



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 23. 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 XR 12000 Series Router*.

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

Release	Modification
Release 3.2	This feature was introduced.
Release 3.3.0	The term Logical Router (LR) was changed to Secure Domain Router (SDR). Support was added for SDR-specific software package activation.

This module contains the following topics:

- [Prerequisites for Working with Secure Domain Routers](#), page 1
- [Information About Configuring Secure Domain Routers](#), page 2
- [How to Configure Secure Domain Routers](#), page 10
- [Configuration Examples for Secure Domain Routers](#), page 21
- [Additional References](#), page 22

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 XR 12000 Series Router*.

Required Cards for Each SDR

- Additional route processor (RP) or RP pair must be installed to manage each SDR in the system.

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

- Multiple SDRs, including non-owner SDRs, are supported on Cisco IOS XR Software Release 3.2 or higher.

Maximum SDR Configurations

- We recommend a maximum of four SDRs, including one owner SDR and up to three 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, and independent routers known as *secure domain routers* (SDRs). SDRs are a means of dividing a single physical system into multiple logically separated routers. They perform routing functions similar to a physical router, but they share resources with the rest of the system. For example, the software, the configurations, the protocols, and the routing tables, which are assigned, are unique to a particular SDR. Other functions, such as 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.

Related Topics

[SDR Access Privileges, on page 3](#)

[Non-Owner SDRs, on page 3](#)

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*.

Related Topics

[SDR Access Privileges, on page 3](#)

[Prerequisites for Working with Secure Domain Routers, on page 1](#)

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 XR 12000 Series Router*.

Related Topics

[Root-System Users, on page 4](#)

[root-lr Users, on page 5](#)

[Other SDR Users, on page 5](#)

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 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.

Related Topics

[Configuring a Username and Password for a Non-Owner SDR, on page 17](#)

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 XR 12000 Series 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 to act as the DSDRSC.

DSC and DSDRSCs

You can use a single RP or a redundant RP pair as the DSDRSC for each SDR. Redundant RP pairs must be installed in adjacent redundancy slots. The adjacent redundancy slots are as follows:

- Slot 0 and Slot 1
- Slot 2 and Slot 3
- Slot 4 and Slot 5
- Slot 6 and Slot 7
- Slot 8 and Slot 9
- Slot 10 and Slot 11

- Slot 12 and Slot 13
- Slot 14 and Slot 15

Review the additional information in this section for restrictions regarding RP usage.



Note Only two RPs can be operational in any SDR.

Designated Shelf Controller (DSC)

- The first RP to be booted with the Cisco IOS XR software will become the designated shelf controller (DSC) for the router. This DSC is also the DSDRSC for the owner SDR. The DSC (owner DSDRSC) cannot be removed from the router configuration or reassigned to another SDR. For more information on bringing up a router for the first time, see *Cisco IOS XR Getting Started Guide for the Cisco XR 12000 Series Router*.
- The second RP can be used as the standby DSC. The standby DSC is also the standby DSDRSC for the owner SDR. The RP becomes the standby DSC if the following conditional are met:
 - The RP is installed in an adjacent redundancy slot to the DSC.
 - The RP is booted with the Cisco IOS XR software.
- Additional RPs can be installed in the router, but they will be non-operational until the following conditions are met:
 - The additional RPs are booted with the Cisco IOS XR software.
 - The RPs are added to a non-owner SDR configuration.

Selecting the DSDRSC

- Up to two RPs can be added to a non-owner SDR configuration.
- The first RP running the Cisco IOS XR software that is added to the SDR configuration will become the DSDRSC.
- If a second RP running the Cisco IOS XR software is installed in an adjacent redundancy slot, it will become the standby DSDRSC when added to the SDR configuration.
- If two RPs running the Cisco IOS XR software are installed in adjacent redundancy slots and are added to a new SDR at the same time, they automatically elect a DSDRSC and standby DSDRSC between them.
- Any RPs added to the SDR that are not in the adjacent redundancy slot to the DSDRSC are non-operational.

**Note**

Additional RPs that are not the DSDRSC or standby DSDRSC can be added to an SDR configuration, but they will not be operational. These additional RPs will repetitively reset to prevent them from booting and interfering with other cards in the SDR. In addition, the DSC console displays repetitive error messages. We recommend that you either remove RP cards or assign them to a different SDR.

- Once a DSDRSC is configured for an SDR, an RP installed in the adjacent redundancy slot can be assigned only to that SDR because adjacent redundancy slots form a redundancy pair that cannot be separated by SDR boundaries. For example, if the DSDRSC is installed in slot 2, an RP installed in slot 3 can be assigned only to the same SDR (as the standby DSDRSC).
- RPs that are installed on slots that are not adjacent redundancy slots can be assigned to different SDRs. For example, two RPs installed in slot 0 and slot 1 can be configured only as the DSDRSC and standby DSDRSC because they are installed in adjacent redundancy slots. However, two RPs installed in slot 1 and slot 2 can be used for different SDRs because these are not adjacent redundancy slots.

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.

Related Topics

[Removing Nodes and SDRs, on page 14](#)

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/0/0/CPU0:router(admin)# show install active summary
```

```
Default Profile:
SDRs:
  Owner
  sdr1
Active Packages:
  disk0:c12k-sbc-3.3.0
  disk0:c12k-diags-3.3.0
  disk0:c12k-mgbl-3.3.0
  disk0:c12k-mcast-3.3.0
  disk0:c12k-mpls-3.3.0
  disk0:c12k-k9sec-3.3.0
  disk0:c12k-mini-3.3.0
```

**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 XR 12000 Series 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 XR 12000 Series Router*.

Related Topics

[Configuring a Username and Password for a Non-Owner SDR](#), on page 17

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 to act as a standby DSDRSC.

You can assign two redundant RP cards to each SDR. DRPs are not supported.

Related Topics

[DSC and DSDRSCs, on page 5](#)

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 XR 12000 Series 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 XR 12000 Series 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.

Related Topics

[Default Configuration for New Non-Owner SDRs, on page 7](#)

Restrictions For SDR Creation and Configuration

The following restrictions apply to SDR creation and configuration:

- DRPs are not supported.
- Single RPs and redundant RP pairs are supported for the DSDRSC.
- 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. The DSDRSC is created automatically when you add an RP to the configuration. 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 an RP (that can act as DSDRSC) or 2 RPs in adjacent redundancy slots (that can act as the DSDRSC & standby DSDRSC) and then add additional (non-RP) nodes to the configuration.

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 XR 12000 Series Router*. When a router is booted, the owner SDR is automatically created and cannot be removed. This guide also includes instructions to create owner SDR username and password.

SUMMARY STEPS

1. **admin**
2. **configure**
3. **sdr** *sdr-name*
4. **location** *partially-qualified-nodeid*
5. (Optional) **location** *partially-qualified-nodeid*
6. **location** *partially-qualified-nodeid*
7. Repeat [Step 6, on page 11](#) as needed to add additional nodes to the SDR.
8. **exit**
9. Repeat [Step 3, on page 11](#) through [Step 7, on page 12](#) as needed to create additional SDRs.
10. **commit**
11. (Optional) Create a username and password for the new SDR.

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	<p>configure</p> <p>Example:</p> <pre>RP/0/0/CPU0:router(admin)# configure</pre>	Enters administration configuration mode.
Step 3	<p>sdr sdr-name</p> <p>Example:</p> <pre>RP/0/0/CPU0:router(admin-config)# sdr rname</pre>	<p>Enters administration configuration mode for the specified SDR.</p> <ul style="list-style-type: none"> • If this SDR does not yet exist, it is created when you add a node as described in the following step. • If this SDR existed previously, complete the following steps to add additional nodes. <p>Note We recommend a maximum of four SDRs, including one owner SDR and up to three non-owner SDRs.</p>
Step 4	<p>location partially-qualified-nodeid</p> <p>Example:</p> <pre>RP/0/0/CPU0:router(admin-config-sdr:rname)# location 0/0/*</pre>	<p>Assigns an RP node as the DSDRSC for the non-owner SDR. You can assign a single RP or a redundant RP pair as the DSDRSC.</p> <ul style="list-style-type: none"> • The first RP you assign to the SDR becomes the DSDRSC. • To add a redundant standby RP to the configuration, a second RP must be installed in the adjacent redundancy slot and added to the SDR configuration. For information on redundancy slots, see <i>Related Topics</i>. See Step 5, on page 11 for instructions to add an additional RP to the configuration. • The value of the <i>partially-qualified-nodeid</i> argument is entered in the <i>rack/slot/*</i> notation. The node ID is specified at the slot level, so the wildcard (*) is used to specify the CPU. • DRPs are not supported.
Step 5	<p>location partially-qualified-nodeid</p> <p>Example:</p> <pre>RP/0/0/CPU0:router(admin-config-sdr:rname)# location 0/1/*</pre>	<p>(Optional)</p> <p>Assigns a second RP to act as the standby DSDRSC. If an RP is in an adjacent redundancy slot to the DSDRSC, then the RP automatically becomes the standby DSDRSC.</p> <ul style="list-style-type: none"> • The value of the <i>partially-qualified-nodeid</i> argument is entered in the <i>rack/slot/*</i> notation. The node ID is specified at the slot level, so the wildcard (*) is used to specify the CPU. • Although single RPs are supported, we recommend the use of a redundant RP pair: one to act as the DSDRSC and the second to act as a standby DSDRSC.
Step 6	<p>location partially-qualified-nodeid</p> <p>Example:</p>	<p>Assigns additional nodes to the SDR. Enter the value of the <i>partially-qualified-nodeid</i> argument to specify a single node. The value of the <i>nodeid</i> argument is entered in the <i>rack/slot/*</i> notation. Node IDs are always specified at the slot level, so the wildcard (*) is used to specify the CPU.</p>

	Command or Action	Purpose
	RP/0/0/CPU0:router(admin-config-sdr:rname) # location 0/5/*	
Step 7	Repeat Step 6, on page 11 as needed to add additional nodes to the SDR.	Adds additional nodes to the SDR.
Step 8	exit Example: RP/0/0/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 9	Repeat Step 3, on page 11 through Step 7, on page 12 as needed to create additional SDRs.	Creates additional SDRs.
Step 10	commit	
Step 11	Create a username and password for the new SDR.	(Optional)

Related Topics

[DSC and DSDRSCs, on page 5](#)

[Adding Nodes to a Non-Owner SDR, on page 12](#)

[Configuring a Username and Password for a Non-Owner SDR, on page 17](#)

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 are not supported.
 - RPs can be added individually or in redundant sets. Only two RPs (if installed in the adjacent redundancy slots) can function in each SDR.

Related Topics

[Removing Nodes and SDRs, on page 14](#)

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. **location** *partially-qualified-nodeid*
5. Use one of the following commands:
 - **end**
 - **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	admin Example: RP/0/0/CPU0:router# admin	Enters administration EXEC mode.
Step 2	configure Example: RP/0/0/CPU0:router(admin)# configure	Enters administration configuration mode.
Step 3	sdr <i>sdr-name</i> Example: RP/0/0/CPU0:router(admin-config)# sdr rname	Enters the SDR configuration mode for the specified SDR. • <i>sdr-name</i> is the name assigned to the SDR.
Step 4	location <i>partially-qualified-nodeid</i> Example: RP/0/0/CPU0:router(admin-config-sdr:rname)# location 0/5/*	Adds additional nodes to the SDR. • Enter the value of the <i>partially-qualified-nodeid</i> argument to specify a single node. The value of the <i>nodeid</i> argument is entered in the <i>rack/slot/*</i> notation. Node IDs are always specified at the slot level, so the wildcard (*) is used to specify the CPU. • If you add an RP installed in a redundancy slot next to the DSDRSC, then the second RP becomes the standby DSDRSC.
Step 5	Use one of the following commands:	Saves configuration changes.

Command or Action	Purpose
<ul style="list-style-type: none"> • end • commit <p>Example:</p> <pre>RP/0/0/CPU0:router(admin-config-sdr:rname) # end or RP/0/0/CPU0:router(admin-config-sdr:rname) # commit</pre>	<ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <p style="margin-left: 20px;">Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</p> <ul style="list-style-type: none"> ◦ 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. • Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.

Related Topics

[DSC and DSDRSCs, on page 5](#)

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 a 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. **no location partially-qualified-nodeid**
5. Use one of the following commands:
 - **end**
 - **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	admin Example: RP/0/0/CPU0:router# admin	Enters administration EXEC mode.
Step 2	configure Example: RP/0/0/CPU0:router(admin)# configure	Enters administration configuration mode.
Step 3	sdr sdr-name Example: RP/0/0/CPU0:router(admin-config)# sdr rname	Enters the SDR configuration mode for the specified SDR.
Step 4	no location partially-qualified-nodeid Example: RP/0/0/CPU0:router(admin-config-sdr:rname2)# no location 0/0/*	Removes a node from a non-owner SDR. <ul style="list-style-type: none"> • 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. • Removing all the slots from an SDR deletes that SDR.
Step 5	Use one of the following commands: <ul style="list-style-type: none"> • end • commit 	Saves configuration changes. <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre>

	Command or Action	Purpose
	<p>Example:</p> <pre>RP/0/0/CPU0:router(admin-config-sdr:rname) # end or RP/0/0/CPU0:router(admin-config-sdr:rname) # commit</pre>	<ul style="list-style-type: none"> ◦ 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. <ul style="list-style-type: none"> • Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.

Related Topics

[Adding Nodes to an SDR, on page 13](#)

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/0/0/CPU0:router# admin	Enters administration EXEC mode.
Step 2	configure Example: RP/0/0/CPU0:router(admin)# configure	Enters administration configuration mode.
Step 3	no sdr sdr-name Example: RP/0/0/CPU0:router(admin-config)# no sdr rname	Removes the specified SDR from the current owner SDR. Note All slots belonging to that SDR return to the owner SDR inventory.
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-Ir 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-Ir 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/0/0/CPU0:router# admin	Enters administration EXEC mode.
Step 3	configure Example: RP/0/0/CPU0:router(admin)# configure	Enters administration configuration mode.
Step 4	aaa authentication login remote local Example: RP/0/0/CPU0:router(admin-config)# aaa authentication login remote local	Enables admin plane authentication. <ul style="list-style-type: none"> • 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
		<p>Note You can also use other methods to enable AAA system accounting, such as TACACS+ or RADIUS servers. See the <i>Configuring AAA Services on the Cisco IOS XR Software</i> module of <i>Cisco IOS XR System Security Configuration Guide for the Cisco XR 12000 Series Router</i> for more information.</p> <p>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.</p>
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 <i>username</i> Example: RP/0/0/CPU0:router(config)# username user1	Defines an SDR username and enters username configuration mode. The <i>username</i> argument can be only one word. Spaces and quotation marks are not allowed.
Step 10	secret <i>password</i> Example: RP/0/0/CPU0:router(config-un)# secret 5 XXXX	Defines a password for the user.
Step 11	group <i>root-lr</i> Example: RP/0/0/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/0/0/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. <ul style="list-style-type: none"> • 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 <i>Related Topics</i> for more information.

Related Topics

[Disabling Remote Login for SDRs, on page 20](#)

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/0/0/CPU0:router# admin	Enters administration EXEC mode.

	Command or Action	Purpose
Step 2	configure Example: RP/0/0/CPU0:router(admin)# configure	Enters administration configuration mode.
Step 3	no aaa authentication login remote local Example: RP/0/0/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
sdr rname
location 0/0/*
location 0/1/*
location 0/5/*
end
```

Adding Nodes to an SDR: Example

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

```
admin
configure
sdr rname2
location 0/5/*
end
```

Removing Nodes 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:xxxxxx
```

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	<i>Secure Domain Router Commands on the Cisco IOS XR Software</i> module of <i>Cisco IOS XR System Management Command Reference for the Cisco XR 12000 Series Router</i>
Initial system bootup and configuration information for a router using the Cisco IOS XR software	<i>Cisco IOS XR Getting Started Guide for the Cisco XR 12000 Series Router</i>
Cisco IOS XR master command reference	<i>Cisco IOS XR Commands Master List for the Cisco XR 12000 Series Router</i>
Information about user groups and task IDs	<i>Configuring AAA Services on the Cisco IOS XR Software</i> module of <i>Cisco IOS XR System Security Configuration Guide for the Cisco XR 12000 Series Router</i>
Cisco IOS XR interface configuration commands	<i>Cisco IOS XR Interface and Hardware Component Command Reference for the Cisco XR 12000 Series Router</i>
Information about configuring interfaces and other components on the Cisco CRS-1 from a remote Craft Works Interface (CWI) client management application	<i>Cisco Craft Works Interface User Guide</i>
Information about AAA policies, including instructions to create and modify users and username access privileges	<i>Configuring AAA Services on the Cisco IOS XR Software</i> module of <i>Cisco IOS XR System Security Configuration Guide for the Cisco XR 12000 Series Router</i>

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