Configuring Secure Domain Routers on the Cisco IOS XR Software

Secure domain routers (SDRs) are a means of dividing a single physical system into multiple logically separated routers. SDRs are isolated from each other in terms of their resources, performance, and availability.

For complete descriptions of the SDR commands listed in this module, see Related Documents, on page 24. To locate documentation for other commands that might appear in the course of performing a configuration task, search online in *Cisco IOS XR Commands Master List for the Cisco CRS Router*.

Table 1: Feature History for Configuring Secure Domain Routers on Cisco IOS XR Software

Release	Modification
Release 3.3.0	This feature was introduced. Support included distributed route processor cards (DRPs) and DRP pairs, and SDR-specific software package activation.
Release 3.5.0	DSC migration functionality was improved.
Release 3.5.2	DSC migration was removed.
Release 3.6.3	Support for an SDR with DRPs within a single rack was added.
Release 3.9.0	Support was added for an SDR with DRPs on different racks.

This module contains the following topics:

Prerequisites for Working with Secure Domain Routers

Before configuring SDRs, the following conditions must be met:

Initial Setup

- The router must be running the Cisco IOS XR software , including a designated shelf controller (DSC).
- The root-system username and password must be assigned as part of the initial configuration.
- For more information on booting a router and performing initial configuration, see *Cisco IOS XR Getting Started Guide for the Cisco CRS Router*.

Required Cards for Each SDR

- Additional route processor (RP) pair, DRP or DRP pair must be installed in each line card (LC) chassis to manage each SDR in the system.
- For additional information on DRPs, refer to *Cisco CRS-1 Carrier Routing System 16-Slot Line Card Chassis System Description*. For instructions on installing DRPs, see *Installing the Cisco CRS-1 Carrier Routing System 16-Slot Line Card Chassis*.

Task ID Requirements

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Software Version Requirements

- Cisco IOS XR Software Releases 2.0, 3.0, and 3.2 support only one owner SDR. Multiple (non-owner) SDRs are not supported in these releases. The owner SDR cannot be added or removed from the configuration.
- Multiple SDRs, including non-owner SDRs, are supported on Cisco IOS XR Software Release 3.3.0 or higher.

Maximum SDR Configurations

- A maximum of eight SDRs are supported, including one owner SDR and up to seven non-owner SDRs.

Information About Configuring Secure Domain Routers

Review the sections in this module before configuring secure domain routers.

What Is a Secure Domain Router?

Cisco routers running the Cisco IOS XR software can be partitioned into multiple independent routers known as Secure Domain Routers (SDRs). An user defined SDR is termed as named-SDR.

SDRs are a means of dividing a single physical system into multiple logically separated routers. The SDRs are spawned as Virtual Machines (VMs). Each SDR performs routing functions similar to a physical router, but they share resources with the rest of the system. For example, the software image, configurations, protocols, and routing tables are unique to a particular SDR. Other system functions, including chassis-control and switch fabric, are shared with the rest of the system.

Owner SDR and Administration Configuration Mode

The *owner SDR* is created at system startup and cannot be removed. This owner SDR performs system-wide functions, including the creation of additional *non-owner* SDRs. You cannot create the owner SDR because it always exists, nor can you completely remove the owner SDR because it is necessary to manage the router. By default, all nodes in the system belong to the owner SDR.

The owner SDR also provides access to the administration EXEC and administration configuration modes. Only users with root-system privileges can access the administration modes by logging in to the primary route processor (RP) for the owner SDR (called the *designated shelf controller*, or DSC).

Administration modes are used for the following purposes:

- Create and remove additional non-owner SDRs.
- Assign nodes to the non-owner SDRs.
- View the configured SDRs in the system.
- View and manage system-wide resources and logs.

Note Administration modes cannot be used to configure the features within a non-owner SDR, or view the router configuration for a non-owner SDR. After the SDR is created, users must log into the non-owner SDR directly to change the local configuration and manage the SDR.

Non-Owner SDRs

To create a new non-owner SDR, the root-system user enters administration configuration mode, defines a new SDR name, and assigns a set of cards to that SDR. Only a user with root-system privileges can access the commands in administration configuration mode. Therefore, users without root-system privileges cannot create SDRs or assign cards to the SDRs.

After a non-owner SDR is created, the users configured on the non-owner SDR can log in and manage the router. The configuration for each non-owner SDR is separate from the owner SDR and can be accessed only by logging in to the non-owner SDR.

Note For information regarding support for non-owner SDRs in Cisco IOS XR software releases before release 3.9.0, see *Related Topics*.

SDR Access Privileges

Each SDR in a router has a separate AAA configuration that defines usernames, passwords, and associated privileges.

- Only users with root-system privileges can access the administration EXEC and administration configuration modes.
- Users with root-lr privileges can access only the non-owner SDR in which that username was created.
- Users with other access privileges can access features according to their assigned privileges for a specific SDR.

For more information about AAA policies, see the *Configuring AAA Services on the Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide for the Cisco CRS Router*.

Root-System Users

Users with root-system privileges have access to system-wide features and resources, including the ability to create and remove secure domain routers. The root-system user is created during the initial boot and configuration of the router.

The root-system user has the following privileges:

- Access to administration EXEC and administration configuration commands.
- Ability to create and delete non-owner SDRs.
- Ability to assign nodes (RPs, distributed route processors [DRPs], and line cards) to SDRs.
- Ability to create other users with similar or lower privileges.
- Complete authority over the chassis.
- Ability to log in to non-owner SDRs using admin plane authentication. Admin plane authentication allows the root-system user to log in to a non-owner SDR regardless of the configuration set by the root-lr user.
- Ability to install and activate software packages for all SDRs or for a specific SDR .
- Ability to view the following administration (admin) plane events (owner SDR logging system only):
  - Software installation operations and events.
  - System card boot operations, such as card booting notifications and errors, heartbeat-missed notifications, and card reloads.
  - Card alphanumeric display changes.
  - Environment monitoring events and alarms.

- Fabric control events.
- Upgrade progress information.

root-lr Users

Users with root-lr privileges can log in to an SDR only and perform configuration tasks that are specific to that SDR. The root-lr group has the following privileges:

- Ability to configure interfaces and protocols.
- Ability to create other users with similar or lower privileges on the SDR.
- Ability to view the resources assigned to their particular SDR.

The following restrictions apply to root-lr users:

- Users with root-lr privileges cannot enter administration EXEC or configuration modes.
- Users with root-lr privileges cannot create or remove SDRs.
- Users with root-lr privileges cannot add or remove nodes from an SDR.
- Users with root-lr privileges cannot create root-system users.
- The highest privilege a non-owner SDR user can have is root-lr.

Other SDR Users

Additional usernames and passwords can be created by the root-system or root-lr users to provide more restricted access to the configuration and management capabilities of the owner SDR or non-owner SDRs.

Designated Secure Domain Router Shelf Controller (DSDRSC)

In a router running Cisco IOS XR software, one RP is assigned the role of DSC. The DSC provides system-wide administration and control capability, including access to the administration EXEC and administration configuration modes. For more information on DSCs, refer to *Cisco IOS XR Getting Started Guide for the Cisco CRS Router*.

In each SDR, similar administration and control capabilities are provided by the designated secure domain router system controller (DSDRSC). Each SDR must include a DSDRSC to operate, and you must assign an RP or DRP to act as the DSDRSC.

Note In the owner SDR, the DSC also provides DSDRSC functionality.

DSCs and DSDRSCs

Designated Shelf Controller (DSC)

The primary and standby DSC is always an RP pair. By default, the DSC is also the DSDRSC for the owner SDR. The owner DSDRSCs cannot be removed from the SDR configuration, or assigned to a non-owner SDR.

For information on DSC assignment and initial router configuration, refer to *Cisco IOS XR Getting Started Guide for the Cisco CRS Router*.

Using a DRP or DRP Pair as the DSDRSC

Cisco Systems recommends the use of DRPs as the DSDRSC in non-owner SDRs. An SDR without an RP must designate a DRP or DRP as the potential DSDRSC.

To create a DRP DSDRSC in a non-owner SDR, you must configure a DRP or DRP pair as the primary node for that SDR. The following guidelines apply:

- Although a single DRP can be used as the DSDRSC, we recommend the use of a redundant DRP pair.
- To create a DRP pair and configure it as the DSDRSC, complete the instructions in Creating SDRs , on page 9.
- DRPs cannot be used as the DSC in the owner SDR. Only RPs can be used as the DSC in the owner SDR.
- DRPs cannot be assigned as the DSDRSC if an RP is present in the SDR. To assign a DRP as the DSDRSC, you must first remove any RPs from the SDR configuration, and then add the DRP or DRP pair as the primary node. After the DRP is assigned as the DSDRSC, the RPs can be added to the SDR. For more information, see *Related Topics*.

Note DRPs can also be used to provide additional processing capacity. For additional information on DRPs, see *Cisco CRS-1 Carrier Routing System 16-Slot Line Card Chassis System Description*. For instructions on installing DRPs, see *Installing the Cisco CRS-1 Carrier Routing System 16-Slot Line Card Chassis*. For information on using DRPs for additional processing capacity, see the *Process Placement on Cisco IOS XR Software* module in *Cisco IOS XR System Management Configuration Guide for the Cisco CRS Router*.

Using an RP Pair as the DSDRSC

RP pairs can also be used as the DSDRSC in non-owner SDRs.

- Single RPs cannot be used as the DSDRSC.
- Redundant RPs are installed in slots RP0 and RP1 of each line card chassis.
- To assign an RP pair as the DSDRSC, complete the instructions in How to Configure Secure Domain Routers, on page 9.

Note Although an RP pair can be used as the DSDRSC in non-owner SDRs, we recommend the use of a redundant DRP pair.

Removing a DSDRSC Configuration

There are two ways to remove a DSDRSC from an SDR:

- First remove all other nodes from the SDR configuration, and then remove the DSDRSC node. You cannot remove the DSDRSC node when other nodes are in the SDR configuration.
- Remove the entire SDR. Removing an SDR name deletes the SDR and moves all nodes back to the owner SDR inventory.

Default Configuration for New Non-Owner SDRs

By default, the configuration of a new SDR is blank. The first configuration step after creating an SDR is to log in to the new non-owner SDR using admin plane authentication and create a username and password. You can then log out of the SDR and log back in using the new username and password.

Note When logged in to a non-owner SDR using admin plane authentication, the admin configuration is displayed. However, admin plane authentication should be only used to configure a username and password for the non-owner SDR. To perform additional configuration tasks, log in with the username for the non-owner SDR.

Default Software Profile for SDRs

When a new non-owner SDR is created, the nodes assigned to that SDR are activated with the default software package profile. The default software profile is defined by the last install operation that did not specify an SDR.

To view the default software profile, use the **show install active summary** command in administration EXEC mode. Any new nodes that are configured to become a part of an SDR will boot with the default software profile listed in the output of this command.

```
RP/0/RP0/CPU0:router# show install active summary

Wed Dec 24 01:47:02.076 PST
  Active Packages:
    disk1:hfr-infra-test-3.8.0.25I
    disk1:hfr-fpd-3.8.0.25I
    disk1:hfr-doc-3.8.0.25I
    disk1:hfr-diags-3.8.0.25I
    disk1:hfr-mgbl-3.8.0.25I
    disk1:hfr-mcast-3.8.0.25I
    disk1:hfr-mpls-3.8.0.25I
    disk1:comp-hfr-mini-3.8.0.25I
```

Note For detailed instructions to add and activate software packages, see the *Managing Cisco IOS XR Software Packages* module of *Cisco IOS XR Getting Started Guide for the Cisco CRS Router*. See also the *Software Package Management Commands on the Cisco IOS XR Software* module of *Cisco IOS XR System Management Command Reference for the Cisco CRS Router*.

High Availability Implications

The sections in this module describe various high availability implications.

Fault Isolation

Because the CPU and memory of an SDR are not shared with other SDRs, configuration problems that cause out-of-resources conditions in one SDR do not affect other SDRs.

Rebooting an SDR

Each non-owner SDR can be rebooted independently of the other SDRs in the system. If you reboot the owner SDR, however, then all non-owner SDRs in the system automatically reboot, because the non-owner SDRs rely on the owner SDR for basic chassis management functionality.

Note The DSDRSC of the owner SDR is also the DSC of the entire system.

DSDRSC Redundancy

To achieve full redundancy, each SDR must be assigned two cards: one to act as the primary DSDRSC and one RP or DRP to act as a standby DSDRSC.

We recommend the use of DRP pairs as DSDRSC for all non-owner SDRs the system.

Cisco IOS XR Software Package Management

Software packages are added to the DSC of the system from administration EXEC mode. Once added, a package can be activated for all SDRs in the system or for a specific SDR . For detailed instructions regarding software package management, see the *Upgrading and Managing Cisco IOS XR Software* module of *Cisco IOS XR System Management Configuration Guide for the Cisco CRS Router*. See also the *Software Package Management Commands on the Cisco IOS XR Software* module of *Cisco IOS XR System Management Command Reference for the Cisco CRS Router*.

Note SDR-specific activation is supported for specific packages and upgrades, such as optional packages and SMUs. Packages that do not support SDR-specific activation can only be activated for all SDRs in the system.

- To access **install** commands, you must be a member of the root-system user group with access to the administration EXEC mode.
- Most **show install** commands can be used in the EXEC mode of an SDR to view the details of the active packages for that SDR.

Restrictions For SDR Creation and Configuration

The following restrictions apply to SDR creation and configuration:

- DRPs are supported for the DSDRSC.
- We recommend the configuration of DRP pairs as the DSDRSC for all non-owner SDRs, as described in Using a DRP or DRP Pair as the DSDRSC, on page 6.
- Single RPs are not supported for the DSDRSC. RPs must be installed and configured in redundant pairs.
- Admin plane events are displayed only on the non-owner SDR.
- Some admin plane debug events are not displayed on the owner SDR. For example, a non-owner card cannot send debug events to the DSC, which limits the debugging of administration processes to the non-owner SDR.

How to Configure Secure Domain Routers

To create an SDR, configure an SDR name and then add nodes to the configuration. At least one node in each SDR must be explicitly configured as the DSDRSC. After the SDR is created, you can add or remove additional nodes and create a username and password for the SDR.

Creating SDRs

To create a non-owner SDR, create an SDR name, add a DSDRSC, and then add additional nodes to the configuration. After the SDR is created, you can create a username and password for the SDR to allow additional configuration.

Note The Cisco CRS-1 supports a maximum of eight SDRs, including one owner SDR and up to seven non-owner SDRs.

The 4-slot line card chassis does not support the creation of multiple SDRs.

Before You Begin

The procedures in this section can be performed only on a router that is already running Cisco IOS XR software. For instructions to boot a router and perform the initial configuration, see *Cisco IOS XR Getting Started Guide for the Cisco CRS Router*. When a router is booted, the owner SDR is automatically created, and cannot be removed. This also includes instructions to create the owner SDR username and password.

SUMMARY STEPS

1. **admin**
2. **configure**
3. **pairing** *pair-name*
4. **location** *partially-qualified-nodeid partially-qualified-nodeid*
5. **exit**
6. **sdr** *sdr-name*
7. Do one of the following:
   - **pair** *pair-name* **primary**
   - **location** *partially-qualified-nodeid* **primary**
8. Do one of the following:
   - **location** *partially-qualified-nodeid*
   - **location** *pair-name*
9. Repeat Step 8, on page 12 as needed to add nodes to an SDR.
10. **exit**
11. Repeat Step 3, on page 11 through Step 10, on page 12 through as needed.
12. **commit**
13. Create a username and password for the new SDR.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters administration EXEC mode.
Step 2	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Enters administration configuration mode.

	Command or Action	Purpose
Step 3	**pairing** *pair-name* **Example:** `RP/0/RP0/CPU0:router(admin-config)# pairing drp1`	(Optional) Enter DRP pairing configuration mode. If the DRP name does not exist, the DRP pair is created when you add nodes, as described in the following step. • *pair-name* can be between 1 and 32 alphanumeric characters. The characters '_' or '-' are also allowed. All other characters are invalid. DRP pairs are used as the DSDRSC for a non-owner SDR. **Note** Although a single DRP can be used as the DSDRSC in a non-owner SDR, Cisco systems recommends that two redundant DRPs be installed and assigned to the SDR. **Note** DRPs can also be added to an SDR to provide additional processing capacity. See *Related Topics* for more information on DRP installation and configuration.
Step 4	**location** *partially-qualified-nodeid partially-qualified-nodeid* **Example:** `RP/0/RP0/CPU0:router(admin-config-pairing:drp1)# location 0/3/* 0/4/*`	(Optional) Specifies the location of the DRPs in a DRP pair. The *partially-qualified-nodeid* argument is entered in the *rack/slot/** notation. Node IDs are always specified at the slot level, so the wildcard (*) is used to specify the CPU.
Step 5	**exit** **Example:** `RP/0/RP0/CPU0:router(admin-config-pairing:drp1)# exit`	(Optional) Exits the DRP pairing configuration mode and returns to Administration configuration mode. Complete this step only if you created a DRP pair.
Step 6	**sdr** *sdr-name* **Example:** `RP/0/RP0/CPU0:router(admin-config)# sdr rname`	Enters the SDR configuration sub-mode for the specified SDR. • If this SDR does not yet exist, it is created when you add a node, as described in step 7. • If this SDR existed previously, you can add additional slots as described in step 7 and step 8. • Only alphanumeric characters, "-", and "_" are valid characters to include in the *sdr-name* argument.
Step 7	Do one of the following: • **pair** *pair-name* **primary** • **location** *partially-qualified-nodeid* **primary** **Example:**	Specifies a DSDRSC for the non-owner SDR. You can assign a redundant DRP pair, an RP pair, or a single DRP as the DSDRSC. You cannot assign a single RP as the DSDRSC. Every SDR must contain a DSDRSC. • We recommend the use of DRP pairs as the DSDRSC for all non-owner SDRs.

	Command or Action	Purpose

	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# pair drp1 primary`
	or
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# location 0/0/* primary`
	or
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# location 0/RP*/* primary`
		• The **primary** keyword configures the RPs, DRP pair, or DRP as the DSDRSC. If the **primary** keyword is not used, the node is assigned to the SDR, but it is not be the DSDRSC.
		• If an RP is already assigned to the SDR, it must be removed before a DRP or DRP pair can be assigned as the DSDRSC.

Step 8	Do one of the following:
	• **location** *partially-qualified-nodeid*
	• **location** *pair-name*
	Example:
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# location 0/0/*`
	or
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# location drp1`
	or
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# location 0/RP*/*`
		Adds additional nodes, DRP pairs, or RP pairs to the SDR.

Step 9	Repeat Step 8, on page 12 as needed to add nodes to an SDR.	Adds additional nodes to the SDR.
Step 10	**exit** **Example:** `RP/0/RP0/CPU0:router (admin-config-sdr:rname)# exit`	(Optional) Exits the SDR configuration submode and returns to Administration configuration mode. **Note** Complete this step only if you need to create additional SDRs.
Step 11	Repeat Step 3, on page 11 through Step 10, on page 12 through as needed.	Creates additional SDRs.
Step 12	**commit**	
Step 13	Create a username and password for the new SDR.	

Adding Nodes to a Non-Owner SDR

When adding nodes to an existing non-owner SDR, the following rules apply:

- By default, all nodes in a new system belong to the owner SDR. When a node is assigned to a non-owner SDR, the node is removed from the owner SDR inventory and added to the non-owner SDR.
- When a node is removed from a non-owner SDR, it is automatically returned to the owner SDR inventory.
- To add a node that already belongs to another non-owner SDR, you must first remove the node from the other SDR, and then reassign it to the new SDR.
- You cannot assign the DSC or standby DSC to a non-owner SDR. The DSC and standby DSC can cannot be removed and assigned to a non-owner SDR.
- Note the following points about DSDRSC support:
  - DRPs and DRP pairs are supported.
  - RPs can only be added in redundant pairs.

Adding Nodes to an SDR

This task explains how add nodes to an SDR.

SUMMARY STEPS

1. **admin**
2. **configure**
3. **sdr** *sdr-name*
4. Do one of the following:
   - **location** *partially-qualified-nodeid*
   - **location** *pair-name*
5. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters administration EXEC mode.

	Command or Action	Purpose
Step 2	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Enters administration configuration mode.
Step 3	**sdr** *sdr-name* **Example:** `RP/0/RP0/CPU0:router(admin-config)# sdr rname`	Enters the SDR configuration submode for the specified SDR. • *sdr-name* is the name assigned to the SDR.

Step 4	Do one of the following:
	• **location** *partially-qualified-nodeid*
	• **location** *pair-name*
	
	Example:
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# location 0/0/*`
	or
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# location drp1`
	or
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# location 0/RP*/*`
		Adds additional nodes, DRP pairs, or RP pairs to an SDR.

Step 5	Use one of the following commands:
	• **end**
	• **commit**
	
	Example:
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# end`
	or
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		◦ Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		◦ Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

	Command or Action	Purpose
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Removing Nodes and SDRs

When removing a node or an entire SDR, the following rules apply:

- When a node is removed from a non-owner SDR, it is automatically returned to the owner SDR inventory.
- To remove a DSDRSC, first remove the other nodes in the SDR and then remove the DSDRSC. This rule does not apply when the entire SDR is removed.
- If all nodes are removed from a non-owner SDR, the SDR name is also removed.
- To remove all nodes, including the DSDRSC, remove the SDR name. All nodes are returned to the owner SDR inventory.
- You must first remove a node from a non-owner SDR before it can be reassigned to another non-owner SDR.
- To remove a node from the owner SDR inventory, assign the node to an non-owner SDR.
- The owner SDR cannot be removed, and the owner DSDRSC (DSC) cannot be removed.

Removing Nodes from an SDR

This task explains how remove nodes from an SDR.

SUMMARY STEPS

1. **admin**
2. **configure**
3. **sdr** *sdr-name*
4. Do one of the following:
   - **no location** *partially-qualified-nodeid*
   - **no location** *pair-name*
5. Use one of the following commands:
   - **end**
   - **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters administration EXEC mode.
Step 2	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Enters administration configuration mode.
Step 3	**sdr** *sdr-name* **Example:** `RP/0/RP0/CPU0:router(admin-config)# sdr rname`	Enters the SDR configuration submode for the specified SDR.

Step 4	Do one of the following:
	• **no location** *partially-qualified-nodeid*
	• **no location** *pair-name*
	
	Example:
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# no location 0/0/*`
	or
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# no location drp1`
	or
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# no location 0/RP*/*`
		Removes a node, DRP pair, or RP pair from a non-owner SDR.
		• When a node is removed from an SDR, it is automatically added to the owner SDR inventory. This node may now be assigned to a different SDR, as described in Adding Nodes to a Non-Owner SDR, on page 13.
		• Removing all the slots from an SDR deletes that SDR.

Step 5	Use one of the following commands:
	• **end**
	• **commit**
	
	Example:
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# end`
	or
	`RP/0/RP0/CPU0:router(admin-config-sdr:rname)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		◦ Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.

	Command or Action	Purpose
		◦ Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Removing an SDR

This section provides instructions to remove a secure domain router from your router. To remove an SDR, you can either remove all the nodes in the SDR individually or remove the SDR name. This section contains instructions to remove the SDR name and return all nodes to the owner SDR inventory.

Note The owner SDR cannot be removed. Only non-owner SDRs can be removed.

SUMMARY STEPS

1. **admin**
2. **configure**
3. **no sdr** *sdr-name*
4. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters administration EXEC mode.
Step 2	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Enters administration configuration mode.
Step 3	**no sdr** *sdr-name* **Example:**	Removes the specified SDR from the current owner SDR. **Note** All slots belonging to that SDR return to the owner SDR inventory.

	Command or Action	Purpose
	`RP/0/RP0/CPU0:router(admin-config)# no sdr rname`	
Step 4	**commit**	

Configuring a Username and Password for a Non-Owner SDR

After you create an SDR, you can create a username and password on that SDR. When you assign root-lr privileges to that username, the user can administer the non-owner SDR and create additional users if necessary.

Note Only users with root-system privileges can access administration modes to add or remove SDRs. SDR users cannot add or remove SDRs.

To create a username and password for the new non-owner SDR.

1. On the owner SDR, enable admin plane authentication. This allows you to log in to the non-owner SDR and create local usernames and passwords.
2. Log in to the non-owner SDR.
3. Configure a new username and password on the non-owner SDR. Assign the username to the root-lr group to allow the creation of additional usernames on that SDR.
4. To verify the new username, log out and log back in to the non-owner SDR using the new username and password.
5. Provide the username and password to the SDR user.

Complete the following steps to create usernames and passwords on a non-owner SDR.

SUMMARY STEPS

1. Connect a terminal to the console port of the DSC (DSDRSC of the owner SDR).
2. **admin**
3. **configure**
4. **aaa authentication login remote local**
5. **commit**
6. Connect a terminal to the console port of the non-owner SDR DSDRSC.
7. Log in to the non-owner SDR using admin plane authentication.
8. **configure**
9. **username** *username*
10. **secret** *password*
11. **group root-lr**
12. **commit**
13. **exit**
14. Log back in with the SDR administrator username and password you created.
15. Provide the new username and password to the user.
16. Disable admin plane authentication.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Connect a terminal to the console port of the DSC (DSDRSC of the owner SDR).	**Note** If an IP address has not yet been assigned to the Management Ethernet port, you must connect a terminal directly to the console port of the DSC.
Step 2	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters administration EXEC mode.
Step 3	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Enters administration configuration mode.
Step 4	**aaa authentication login remote local** **Example:** `RP/0/RP0/CPU0:router(admin-config)# aaa authentication login remote local`	Enables admin plane authentication. • The **remote** keyword specifies a method list that uses remote non-owner SDR for authentication. • The **local** keyword specifies a method list that uses the local username database method for authentication. The local authentication cannot fail because the system always ensures that at least one user is present in the local database, and a rollover cannot happen beyond the local method.

	Command or Action	Purpose
		Note You can also use other methods to enable AAA system accounting, such as TACACS+ or RADIUS servers. See the *Configuring AAA Services on the Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide for the Cisco CRS Router* for more information. **Note** When logged in to a non-owner SDR using admin plane authentication, the admin configuration is displayed. However, admin plane authentication should only be used to configure a username and password for the non-owner SDR. To perform additional configuration tasks, log in with the username for the non-owner SDR, as described in the following steps.
Step 5	**commit**	
Step 6	Connect a terminal to the console port of the non-owner SDR DSDRSC.	**Note** A terminal server connection is required for Telnet connections to the console port because an IP address has not yet been assigned to the management Ethernet port.

Step 7	Log in to the non-owner SDR using admin plane authentication.
	Example:
	`Username:xxxx@admin`
	`Password:pppp`
		Logs a root-system user into the SDR using admin plane authentication.
		Note When prompted for the Username, use your username followed by **@admin** .

Step 8	**configure**	
Step 9	**username** *username* **Example:** `RP/0/RP0/CPU0:router(config)# username user1`	Defines an SDR username and enters username configuration mode. The *username* argument can be only one word. Spaces and quotation marks are not allowed.
Step 10	**secret** *password* **Example:** `RP/0/RP0/CPU0:router(config-un)# secret 5 XXXX`	Defines a password for the user.
Step 11	**group root-lr** **Example:** `RP/0/RP0/CPU0:router(config-un)# group root-lr`	Adds the user to the predefined root-lr group. **Note** Only users with root-system authority or root-lr authority may use this option.
Step 12	**commit**	
Step 13	**exit** **Example:** `RP/0/RP0/CPU0:router# exit`	Closes the active terminal session and log off the router.

	Command or Action	Purpose

Step 14	Log back in with the SDR administrator username and password you created.
	
	Example:
	`Press RETURN to get started.`
	`Username:xxxx`
	`Password:ppppp`
		Logs back in with the SDR administrator username and password you created. This username is used to configure the secure domain router and create other users with fewer privileges.
		• This step verifies proper SDR administrator username and password configuration.
		• After you create the SDR username and password, you need to provide the SDR username and password to the operators who will use that SDR.

Step 15	Provide the new username and password to the user.	—
Step 16	Disable admin plane authentication.	See *Related Topics* for more information.

Disabling Remote Login for SDRs

When you disable admin plane authentication, the admin username cannot be used to log in to non-owner SDRs. Only local SDR usernames can be used to log into the SDR.

SUMMARY STEPS

1. **admin**
2. **configure**
3. **no aaa authentication login remote local**
4. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters administration EXEC mode.
Step 2	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Enters administration configuration mode.

	Command or Action	Purpose
Step 3	**no aaa authentication login remote local** **Example:** `RP/0/RP0/CPU0:router(admin-config)# no aaa authentication login remote local`	Disables remote login.
Step 4	**commit**	

Configuration Examples for Secure Domain Routers

Creating a New SDR: Example

The following example shows how to create a new SDR:

```
admin
  configure
    pairing drp1
      location 0/3/* 0/4/*
      exit
    sdr rname2
      pair pair1 primary
      location 0/0/*
      end
```

Adding Nodes to an SDR: Example

The following example shows how to add nodes to an SDR:

```
admin
  configure
    sdr rname2
      location 0/0/*
      end
```

Removing Notes from an SDR: Example

The following example shows how to remove nodes from an SDR:

```
admin
  configure
    sdr rname2
      no location 0/0/*
      end
```

Removing an SDR from the Router: Example

The following example shows how to remove an SDR from the router:

```
admin
  configure
    no sdr rname2
    end
```

Configuring a Username and Password for a Non-Owner SDR: Example

The following example shows how to connect to the DSC of the owner SDR:

```
admin
  configure
    aaa authentication login remote local
    end
```

To continue, connect a terminal to the console port of the non-owner SDR DSDRSC.

```
Username:xxxx@admin
  Password:xxxx
  configure
   username user1
    secret 5 XXXX
    group root-lr
    end
   exit

  Press RETURN to get started.
  Username:user1
  Password:xxxxx
```

Disabling Remote Login for SDRs: Example

The following example shows how to disable remote login for an SDR:

```
admin
  configure
    no aaa authentication login remote local
    end
```

Additional References

The following sections provide references related to SDR configuration.

Related Documents

Related Topic	Document Title
SDR command reference	*Secure Domain Router Commands on the Cisco IOS XR Software* module of *Cisco IOS XR System Management Command Reference for the Cisco CRS Router*
DRP pairing command reference	*Distributed Route Processor Commands on the Cisco IOS XR Software* module of *Cisco IOS XR System Management Command Reference for the Cisco CRS Router*
Initial system bootup and configuration information for a router using the Cisco IOS XR software	*Cisco IOS XR Getting Started Guide for the Cisco CRS Router*
DRP description and requirements	*Cisco CRS-1 Carrier Routing System 16-Slot Line Card Chassis System Description*
Instructions to install DRP and DRP PLIM cards	*Installing the Cisco CRS-1 Carrier Routing System 16-Slot Line Card Chassis*
Cisco IOS XR master command reference	*Cisco IOS XR Commands Master List for the Cisco CRS Router*
Information about user groups and task IDs	*Configuring AAA Services on the Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide for the Cisco CRS Router*
Cisco IOS XR interface configuration commands	*Cisco IOS XR Interface and Hardware Component Command Reference for the Cisco CRS Router*
Information about configuring interfaces and other components on the Cisco CRS-1 from a remote Craft Works Interface (CWI) client management application	*Cisco Craft Works Interface User Guide*
Information about AAA policies, including instructions to create and modify users and username access privileges	*Configuring AAA Services on the Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide for the Cisco CRS Router*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html