



# Configuring Route Processor Redundancy for PKI

Route Processor Redundancy provides an alternative to the High System Availability feature. HSA enables a system to reset and use a standby Route Switch Processor, if the active RSP fails. Using RPR, you can reduce unplanned downtime because RPR enables a quicker switchover between an active and standby RSP if the active RSP experiences a fatal error.

Route Processor Redundancy feature currently available on Cisco ASR platforms with dual RP support such as ASR 1006, ASR 1009, and ASR 1013.



---

**Note** Route Processor Redundancy supports trustpool import.

---

- [Finding Feature Information, on page 1](#)
- [Prerequisites for Configuring Route Processor Redundancy, on page 1](#)
- [Restrictions for Configuring Route Processor Redundancy, on page 2](#)
- [How To Configure Route Processor Redundancy, on page 2](#)
- [Route Processor Redundancy SSO Mode Configuration Example, on page 2](#)
- [Route Processor Redundancy SSO Mode Verification Example, on page 3](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Prerequisites for Configuring Route Processor Redundancy

- You must use the same memory in both RSPs because the secondary RSP must be able to support the primary RSP during a failover.

## Restrictions for Configuring Route Processor Redundancy

- Route Processor Redundancy feature only supports platforms with dual RP support.
- Route Processor Redundancy is supported only on routers that support dual RSPs.
- It is not recommended to configure RA (Registration Authority) as it is not validated.

## How To Configure Route Processor Redundancy

### Configuring Route Processor Redundancy SSO Mode

```
configure terminal
redundancy
mode sso
main-cpu
standby console enable
exit
```

### Verifying Route Processor Redundancy

```
show redundancy states
show crypto pki server
show crypto pki certificates tname
```

## Route Processor Redundancy SSO Mode Configuration Example

Example for server side configuration:

```
asr1k(config)#ip http server
asr1k(config)#crypto pki trustpoint ROOTCA
asr1k(ca-trustpoint)#hash sha512
asr1k(ca-trustpoint)#revocation-check none
asr1k(ca-trustpoint)#rsa-keypair ROOTCA 2048
asr1k(ca-trustpoint)#crypto pki server ROOTCA
asr1k(cs-server)#issuer-name CN=ROOTCA C=pki
asr1k(cs-server)#lifetime certificate 00 00 15
asr1k(cs-server)#lifetime ca-certificate 00 00 25
asr1k(cs-server)#lifetime crl 6
asr1k(cs-server)#serial-number 0x1
```

```
asrlk(cs-server)#auto-rollover 00 00 24

% The archive password is not configured. Rollover CA keys and certificates will not be
automatically archived.

asrlk(cs-server)#grant auto

asrlk(cs-server)#database url tftp://<ip>

% Server database url was changed. You need to move the
% existing database to the new location.

asrlk(cs-server)#database url p12 tftp://<ip>

asrlk(cs-server)#database level complete

asrlk(cs-server)#database archive pkcs12 password <pwd>

asrlk(cs-server)#end
```

#### Example for client side configuration:

```
crypto pki trustpoint client
  enrollment url http://<ip>:80
  usage ike
  subject-name CN=R1 C=pki
  revocation-check crl
  rsakeypair client 2048
  hash sha512
```

## Route Processor Redundancy SSO Mode Verification Example

#### show redundancy states

```
my state = 13 -ACTIVE
peer state = 8 -STANDBY HOT

Mode = Duplex
Unit = Primary

Unit ID = 48

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured) = sso
Redundancy State = sso

Maintenance Mode = Disabled
```

```

Manual Swact = enabled
Communications = Up

client count = 132
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0

```

**show crypto pki server**

Certificate Server ROOTCA:

```

Status: enabled
State: enabled

Server's configuration is locked (enter "shut" to unlock it)
Issuer name: CN=ROOTCA C=pki
CA cert fingerprint: F2BF3707 D9F6F5F3 E0D111D8 A8486437
Granting mode is: auto
Last certificate issued serial number (hex): 2
CA certificate expiration timer: 14:15:50 IST Mar 31 2019
CRL NextUpdate timer: 14:15:50 IST Mar 31 2019
Current primary storage dir: tftp://9.45.3.3//
Current storage dir for .p12 files: tftp://9.45.3.3//
Database Level: Complete - all issued certs written as <serialnum>.cer
Auto-Rollover configured, overlap period 0 days
Autorollover timer: 13:51:50 IST Mar 31 2019
Redundancy configured. This is active.

```




---

**Note** Server is enabled only on active RP and is in disabled state in standby mode.

---

**show crypto pki certificates client**

```

Certificate

Status: Available

Certificate Serial Number (hex): 03

Certificate Usage: General Purpose

Issuer:

cn=ROOTCA C=pki

```

```
Subject:
  Name: asrlk
  hostname=asrlk
  cn=R1 C=pki
Validity Date:
  start date: 00:42:04 IST Mar 11 2019
  end   date: 01:02:04 IST Mar 11 2019
Associated Trustpoints: client
```

#### CA Certificate

```
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: Signature
Issuer:
  cn=ROOTCA C=pki
Subject:
  cn=ROOTCA C=pki
Validity Date:
  start date: 00:40:34 IST Mar 11 2019
  end   date: 00:40:34 IST Mar 9 2020
Associated Trustpoints: client
```

