idle-timeout** option is specified.

- Local QoS Profiles

  The SAE can obtain local QoS profile information from the router running JUNOSe Software. The local QoS profile is attached by means of other policy management tools on the router, such as the router CLI or Service Manager. The router reports all attached QoS profiles within the interface stack to the SAE. In turn, the SAE makes this information available for plug-ins, interface classification, subscriber classification, and the remote API.

- Subscriber Sessions for Policies Managed by External Policy Manager

  The SAE can manage services for subscribers on routers running JUNOSe Software, where policies are managed through an external policy management system. The SAE creates subscriber sessions on an interface that does not have default policies configured and manages the interface. In this case, you configure the SAE to manage an interface, and you configure an empty policy group to be assigned to the interface. The empty policy group does not contain a policy list.

NOTE: If you used empty policy groups before SRC Release 4.0.0, the interface was unmanaged.

Starting with SRC Release 4.0.0, the interface is managed without installation of any default policies on the router.

SIC

- Subscriber Information Collector (SIC)

  The subscriber information collector (SIC) is used in conjunction with the MX Series Ethernet Services Router running the packet-triggered subscribers and policy control (PTSP) solution. The role of the SIC is to listen for RADIUS accounting requests and filter undesired events based on attachment session attributes. The SIC can store accounting events in either the session state registrar database or forward them to a downstream accounting target. Optionally, the SIC can edit the accounting requests before sending the request to the specified accounting target.

SSR

- Session State Registrar (SSR)

  The Session State Registrar (SSR) solution implements a stateless, highly reliable and highly available cluster. It separates front-end processes from back-end data functions that take place on two or four data servers. Multiple C Series Controllers collaborate and perform different aspects of operation within the cluster to provide a common sessions database in a highly available, redundant environment. The common shared resources of the cluster can be accessed simultaneously by up to twenty-four C Series Controllers acting as SSR clients.

  When used in conjunction with an MX Series router running the packet-triggered subscribers and policy control (PTSP) solution, the SSR stores the IP edge attachment sessions learned from IP edge devices in the centralized SSR database. The IP edge session stored in the SSR database can be used by the SAE to map the sessions received from the MX Series router. An IP edge session is uniquely identified by IP address and VPN ID, and includes subscriber identity information, which is used to locate the subscriber profile for MX sessions that have the same subscriber IP address.

  Use of SSR component is subject to prior purchase of an SSR license.

Features Not Fully Qualified

The SRC Release 4.0.x documentation set describes some features that are present in the code but that have not yet been fully qualified by Juniper Networks. These features will be fully tested and supported in a future release. We expect these features to operate as documented; however, if you use any of these features before they have been fully qualified, it is your responsibility to ensure that the feature operates correctly in your targeted configuration.

The following features are present but not fully qualified in this release.

JPS

- Juniper Policy Server (JPS)

  JPS acts as a policy decision point (PDP) and policy enforcement point (PEP) that manages the relationships between application managers and CMTS devices in a PCMM environment.

  Contact the Juniper Networks Technical Assistance Center (JTAC) for information about qualification of this feature.

  Reference: TIC 13313

Upgrading the System Software

To upgrade the system software to Release 4.0.0 from a release earlier than Release 3.2.0, you must resize the disk to support additional components and the Juniper Networks database before upgrading the software.

To upgrade the software:

1. Enter the **request system install package IPMupgrade url *url*** command, where ***url*** is the path to the image file.

   This command resizes the disk of the C Series Controller and requires the C Series Controller to reboot twice.

2. Enter the **request system upgrade url *url*** command to upgrade the system software.

Recovering System Software on a C Series Controller

If you encounter a software failure on a C Series Controller, in most cases you can recover from the failure by restoring the software from a snapshot by using the **request system restore** command.

If, however, the operating system on the main partition on a C Series Controller is damaged, the operating system tries to boot from the snapshot partition. If the system does not boot from the snapshot partition, you can try to manually reboot the system and use the software snapshot.

If a software failure damages the snapshot partition on a C Series Controller, you can boot the system from the USB storage device supplied with the C Series Controller. After the system boots, it installs the system software from the USB storage device. The USB storage device supplied with the C Series Controller is a read-only device that contains a copy of the system software.

When you install the SRC software from a USB storage device, all system software, including the operating system, is installed, and the system hard drives are partitioned. As a result, any data, including data previously in the snapshot partition, is lost.

To boot a C Series Controller from the system snapshot:

1. Connect a console terminal to the C Series Controller.

   See your *C Series Controller Hardware Guide*.

2. Initiate a system reboot in one of the following ways.

   - Power off and then power on the C Series Controller.
   - From a terminal server, enter the break command appropriate to your console.

3. In the boot menu, select the backup partition.

   If a software failure damages the boot partition on a C Series Controller, you can install the system software from the USB storage device that is supplied with a C Series Controller.

To boot the system from the USB storage device and install the SRC software on a C Series Controller:

1. Plug the USB storage device into the USB port on the C Series Controller.
2. Connect a console terminal to the C Series Controller.

   See your *C Series Controller Hardware Guide*.

3. Power on the system.
4. At the boot prompt, press the Enter key, or follow the instructions on the display to cancel the operation.
5. After the C Series Controller reboots and the software installation is complete, set up the initial configuration.

   See your *C Series Controller Hardware Guide*.

Recovering the root Password

If you lose the root password, you will not be able to log in as the root user unless you perform one of these tasks:

- Reset the password with the USB storage device.
- Restore the default configuration from the console.

NOTE: **Restoring the default configuration replaces the existing configuration with the basic default configuration supplied with the SRC software.**

To reset the password with the USB storage device:

1. Plug the USB storage device into the USB port on the C Series Controller.
2. Connect a console terminal to the C Series Controller.

   See your *C Series Controller Hardware Guide*.

3. Power on the system.
4. At the boot prompt, enter **rescue**, and follow the instructions on the display to mount the existing system image and go into the shell.
5. In the shell, use the **chroot** command to change root directory to the attached system image.
6. In the shell, use the **passwd** command to reset the password.
7. Exit the shell. After the C Series Controller reboots and returns to the boot prompt, power off the system and remove the USB storage device before powering on the system.

   The root password should be set to the password you specified in Step 6.

To restore the default password from the console by loading the default configuration:

1. Connect to the console for the C Series Controller.
2. When the boot menu appears, press **a** to get to the boot command line.
3. Enter **4** as the argument at the end of the boot command line to run level 4, which will load the default configuration (including the password) that was supplied with the SRC software.

   The default configuration replaces the existing configuration.

Recovering Passwords for the Juniper Networks Database

The documentation does not disclose the default passwords that the Juniper Networks database uses. If you need access to these passwords or need to recover a password, contact Juniper Networks Technical Assistance Center (JTAC) for assistance.

Migrating SDX Data to a Juniper Networks Database

If you have an existing SDX installation and want to migrate your data from the directory storing the SDX data to the Juniper Networks database on an SRC platform, contact Juniper Networks Professional Services.

Known Behavior

This section describes certain SRC software behaviors and related issues to emphasize how the system works.

ACP

- ANCP update information from two routers might conflict.

  ACP uses the NasPortId as a unique identifier for ANCP update information stored in the remote update database. However, the NasPortId is only unique within a router so ANCP update information from two routers can conflict with each other and cause one update to overwrite the other.

  Reference: TIC 16592

Aggregate Services

- If you use aggregate services and specify a primary username for a subscriber reference expression, note that the configuration scenarios provided with the NIC do not provide a mapping from a primary username to the managing SAE. Consider using the login name instead. If you want to use the primary username as the subscriber reference expression for a fragment service, contact Juniper Networks Professional Services for assistance with setting up the NIC configuration to resolve the primary username to locate the managing SAE.

  Reference: None

Configuration Backups

- Save configurations in XML format for proper loading.

  You must save configurations in XML format using the **save** command. Other formats, such as configurations saved in text format or the output of the **display set** command, may not load properly.

  Reference: TIC 16244

Configuration Updates

- When you use the **load merge**, **load override**, or **load replace** command at any hierarchy level, the command loads all the configuration in the specified file.

  If you want to load the configuration for a specified hierarchy level:

  - Ensure that the file contains the **sdx:current=true** text to identify the level at which the configuration is to be loaded.
  - Run a **load** command with the **relative** option at the level at which you want to update the configuration.

  If a file contains configuration statements other than those at and below the level identified by **sdx:current=true**, the command disregards the other statements.

  If you enter a **load** command with the **relative** option and the file does not contain the text **sdx:current=true**, you receive a message indicating that the configuration cannot be loaded.

Reference: None

Console Authentication

- Logging in after entering the wrong password the first time.

  If you enter the wrong username/password combination when you log into the console, you are prompted for the LDAP password. This request is for the same password that you should have entered on your first try.

  Reference: TIC 14193

Juniper Networks Database

- Recommendations for use of multiple primary Juniper Networks databases.

  We recommend that you configure two to four Juniper Networks databases as primary databases in a community. If you plan to use more than two Juniper Networks databases in a primary role and expect to have frequent updates to the Juniper Networks database, we recommend that you test your application scenario with a projected traffic load. For assistance testing your application scenario, contact Juniper Networks Professional Services or JTAC.

  Reference: None

- Juniper Networks databases in community mode require hostname configuration.

  If you run Juniper Networks databases in community mode, all C Series Controllers that have a Juniper Networks database configured to be part of a community require hostname configuration.

  You can either configure Domain Name System (DNS) and enter the controller names into DNS or configure the controller names as static hostnames in all C Series Controllers.

  To configure each C Series Controller to use DNS:

  1. Navigate to the **[edit system]** hierarchy level.

     ```
     [edit]
     user@host# edit system
     ```

  2. Specify the name of a name server.

     ```
     [edit system]
     user@host# set name-server name-server
     ```

     where ***name-server*** is the IP address of a DNS name server.

  To configure static hostnames for each C Series Controller:

  1. Navigate to the **[edit system]** hierarchy level.

     ```
     [edit]
     user@host# edit system
     ```

  2. Specify the name of a C Series Controller as the static hostname.

```
[edit system]
user@host# set static-host-mapping host-name
```

where ***host-name*** is the fully qualified name.

Reference: TIC 13364

- Changing the mode of Juniper Networks databases.

  When you change the mode of two Juniper Networks databases from standalone to community, and assign one a primary role and the other a secondary role, review the error log in the */var/UMC/jdb/log* directory on the primary Juniper Networks database for the following message:

  ```
  [22/Mar/2007:11:27:15 -0400] agmt="cn=champ2golem.kanlab.jnpr.net"
  (golem:389) - Can't locate CSN 46029ccc000000010000 in the changelog (DB
  rc=-30990). The consumer may need to be reinitialized.
  ```

  Workaround: If you see a similar message, change the mode of the secondary Juniper Networks database from community to standalone, then back to community.

  For information about configuring Juniper Networks databases, see the *SRC PE Getting Started Guide*.

  Reference: TIC 13371

- Changing the role of a Juniper Networks database.

  If you change the role of a Juniper Networks database from primary to secondary, restart the Juniper Networks database after you set the role to secondary. If you do not restart the database, you receive a message similar to the following one at the CLI:

  ```
  javax.naming.NamingException: [LDAP: error code 1 - Mapping tree node for
  o=umc is set to return a referral, but no referral is configured for it];
  remaining name 'retailerName=default,o=users,o=UMC' commit completed
  with the above exception(s).
  ```

  Reference: TIC 13372

- Deleting statements on platforms running a secondary Juniper Networks database.

  When you delete statements from the CLI for a Juniper Networks database assigned a secondary role, you can receive a message for **ContextNotEmptyException** such as:

  ```
  [edit]
  root@golem# commit
  javax.naming.ContextNotEmptyException:
  ou=local,retailerName=ldapcommret1,o=users,o=UMC cannot be deleted
  commit completed with the above exception(s).
  commit complete.
  ```

  Workaround: Enter the commands to delete the same statements from a Juniper Networks database assigned a primary role. Whenever you delete statements for a Juniper Networks database, do so from a Juniper Networks database assigned a primary role.

  Reference: TIC 13376

JPS

- During shutdown, the JPS sometimes logs the following stack trace to stderr. This message is harmless and can safely be ignored.

  ```
  2006-04-24 15:38:48| java.io.InterruptedIOException
  2006-04-24 15:38:48| at java.io.FileOutputStream.writeBytes
  (Native Method)
  2006-04-24 15:38:48| at java.io.FileOutputStream.write
  (FileOutputStream.java:260)
  2006-04-24 15:38:48| at org.mortbay.util.RolloverFileOutputStream.write
  (RolloverFileOutputStream.java:220)
  2006-04-24 15:38:48| at org.mortbay.util.ByteArrayISO8859Writer.writeTo
  (ByteArrayISO8859Writer.java:95)
  2006-04-24 15:38:48| at org.mortbay.util.OutputStreamLogSink.log
  (OutputStreamLogSink.java:459)
  2006-04-24 15:38:48| at org.mortbay.util.OutputStreamLogSink.log
  (OutputStreamLogSink.java:437)
  2006-04-24 15:38:48| at org.mortbay.util.Log.message(Log.java:304)
  2006-04-24 15:38:48| at org.mortbay.util.Log.message(Log.java:234)
  2006-04-24 15:38:48| at org.mortbay.util.Log.event(Log.java:250)
  2006-04-24 15:38:48| at org.mortbay.util.ThreadedServer$Acceptor.run
  (ThreadedServer.java:612)
  ```

  Reference: TIC 11909

Policies

- Do not disable the Juniper Networks database (jdb component) while configuring policies with the Policies, Services, and Subscribers Editor.

  Workaround: Enable the Juniper Networks database and restart the CLI.

  Reference: TIC 15573

- Deleting policies that are being used can cause problems.

  Do not delete policies, especially default policies, that are in use.

  Reference: TIC 15153

Policy Management

- Use care when modifying configurations with other policy management tools for interfaces on JUNOSe routers that are managed by the SRC software.

  When applying policies to interfaces on JUNOSe routers that are managed by the SRC software, carefully consider using other policy management tools, such as CLI, RADIUS, CoA, or Service Manager. Policies that are applied to the interface before SRC management begins, such as at access-accept time, are properly replaced. However, if other policy managers change existing policies while SRC management is active, problems can occur.

  - If you have a preconfigured policy through CLI or RADIUS as part of subscriber PVC/VLAN provisioning, the existing policy becomes inactive and the SAE manages the subscriber interface. When the SAE stops managing the interface, the

preconfigured policy becomes active. However, if you change the policy on the interface using CLI or CoA, problems can occur.

- If you have a policy in Access-Accept, the existing policy becomes inactive and the SAE manages the interface.

SAE

- When using VPN ID to identify subscriber sessions for MX Series routers that support the packet-triggered subscribers and policy control (PTSP) feature, the NIC and Dynamic Service Activator are not supported.

  Reference: TIC 16565

- When specifying the name of a device at the **[edit shared network device]** hierarchy level, you must use lowercase characters.

  Reference: TIC 14568

- SAE shared properties cannot be created until local SAE properties are edited for the configuration group.

  If you want to use the configuration group for the SAE, edit the SAE shared properties at the [edit slot 0 sae] hierarchy level, then the group properties.

  Workaround: Configure a group within the SAE. To do so:

  1. At the **[edit slot 0 sae]** hierarchy level, specify a group name.

     ```
     [edit slot 0 sae]
     user@host# set shared /SAE/<group name>
     user@host# commit
     commit complete.
     ```

  2. Review the local properties.

     ```
     user@host# show
     real-portal-address 10.10.4.24;
     shared /SAE/<group name>
     initial {
        directory-connection {
           url ldap://127.0.0.1:389/;
           principal cn=ssp,ou=Components,o=Operators,<base>;
           credentials ********;
           blacklist;
        }
        directory-eventing {
           eventing;
           polling-interval 30;
        }
     }
     radius {
        local-address 10.10.4.24;
        local-nas-id SAE.myCseries;
     }
     ```

3. Change properties as needed (you must change at least one value to create the group) and commit the configuration.

4. Configure the group within a shared SAE configuration.

```
[edit]
user@host# edit shared sae group <group name>
```

Reference: TIC 12487

- Output for **show sae slot 0 statistics process** command.

  If you run the **show sae slot 0 statistics process** command shortly after you start the SAE, the CLI may become inoperative.

  Workaround: Wait for several minutes after you start the SAE before you run the **show sae slot 0 statistics process** command. If the CLI becomes inoperative, press Ctrl+c, wait a few seconds, and enter the command again.

  Reference: TIC 13387

- During synchronization in COPS-PR mode, the JUNOSe router can send delete request state (DRQ) messages for interfaces for which a request (REQ) message has not been received. In this case, the SAE logs an error message similar to the following:

```
11:30:33.140 EDT 26.08.2005 [CopsHandler-15/0xAC001FCE]
[UnsolicitedMessage] [50] Unable to handle message for
unknown context: {Message type: 3,
ClientType: 24754, Handle: Handle(C-Num=1,C-Type=1,handle=0xAC001FCE)
```

  You can ignore messages similar to the one above.

  Reference: TIC 10927

- The SAE sometimes prints a stack trace when a Blocks Extensible Exchange Protocol (BEEP) session is being taken down during an administrative change of address of the interface that the JUNOS routing platform uses to connect to the SAE. No data is lost in this procedure. You can safely ignore this exception.

  Reference: TIC 9612

- During shutdown, the SAE sometimes logs the following stack trace to stderr. This message is harmless and can safely be ignored.

```
2004-12-24 11:35:25| java.io.InterruptedIOException
2004-12-24 11:35:29| at java.io.FileOutputStream.write(Native Method)
2004-12-24 11:35:29| at java.io.FilterOutputStream.write
(FilterOutputStream.java:60)
2004-12-24 11:35:29| at java.io.FilterOutputStream.write
(FilterOutputStream.java:108)
2004-12-24 11:35:29| at org.mortbay.util.ByteArrayISO8859Writer.writeTo
(ByteArrayISO8859Writer.java:95)
2004-12-24 11:35:29| at org.mortbay.util.OutputStreamLogSink.log
(OutputStreamLogSink.java:467)
2004-12-24 11:35:29| at org.mortbay.util.OutputStreamLogSink.log
   (OutputStreamLogSink.java:445)
2004-12-24 11:35:29| at org.mortbay.util.Log.message(Log.java:297)
2004-12-24 11:35:29| at org.mortbay.util.Log.message(Log.java:232)
2004-12-24 11:35:29| at org.mortbay.util.Log.event(Log.java:248)
```

```
2004-12-24 11:35:29| at org.mortbay.util.ThreadedServer$Acceptor.run
(ThreadedServer.java:543)
```

Reference: TIC 9506

Services

- Service names are case-preserving.

  Do not mix cases in service names. Make sure you use the same names when specifying the service and subscription.

  Reference: TIC 14932

- Runtime parameters are not resolved when activating sample AAA policies.

  Do not use the user_ipMask and user_ipAddress runtime parameters for activate-on-login services.

  Reference: TIC 15181

Upgrade

- If the Java Web server is not enabled during upgrade from Release 2.1.0 to Release 3.0.0, an exception message might appear.

  During the upgrade procedure, the following message sometimes appears when the Java Web server (www component) is not enabled. This message can safely be ignored.

```
Stopping WWW: done
Jul 15, 2008 11:32:53 AM org.apache.catalina.startup.Catalina stopServer
SEVERE: Catalina.stop:
java.net.ConnectException: Connection refused
    at java.net.PlainSocketImpl.socketConnect(Native Method)
    at java.net.PlainSocketImpl.doConnect(PlainSocketImpl.java:333)
    at java.net.PlainSocketImpl.connectToAddress(PlainSocketImpl.java:195)
    at java.net.PlainSocketImpl.connect(PlainSocketImpl.java:182)
    at java.net.SocksSocketImpl.connect(SocksSocketImpl.java:366)
    at java.net.Socket.connect(Socket.java:519)
    at java.net.Socket.connect(Socket.java:469)
    at java.net.Socket.<init>(Socket.java:366)
    at java.net.Socket.<init>(Socket.java:180)
    at org.apache.catalina.startup.Catalina.stopServer(Catalina.java:394)
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
    at
       sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:25)
    at java.lang.reflect.Method.invoke(Method.java:597)
    at org.apache.catalina.startup.Bootstrap.stopServer(Bootstrap.java:320)
    at org.apache.catalina.startup.Bootstrap.main(Bootstrap.java:411)
```

Reference: TIC 15179

Known Problems and Limitations

This section identifies known problems and limitations in this release.

C-Web Interface

- Modifications to parts of the configuration tree do not appear automatically.

  When editing one part of the configuration tree automatically creates modifications in other parts of the configuration tree, you must click **Refresh** to see the modifications in the other parts of the configuration tree.

  Reference: TIC 13881

SAE

- Two identical interfaces are created for dual-stack interface on JUNOSe routers.

  When a dual-stack interface is defined for JUNOSe interfaces, the SAE creates two identical interfaces.

  Reference: TIC 13901

- Assertion error occurs with fast resynchronization and empty policy lists.

  With fast resynchronization, some inconsistencies may arise during cleanup that allow for a proper recovery during full synchronization. This assertion error indicates that there were empty policy lists.

  Reference: TIC 13950

Migration

This section provides information about migrating from earlier SRC software releases to SRC Release 4.0.0.

Policy Changes

Starting with SRC Release 4.0.0, an action configured for a policy rule no longer requires a name to identify the action. Old configurations with a name are accepted.

NOTE: **You cannot have multiple instances of the same action configured for one rule.**

Restrictions and Recommendations

CMTS Devices

SRC Release 4.0.0 should be suitable for use with any CMTS device that implements the PacketCable Multimedia Specification (PKT-SP-MM-I02-040930).

RADIUS Server

Juniper Networks SRC Release 4.0.0 was tested with the following RADIUS server products:

- Juniper Networks Steel-Belted Radius/Service Provider Edition (SPE) server

Any RADIUS product compliant with RFC 2865 and RFC 2866 should be suitable for use with SRC Release 4.0.0, including the following products:

- Merit RADIUS 4.1.2
- Interlink Networks RAD-Series RADIUS Server 6.0 and later
- FreeRADIUS Server Project freeRADIUS server
- Open System Consultants Radiator

Known issues exist with Steel-Belted Radius/SPE 4.0.3 and earlier.

Web Browsers

The C-Web interface in SRC Release 4.0.0 was tested with and supports use only with the following Web browsers:

- Firefox 2.0 or later
- Internet Explorer 6.0 or later

SRC Software Compatibility Matrix

Table 1 on page 21 shows which versions of the SRC software are compatible with specified versions of the JUNOS Software and JUNOSe Software.

For the most current information about supported software releases, contact JTAC.

Table 1: SRC Software Compatibility with JUNOSe Software and JUNOS Software

SRC Software Release	Tested with JUNOSe Release	Intended to Be Tested with JUNOSe Release	Tested with JUNOS Release	Intended to Be Tested with JUNOS Release
2.1.0	9.1.0p0-1		8.3	
3.0.0	9.0, 9.0.1, 9.1.1		9.0, 9.1	
3.1.0	9.2, 9.3, 10.0		9.2R3, 9.3R2, 9.4R1	
3.2.0	10.1.1, 10.2.1	10.3.0	9.4R3.5, 9.5R2.7, 9.6R1.3[1]	10.0R1
4.0.0R3	10.3, 11.0, 11.1		10.1, 10.2[2]	
4.0.0R7	10.3.3, 11.3.1, 12.0.0, 12.1.1		10.3R2, 11.1R1.14[2]	

[1]To use the DPI script service, SRC Release 3.2.0 was tested with JUNOS Release 9.5R4, Release 9.6R3, Release 10.0R3, and Release 10.1B3. It is intended to work with JUNOS Release 10.1R1.

[2]To support the PTSP feature, use JUNOS Release 10.2R1 and later.

Third-Party Software

This section lists the third-party software that is included with SRC Release 4.0.0. The third-party software is required to work with certain SRC components, and Juniper Networks supports issues associated with this software.

- Apache-Axis 1.4 (http://ws.apache.org/axis)
- Apache-Avalon 4.1.4 (http://avalon.apache.org)
- Beepcore-java 0.0.08 (http://www.beepcore.org)
- BouncyCastle CryptoAPI 1.33 (http://bouncycastle.org/java.html)
- Castor 0.9-AA (http://www.castor.org)
- Centos 4.9 (http://centos.org)
- GNUPROLOG for Java (http://gnuprologjava.sourceforge.net)
- ini4j 0.4 (http://ini4j.sourceforge.net)
- JacORB 2.3.1 (http://www.jacorb.org)
- Jakarta Commons Collections 3.1 (http://jakarta.apache.org/commons/collections)
- Jakarta Struts 1.1-Beta3 (http://jakarta.apache.org/struts/index.html)
- jax 0.0.15 (http://www.ibr.cs.tu-bs.de/projects/jasmin/jax.html)
- JBoss J2EE Server 4.2.1.GA (http://jboss.org)
- JDBM 0.12 (http://jdbm.sourceforge.net)
- JETTY 4.2.6 (http://jetty.mortbay.org)
- Jython 2.2 (http://www.jython.org)
- libart_lgpl 2.3.16-3 (http://www.linuxfromscratch.org/blfs/view/svn/general/libart_lgpl.html)
- libpng 1.2.7-3 (http://www.libpng.org/pub/png/libpng.html)
- mozilla rhino javascript engine 1.5 (http://www.mozilla.org/rhino)
- MySQL Cluster 7.1 (http://www.mysql.com/products/cluster)
- NetSNMP 5.4.1 (http://www.net-snmp.org)
- OmniORB 4.0.7 (http://omniorb.sf.net)
- omniORBpy-2.7 (http://omniorb.sf.net)
- OpenJDK 1.6.0_23 (http://openjdk.java.net)
- perl-Config-General 2.38-1 (http://search.cpan.org/dist/Config-General/General.pm)
- perl-RRD-Simple 1.44-1 (http://search.cpan.org/dist/RRD-Simple)
- perl-rrdtool 1.2.23-1 (http://rpmfind.net/linux/rpm2html/search.php?query=perl-rrdtool)
- PYSNMP (http://pysnmp.sourceforge.net)

- RRD Tool 1.2.23-3 (http://oss.oetiker.ch/rrdtool)
- RRD Bot 0.9 (http://memberwebs.com/stef/software/rrdbot)
- Terracotta 3.1.0 ES edition (http://www.terracotta.org/)

SRC Documentation and Release Notes

For a list of related SRC documentation, see http://www.juniper.net/techpubs/software/management/src/.

If the information in the latest release notes differs from the information in the documentation, follow the *SRC PE Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/customers/support/downloads/710059.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/

- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting support.html.

Revision History

September 2011—Revision 12, SRC Release 4.0.0