active through issu set rollback-timer

aaa-authorization

To enable AAA authorization to run IOS commands that enable the collection of output for a Call-Home message, use the **aaa-authorization** command in call home configuration mode. To disable AAA authorization, use the **no** form of this command.

aaa-authorization [**username** *username*]
no aaa-authorization [**username**]

Syntax Description

username *username*	Specifies the username for authorization. Default username is callhome. Maximum length is 64.

Command Default

AAA authorization is disabled for Call-Home service as an embedded application to run IOS commands.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

The **aaa-authorization** command allows you to enable or disable AAA authorization when the Call-Home service is running IOS commands for the collection of output for Call-Home messages. To change the AAA authorization username, use the **aaa-authorization username** command. To change it back to the default username, use the **no** form of the **aaa-authorization username**command. After you enable AAA authorization, you must configure the Call-Home aaa-authorization username as the username on the TACACS server so that the Call-Home service can run the IOS commands.

Note When AAA authorization is disabled, you are not required to enter an AAA authorization username to send correct Call-Home messages.

Examples

The following example shows how AAA authorization is enabled:

```
Router(cfg-call-home)# aaa-authorization
```

The following example shows how AAA authorization username is changed to cisco:

```
Router(cfg-call-home)# aaa-authorization username cisco
```

Related Commands

Command	Description
call-home	Enters call home configuration mode.

active (call home)

To enable a destination profile for Call Home, use the active command in call home profile configuration mode. To disable a profile, use the **no** form of the command. To enable a user-defined profile, use the **default** form of the command, or to disable the CiscoTac-1 predefined profile, use the **default** form of the command.

active
no active
default active

Command Default

A user-defined destination profile is automatically enabled in Call Home after it is created. The predefined CiscoTac-1 profile is disabled.

Command Default

Command Modes

Call home profile configuration (cfg-call-home-profile)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS XE Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

A destination profile in Call Home is enabled when it is created. To disable a profile, use the **no active** command.

Examples

The following shows how to disable a destination profile that is automatically activated upon creation:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# no
 active
```

The following shows how to reactivate a destination profile that is disabled:

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# active
```

Related Commands

Command	Description
call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.

Command	Description
profile (call home)	Configures a destination profile to specify how alert notifications are delivered for Call Home and enters call home profile configuration mode.
show call-home	Displays Call Home configuration information.

active (diagnostic signature)

To activate diagnostic signatures on a device, use the **active** command in call-home diagnostic-signature configuration mode. To disable diagnostic signatures, use the **no** form of this command. To set the diagnostic signature feature to default, use the **default** form of this command.

active
no active
default active

Syntax Description

This command has no arguments or keywords.

Command Default

Diagnostic signatures is enabled.

Command Modes

Call-home diagnostic-signature configuration (cfg-call-home-diag-sign)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

Diagnostic signatures on a device is enabled by default. However, you must configure the **call-home** command for diagnostic signatures to function.

Example

The following example shows how to enable diagnostic signatures on a device:

```
Device> enable
Device# configure terminal
Device(config)# call-home
Device(cfg-call-home)# diagnostic-signature
Device(cfg-call-home-diag-sign)# active
Device(cfg-call-home-diag-sign)# end
```

Related Commands

Command	Description
call-home	Enters call-home configuration mode.
diagnostic-signature	Enters call-home diagnostic-signature configuration mode.
service call-home	Enables call-home services.

add-command

To add IOS commands to the Snapshot alert group, use the **add-command** command in snapshot configuration mode. To remove IOS commands from the alert group, use the **no** form of this command.

add-command *command string*
no add-command *command string*

Syntax Description

command string	IOS command. Maximum length is 128. **Note** The IOS command string must be enclosed in quotes (“”) if it contains white spaces.

Command Default

The Snapshot alert group has no command to run.

Command Modes

Snapshot configuration (cfg-call-home-snapshot)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

When you add commands to the Snapshot alert group, the output of the commands added are included in the snapshot message.

Examples

The following example shows the **show version** command added to the snapshot alert group:

```
Router(cfg-call-home-snapshot)# add-command “show version”
```

Related Commands

Command	Description
alert-group-config snapshot	Enters snapshot configuration mode.

alert-group

To enable an alert group, use the **alert-group** command in call home configuration mode. To disable an alert group, use the **no** form of this command.

alert-group {**all** | **configuration** | **diagnostic** | **environment** | **inventory** | **syslog**}
no alert-group

Syntax Description

all	Specifies all the alert groups.
configuration	Specifies the configuration alert group.
diagnostic	Specifies the diagnostic alert group.
environment	Specifies the environmental alert group.
inventory	Specifies the inventory alert group.
syslog	Specifies the syslog alert group.

Command Default

All alert groups are enabled.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

An *alert group* is a predefined subset of Call Home alerts supported on a platform. Different types of Call Home alerts are grouped into different alert groups depending on their type. The alert are as follows:

- Configuration
- Diagnostic
- Environment
- Inventory
- Syslog

Note The diagnostic alert group is not supported in Cisco IOS Release 12.4(24)T.

Call Home trigger events are grouped into alert groups with each alert group assigned command-line interface commands to execute when an event occurs. These alert group trigger events and executed commands are platform-dependent. For more information, see the platform-specific configuration guides on the Smart Call Home site on Cisco.com at:

http://www.cisco.com/en/US/products/ps7334/serv_home.html

Examples

The following example shows how to enable a specific alert group:

```
Router(config)# call-home
Router(cfg-call-home)# alert-group configuration
```

The following example shows how to enable all alert groups:

```
Router(cfg-call-home)# alert-group all
```

The following example shows how to disable a specific alert group:

```
Router(cfg-call-home)# no alert-group syslog
```

The following example shows how to disable all alert groups:

```
Router(cfg-call-home)# no alert-group all
```

Related Commands

call-home (global configuration)	Enters call home configuration mode.
show call-home	Displays call home configuration information.

alert-group-config snapshot

To enter snapshot configuration mode to enable the addition of IOS commands to the Snapshot alert group, use the **alert-group-config snapshot** command in call home configuration mode. To remove all IOS commands from the Snapshot alert group, use the **no** form of this command.

alert-group-config snapshot
no alert-group-config snapshot

Syntax Description

This command has no arguments or keywords.

Command Default

No IOS commands are added to the Snapshot alert group.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Examples

The following example shows how to enter snapshot configuration mode:

```
Router(cfg-call-home)# alert-group-config snapshot
```

Related Commands

Command	Description
add-command	Adds IOS commands to the Snapshot alert group.
call-home	Enters call home configuration mode.

anonymous-reporting-only

To set the TAC profile to anonymous mode, use the **anonymous-reporting-only** command in TAC profile configuration mode. To disable anonymous reporting, use the **no** form of this command.

anonymous-reporting-only
no anonymous-reporting-only

Syntax Description

This command has no arguments or keywords.

Command Default

Anonymous reporting is disabled. TAC profile sends a full report of all types of events subscribed in the profile.

Command Modes

TAC profile configuration (cfg-call-home-profile)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

When anonymous-reporting-only is set, only crash, inventory, and test messages are sent.

Examples

The following example shows how TAC profile is set to anonymous mode:

```
Router(cfg-call-home-profile)# anonymous-reporting-only
```

Related Commands

Command	Description
profile	Enables TAC profile configuration mode.

call-home (global configuration)

To enter call home configuration mode for the configuration of Call Home settings, use the **call-home** command in global configuration mode.

call-home

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

When you use the **call-home** command, you enter call home configuration mode and you can configure settings for the Call Home feature in your system.

When a call home message is sent only to a call home back-end server, the server checks the output length of each message. If the message length exceeds 10KB, the server compresses the output length. If the compressed message length still exceeds 10KB, the server drops the message.

Examples

The following example shows how to enter call home configuration mode and lists the commands that are available for Call Home configuration depending on your release:

```
Device(config)# call-home

Device(cfg-call-home)#?

Call-home configuration commands:
  alert-group         Enable or disable alert-group
  contact-email-addr  System Contact's email address
  contract-id         Contract identification for Cisco AutoNotify
  copy                Copy a call-home profile
  customer-id         Customer identification for Cisco AutoNotify
  default             Set a command to its defaults
  exit                Exit from call-home configuration mode
  mail-server         Configure call-home mail_server
  no                  Negate a command or set its defaults
  phone-number        Phone number of the contact person
  profile             Enter call-home profile configuration mode
  rate-limit          Configure call-home message rate-limit threshold
  rename              Rename a call-home profile
```

```
sender              Call home msg's sender email addresses
site-id             Site identification for Cisco AutoNotify
street-address      Street address for RMA part shipments
vrf                 VPN Routing/Forwarding instance name
```

Related Commands

Command	Description
alert-group	Enables an alert group.
contact-email-addr	Assigns the e-mail address to be used for customer contact for Call Home.
contract-id	Assigns the customer's contract identification number for Call Home.
copy profile	Creates a new destination profile with the same configuration settings as an existing profile.
customer-id (call home)	Assigns a customer identifier for Call Home.
mail-server	Configures an SMTP e-mail server address for Call Home.
phone-number	Assigns the phone number to be used for customer contact for Call Home.
profile (call home)	Configures a destination profile to specify how alert notifications are delivered for Call Home and enters call home profile configuration mode.
rate-limit (call home)	Configures the maximum number of messages per minute for Call Home.
rename profile	Changes the name of a destination profile.
sender	Assigns the e-mail addresses to be used in the from and reply-to fields in messages for Call Home.
service call-home	Enables Call Home.
show call-home	Displays Call Home configuration information.
site-id	Assigns a site identifier for Call Home.
street-address	Specifies a street address where RMA equipment for Call Home can be sent.
vrf (call home)	Associates a VRF instance for Call Home e-mail message transport.

call-home diagnostic-signature

To download, install, and uninstall diagnostic signature files on a device, use the **call-home diagnostic-signature** command in privileged EXEC mode.

call-home diagnostic-signature {{**deinstall** | **download**}{*ds-id* | **all**} | **install** *ds-id* | {**load***ds-file-name*}}

Syntax Description

deinstall	Removes diagnostic signature files from a device's memory and disk, thereby removing the registration of associated diagnostic signature events and actions.
download	Downloads diagnostic signature files from web servers (HTTP/HTTPS destination configured in the diagnostic signature profile). This download is called "on-demand" downloading.
ds-id	Diagnostic-signature ID of the file that must be downloaded, installed, or uninstalled.
all	Allows downloading and removal of all diagnostic-signature files on a device.
install	Manually installs already downloaded diagnostic signature files through an interactive session on the device. Normal diagnostic signature files are installed automatically as soon as they are downloaded. However, some diagnostic signature files include an interactive session. You must use the **install** keyword to manually install these diagnostic signature files.
load*ds-file-name*	Loads a call-home diagnostic-signature file from disk. Specify name of the diagnostic-signature file located on the disk.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

Download diagnostic signature files from: https://tools.cisco.com/its/service/oddce/services/DDCEService. Configure these diagnostic signature files using the **destination address http** command in call-home profile configuration mode. If you are using a transport gateway, configure a user destination profile and configure an HTTP destination that points to the transport gateway.

There are two types of diagnostic signature download requests: regular and forced. A regular diagnostic signature update involves requesting the download of any updated diagnostic signature files from HTTP/HTTPS servers. For a request download, you can either configure a periodic request trigger or by initiating an on-demand download request.

Forced downloading involves requesting for a specific diagnostic signature file. You can trigger forced download by initiating an "on-demand" downloading request.

Use the **call-home diagnostic-signature download** command for on-demand downloads.

Example

The following example shows how to download diagnostic signature file 6030 on a device. The download success message is displayed on the console.

```
Device# call-home diagnostic-signature download 6030

*Jan 16 06:10:22.142: %CALL_HOME-6-DS_UPDATE_SUCCESS:
call-home diagnostic-signature ondemand downloaded to flash:/call-home,
1 diagnostic-signature(s) added, 0 diagnostic-signature(s) updated.
```

The following example shows how to download diagnostic signature file 6033 on a device. The download success message is displayed on the console.

```
Device# call-home diagnostic-signature download 6033

*Jan 16 06:11:48.038: %CALL_HOME-6-DS_UPDATE_SUCCESS:
call-home diagnostic-signature ondemand downloaded to flash:/call-home,
1 diagnostic-signature(s) added, 0 diagnostic-signature(s) updated.
```

The following example shows how to install a diagnostic signature file 6030. The message displayed on the console indicates that 6030 does not include an interactive session for installation.

```
Device# call-home diagnostic-signature install 6030

Diagnostic-signature 6030 doesn't contain any prompt variables.
```

The following example shows how to install a diagnostic signature file 6033. The message displayed on the console indicates that 6033 includes an interactive session for installation.

```
Device# call-home diagnostic-signature install 6033

Please Enter Module Number (1-9): 1
All prompt variables are configured successfully.
```

The following example shows how to load a call-home diagnostic-signature file from disk.

```
Device# call-home diagnostic-signature load flash:DS_10492.xml

Load file flash:DS_10492.xml success
```

Related Commands

Command	Description
destination address http	Configures the address to which call home messages are sent.

call-home reporting

To enable Smart Call Home service with full reporting or anonymous reporting, use the **call-home reporting** command in global configuration mode.

call-home reporting {**anonymous** | **contact-email-addr** *email-address*} [**http-proxy** {*ipv4-addressipv6-addressname*} **port** *port-number*]

Syntax Description

anonymous	Enables Call-Home TAC profile to only send crash, inventory, and test messages and send the messages in an anonymous way.
contact-email-addr *email-address*	Enables Smart Call Home service full reporting capability and sends a full inventory message from Call-Home TAC profile to Smart Call Home server to start full registration process.
http-proxy {*ipv4-address*| *ipv6-address* | *name*}	(Optional) IP (ipv4 or ipv6) address or name of proxy server. Maximum length is 64.
port *port-number*	(Optional) Port number. Range: 1 to 65535.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

After successfully enabling Call Home either in anonymous or full registration mode using the **call-home reporting** command, an inventory message is sent out. If Call Home is enabled in full registration mode, a Full Inventory message for full registration mode is sent out. If Call Home is enabled in anonymous mode, an anonymous inventory message is sent out.

The **call-home reporting** command is not present in running or startup configuration files and there is no support for the no form of this command.

To disable the Call-Home feature, use the **no** form of the **service call-home** command in global configuration mode.

no service call-home

To remove the assigned e-mail address, use the **no** form of the **contact-email-addr** in call home configuration mode.

no contact-email-addr *email-address*

The HTTP proxy option allows you to make use of your own proxy server to buffer and secure Internet connections from your devices.

To disable the specified HTTP proxy server and port for the HTTP request, use the **no** form of the **http-proxy** command in call home configuration mode.

no http-proxy

To disable a destination profile, use the **no** form of the **active** command in call home profile configuration mode.

no active

To disable the CiscoTac-1 predefined profile, use the **default** form of the **active** command in call home profile configuration mode.

default active

If you decide not to use Smart Call Home, you can still enable Anonymous Reporting to allow Cisco to securely receive minimal error and health information from the device. For more information, see Configuring Call Home for Cisco Integrated Service Routers .

To disable anonymous reporting, use the **no** form of the **anonymous-reporting-only**command in TAC profile configuration mode.

no anonymous-reporting-only

Examples

The following example shows the Call-Home TAC profile enabled for all alert group messages, allowing it to send a full inventory message to start Smart Call Home registration:

Router(config)# **call-home reporting contact-email-addr email@company.com**

The following example shows the Call-Home TAC profile enabled to send crash, inventory, and test messages anonymously to port 1 of proxy server 1.1.1.1:

```
Router(config)# call-home reporting anonymous http-proxy 1.1.1.1 port 1
```

call-home request

To submit information about your system to Cisco for report and analysis information, use the **call-home request** command in privileged EXEC mode.

call-home request {**bugs-list** | **command-reference** | **config-sanity** | **output-analysis** "*show-command*" | **product-advisory**} {**profile** *name* [**ccoid** *user-id*] | **ccoid** *user-id* [**profile** *name*]}

Syntax Description

bugs-list	Requests report of known bugs in the running version and in the currently applied features.
command-reference	Requests report of reference links to all commands in the running configuration.
config-sanity	Requests report of information on best practices related to the current running configuration.
output-analysis “ *show-command* ”	Sends the output of the specified CLI show command for analysis. The show command must be contained in quotes (“ ”).
product-advisory	Requests report of Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect devices in your network.
profile *name*	Specifies an existing Call Home destination profile to which the request is sent. If no profile is specified, the request is sent to the CiscoTAC-1 profile.
ccoid *user-id*	Specifies the identifier of a registered Smart Call Home user. If a *user-id* is specified, the resulting analysis report is sent to the e-mail address of the registered user. If no *user-id* is specified, the report is sent to the contact e-mail address of the device.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

When you use this command, an analysis report is sent by Cisco to a configured contact e-mail address. The recipient profile does not need to be enabled for the call-home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message can be forwarded to the Cisco TAC and the user can receive the reply from the Smart Call Home service.

Based on the keyword option specified, the output of a predetermined set of commands as applicable to your system such as the **show running-config all**, **show version**, and **show module** (standalone) or **show module switch all**(VS system) commands, is sent to Cisco for analysis.

Examples

The following example shows a request for analysis of the **show diagnostic result module all** command to be sent to the contact information specified for the Call Home destination profile named "TG":

```
Router# call-home request output-analysis "show diagnostic result module all" profile TG
```

The following example shows a request for the known bugs list to be sent to the Call Home destination profile named "CiscoTAC-1" and a registered CCO userid "myuserid":

```
Router# call-home request bugs-list profile CiscoTAC-1 ccoid myuserid
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
call-home send	Executes an EXEC-level CLI command and sends the command output for Call Home using e-mail.
call-home send alert-group	Manually sends an alert group message for Call Home.
service call-home	Enables Call Home.
show call-home	Displays Call Home configuration information.

call-home send

To execute an EXEC-level CLI command and send the command output for Call Home using e-mail, use the **call-home send** command in privileged EXEC mode.

call-home send *"exec-command"* {**email** *email-addr* [**tac-service-request** *request-number*] | **tac-service-request** *request-number* [**email** *email-addr*]}

Cisco 7600 Series Routers in Cisco IOS Release 12.2(33)SRC
call-home send *"exec-command"* {**email** *email-addr* [**service-number** *SR*] | **service-number** *SR*}

Syntax Description

" *exec-command* **"**	Specifies an EXEC-level CLI command to be executed. The command output is sent by e-mail. The EXEC command must be contained in quotes (" ").
email *email-addr*	Specifies the e-mail address to which the CLI command output is sent. If no e-mail address is specified, the command output is sent to the Cisco TAC at attach@cisco.com.
service-number *SR*	(Cisco 7600 Series Routers in Cisco IOS Release 12.2(33)SRC) Specifies an active TAC case number to which the command output pertains. This number is required only if no e-mail address (or a TAC e-mail address) is specified, and will appear in the e-mail subject line.
tac-service-request *request-number*	Specifies the TAC service request number that appears in the subject line of the e-mail. This keyword is optional if used after entering the **email** option.

Command Default

This command has no default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI. The **service-number**keyword option is replaced by the **tac-service-request** keyword option.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

This command causes the specified CLI command to be executed on the system. The command must be enclosed in quotes (" "), and can be any EXEC-level command, including commands for all modules.

The command output is then sent by e-mail to the specified e-mail address. If no e-mail address is specified, the command output is sent to the Cisco TAC at attach@cisco.com. The e-mail will be sent in long text format with the service number, if specified, in the subject line.

Examples

This example shows how to send a CLI command and have the command output e-mailed:

```
Router# call-home send "show diagnostic result module all" email support@example.com
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
call-home send alert-group	Manually sends an alert group message for Call Home.
service call-home	Enables Call Home.
show call-home	Displays Call Home configuration information.

call-home send alert-group

To manually send an alert-group message for the Call Home feature, use the **call-home send alert-group** command in privileged EXEC mode.

Cisco Catalyst 4500 Series Switches, Cisco Catalyst 6500 Series Switches, Cisco 7600 Series Routers
call-home send alert-group {**configuration** | **crash** | **diagnostic module** *number* | **inventory**} [**profile** *profile-name*]

Cisco ASR 1000 Series Aggregation Services Routers
call-home send alert-group {**configuration** | **crash** | **diagnostic slot** *number* | **inventory**} [**profile** *profile-name*]

Syntax Description

configuration	Sends the configuration alert-group message to the destination profile.
crash	Sends the system crash message with the latest crash information to the destination profile.
diagnostic module *number*	Sends the diagnostic alert-group message to the destination profile for a specific module, slot/subslot, or slot/bay number. The *number* value can be the module number, the slot/subslot number, or the slot/bay number. This option is supported on the Cisco Catalyst 4500 series switch, the Cisco Catalyst 6500 series switch, and the Cisco 7600 series router.
diagnostic slot *number*	Sends the diagnostic alert-group message to destination profiles for the specified slot, such as R0 for Route Processor (RP) slot 0. This option is supported on the Cisco ASR 1000 series router.
inventory	Sends the inventory call-home message to the destination profile.
profile *profile-name*	(Optional) Specifies the name of the destination profile.

Command Default

A Call Home alert group message is not sent manually.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Release	Modification
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6. The **diagnostic slot** keyword was added.
15.2(3)T	This command was modified. The **crash** keyword was added.

Usage Guidelines

The Cisco ASR 1000 series router does not support the **diagnostic module** keyword. Instead, use the **diagnostic slot** keyword.

If you do not specify the keyword-argument pair **profile** *profile-name*, the message is sent to all subscribed destination profiles. If you do specify a profile, the destination profile does not need to be subscribed to the alert group.

Only the configuration, crash, diagnostic, and inventory alert group messages can be sent manually.

Examples

The following example shows how to send a configuration alert-group message to a destination profile:

```
Device# call-home send alert-group configuration
```

The following example shows how to send a system crash message with the latest crash information to a destination profile:

```
Device# call-home send alert-group crash
```

The following example shows how to send a diagnostic alert-group message to all subscribed destination profiles that have a lower severity subscription than the diagnostic result for a specific module, slot/subslot, or slot/bay number:

```
Device# call-home send alert-group diagnostic module 3/2
```

The following example shows how to send a diagnostic alert-group message to a destination profile named profile1 for a specific module, slot/subslot, or slot/bay number:

```
Device# call-home send alert-group diagnostic module 3/2 profile profile1
```

The following example shows how to send a diagnostic alert-group message to a destination profile named profile1 on RP slot 0 on a Cisco ASR 1000 Series Router:

```
Device# call-home send alert-group diagnostic slot R0 profile profile1
```

The following example shows how to send an inventory call-home message to a destination profile:

```
Device# call-home send alert-group inventory
```

Related Commands

call-home (global configuration)	Enters call-home configuration mode.
call-home test	Manually sends a Call Home test message to a destination profile.
service call-home	Enables the Call Home feature.
show call-home	Displays the Call Home configuration information.

call-home test

To manually send a Call Home test message to a destination profile, use the **call-home test** command in privileged EXEC mode.

call-home test ["*test-message*"] **profile** *profile-name*

Syntax Description

" *test-message* **"**	(Optional) Test message text enclosed in required quotation marks (" ").
profile *profile-name*	Specifies the name of the destination profile.

Command Default

This command has no default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

This command sends a test message to the specified destination profile. If you enter test message text, you must enclose the text in quotes (" ") if it contains spaces. If you do not enter a message, a default message is sent.

Examples

The following example shows how to manually send a Call Home test message with the text "test of the day" to the profile named CiscoTAC-1:

```
Router# call-home test "test of the day" profile CiscoTAC-1
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
call-home send alert-group	Manually sends an alert group message for Call Home.
service call-home	Enables Call Home.
show call-home	Displays Call Home configuration information.

clear call-home diagnostic-signature statistics

To clear the statistics counters or downloading counters associated with the diagnostic signature on a device, use the **clear call-home diagnostic-signature statistics** command in privileged EXEC mode.

clear call-home diagnostic-signature statistics [**download**]

Syntax Description

download	(Optional) Clears the periodic or on-demand download counters.

Command Default

If you do not specify any optional keywords or arguments, call-home diagnostic signature execution counters are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

The execution statistics data for diagnostic signatures that have an execution limit configured cannot be cleared. Warning messages are displayed on the console in such cases.

Example

The following is sample output from the **show call-home diagnostic-signature statistics** command before the **clear call-home diagnostic-signature statistics** command is entered:

```
Device# show call-home diagnostic-signature statistics

                                                        Average Run
DS ID     DS Name                 Triggered/Max/Deinstall  Time(sec)  Max Run Time(sec)
--------  ------------------------------  -------------  -----------  ---------
6015      CronInterval                      4/0/N            9.872        9.981
6030      ActCH                             932/0/N          13.333       1357.860
6032      MultiEvents                       10/0/N           6.362        6.692
6033      PureTCL                           15/0/N           6.363        7.620
```

The following is a message displayed on the console from the **clear call-home diagnostic-signature statistics** command. This command clears the execution counter for the diagnostic signature.

```
Device# clear call-home diagnostic-signature statistics

% The statistics of diagnostic-signature with maximum execution times limitation will not
be cleared.
```

The following is sample output from the **show call-home diagnostic-signature statistics** command after the **clear call-home diagnostic-signature statistics** command is entered:

```
Device# show call-home diagnostic-signature statistics

                                                        Average Run
DS ID     DS Name                 Triggered/Max/Deinstall  Time(sec)  Max Run Time(sec)
```

```
--------  -------------------------------  -------------  -----------  ---------
6030      ActCH                            0/0/N          0.000        0.000
6032      MultiEvents                      0/0/N          0.000        0.000
6033      PureTCL                          0/0/N          0.000        0.000
```

The following is sample output from the **show call-home diagnostic-signature statistics download** command before the **clear call-home diagnostic-signature statistics download** command is entered:

```
Device# show call-home diagnostic-signature statistics download

Download-type    In-queue      Fail    Success   Last request sent
-------------   ----------    -----   ---------  ------------------------------
Periodic            0          0        0
Ondemand            0          1        1        2013-01-16 04:49:52 GMT+00:00
```

The following is sample output from the **show call-home diagnostic-signature statistics download** command after the **clear call-home diagnostic-signature statistics download** command is entered:

```
Device# clear call-home diagnostic-signature statistics download

Device# show call-home diagnostic-signature statistics download

Download-type    In-queue      Fail    Success   Last request sent
-------------   ----------    -----   ---------  ------------------------------
Periodic            0          0        0
Ondemand            0          0        0
```

Related Commands

Command	Description
call-home diagnostic-signature	Downloads, installs, and uninstalls diagnostic signature files on a device.
show call-home diagnostic-signature statistics	Displays statistics and attributes of a diagnostic signature file on a device.

clear ip rsvp high-availability counters

To clear (set to zero) the Resource Reservation Protocol (RSVP) traffic engineering (TE) high availability (HA) counters that are being maintained by a Route Processor (RP), use the **clear ip rsvp high-availability counters** command in privileged EXEC mode.

clear ip rsvp high-availability counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **clear ip rsvp high-availability counters**command to clear (set to zero) the HA counters, which include state, resource failures, and historical information.

Examples

The following example clears all the HA information currently being maintained by the RP:

```
Router# clear ip rsvp high-availability counters
```

Related Commands

Command	Description
show ip rsvp high-availability counters	Displays the RSVP TE HA counters that are being maintained by an RP.

clear issu state

To clear the state and current version of the Route Processors (RPs) during the In Service Software Upgrade (ISSU) process, use the **clear issu state** command in user EXEC or privileged EXEC mode.

clear issu state

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

This command clears the state and current version of RPs during the ISSU process.

Examples

The following example clears state and current version of the RPs during the ISSU process:

```
Router# clear issu state
```

configure issu set rollback timer

To configure the rollback timer value, use the **configure issu set rollback timer**command in global configuration mode.

configure issu set rollback timer *seconds*

Syntax Description

seconds	The rollback timer value, in seconds. The valid timer value range is from 0 to 7200 seconds (two hours). A value of 0 seconds disables the rollback timer.

Command Default

Rollback timer value is 45 minutes.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	Enhanced Fast Software Upgrade (eFSU) support was added on the Cisco 7600 series routers. In Service Software Upgrade (ISSU) is not supported in Cisco IOS Release 12.2(33)SRB.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use the configure issue set rollback timer command to configure the rollback timer value. Note that you can enable this command only when the Route Processors (RPs) are in the init state.

Examples

The following example sets the rollback timer value to 3600 seconds, or 1 hour:

```
Router(config)# configure issu set rollback timer 3600
```

Related Commands

Command	Description
issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
show issu rollback timer	Displays the current setting of the ISSU rollback timer.

contact-email-addr

To assign the e-mail address to be used for customer contact for Call Home, use the **contact-email-addr** command in call home configuration mode. To remove the assigned e-mail address, use the **no** form of this command.

contact-email-addr *email-address*
no contact-email-addr *email-address*

Syntax Description

email-address	Up to 200 characters in standard e-mail address format (contactname@domain) with no spaces.

Command Default

No e-mail address is assigned for customer contact.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

To support the Call Home feature, the **contact-email-addr** command must be configured.

Examples

The following example configures the e-mail address “username@example.com” for customer contact:

```
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr username@example.com
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
show call-home	Displays call home configuration information.

contract-id

To assign the customer's contract identification number for Call Home, use the **contract-id** command in call home configuration mode. To remove the contract ID, use the **no** form of this command.

contract-id *alphanumeric*
no contract-id *alphanumeric*

Syntax Description

alphanumeric	Contract number, using up to 64 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (" ").

Command Default

No contract ID is assigned.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

You must have a service contract for your Cisco device to use the Smart Call Home service. You can specify this contract number in the Call Home feature using the **contract-id (call home)** command.

Examples

The following example configures "Company1234" as the customer contract ID:

```
Router(config)# call-home
Router(cfg-call-home)# contract-id Company1234
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
show call-home	Displays call home configuration information.

copy profile

To create a new destination profile with the same configuration settings as an existing profile, use the **copy profile**command in call home configuration mode.

copy profile *source-profile target-profile*

Syntax Description

source-profile	Name of the existing destination profile that you want to copy.
target-profile	Name of the new destination profile that you want to create from the copy.

Command Default

No default behavior or values.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

To simplify configuration of a new profile, use the **copy profile** command when an existing destination profile has configuration settings that you want to use as a basis for a new destination profile.

After you create the new profile, you can use the **profile (call home)** command to change any copied settings that need different values.

Examples

The following example creates a profile named “profile2” from an existing profile named “profile1”:

```
Router(config)# call-home
Router(cfg-call-home)# copy profile profile1 profile2
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
profile (call home)	Configures a destination profile to specify how alert notifications are delivered for Call Home and enters call home profile configuration mode.
show call-home	Displays call home configuration information.

crashdump-timeout

To set the longest time that the newly active Route Switch Processor (RSP) will wait before reloading the formerly active RSP, use the **crashdump-timeout** command in redundancy mode. To reset the default time that the newly active RSP will wait before reloading the formerly active RSP, use the **no** form of this command.

crashdump-timeout
[{**mm** | **hh:** *mm*}]
no crashdump-timeout

Syntax Description

mm	(Optional) The time, in minutes, that the newly active RSP will wait before reloading the formerly active RSP. The range is from 5 to 1080 minutes.
hh **:** *mm*	(Optional) The time, in hours and minutes, that the newly active RSP will wait before reloading the formerly active RSP. The range is from 5 minutes to 18 hours.

Command Default

The default timeout for this command is 5 minutes.

Command Modes

Redundancy

Command History

Release	Modification
12.0(22)S	This command was introduced on the Cisco 7500 series routers.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(20)S	Support was added for the Cisco 7304 router. The Cisco 7500 series router is not supported in Cisco IOS Release 12.2(20)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(31)SXH.

Usage Guidelines

Use this command to specify the length of time that the newly active RSP will wait before reloading the previously active RSP. This time can be important when considering how long to wait for a core dump to complete before reloading the RSP.

In networking devices that support stateful switchover (SSO), the newly active primary processor runs the core dump operation after the switchover has taken place. Following the switchover, the newly active RSP will wait for a period of time for the core dump to complete before attempting to reload the formerly active RSP.

In the event that the core dump does not complete within the time period provided, the standby RSP is reset and reloaded based on the **crashdump timeout** command setting, regardless of whether it is still performing a core dump.

Note The core dump process adds the slot number to the core dump file to identify which processor generated the file content. For more information on how to configure the system for a core dump, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* , Release 12.4.

Examples

The following example sets the time before the previously active RSP is reloaded to 10 minutes:

```
Router(config-r)# crashdump-timeout 10
```

customer-id (call home)

To assign a customer identifier for Call Home, use the **customer-id**command in call home configuration mode. To remove the customer ID, use the **no** form of this command.

customer-id *alphanumeric*
no customer-id *alphanumeric*

Syntax Description

alphanumeric	Customer identifier, using up to 256 alphanumeric characters. If you include spaces, you must enclose your entry in quotes (“ ”).

Command Default

No customer ID is assigned.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **customer-id** command is optional.

Examples

The following example configures “Customer1234” as the customer ID:

```
Router(config)# call-home
Router(cfg-call-home)# customer-id Customer1234
```

Related Commands

call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
show call-home	Displays call home configuration information.

data-privacy

To scrub data from running configuration files to protect the privacy of users, use the **data-privacy** command in call home configuration mode. To revert back to data privacy default configuration, use the **no** form of this command.

data-privacy {**level** {**normal** | **high**} | **hostname**}
no data-privacy {**level** | **hostname**}

Syntax Description

level	Specifies the level of commands to be scrubbed.
normal	Scrubs all normal-level commands. This is the default data-privacy level.
high	Scrubs all normal-level commands plus the IP domain name and IP address commands.
hostname	Scrubs all high-level or normal-level commands plus the **hostname** command. **Note** Scrubbing the hostname from configuration messages can cause Smart Call Home processing failure on some platforms.

Command Default

Default level is normal and hostname scrubbing is disabled. Password/secret and other commands are scrubbed from running configuration files.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

The **data-privacy** command scrubs data, such as IP addresses, from running configuration files to protect the privacy of customers. For Cisco IOS Release 15.2(2)T and earlier releases, the output of show commands are not being scrubbed except for configuration messages in the **show running-config all** and **show startup-config** data.

Note Enabling the **data-privacy** command can affect CPU utilization when scrubbing a large amount of data.

Examples

The following example shows how to scrub all normal-level commands plus the IP domain name and IP address commands from the running configuration file:

```
Router(cfg-call-home)# data-privacy level high
```

Related Commands

Command	Description
call-home	Enters call home configuration mode.

destination (call home)

To configure the message destination parameters in a profile for Call Home, use the **destination (call home)**command in call home profile configuration mode. To remove the destination parameters, use the **no** form of this command.

destination {**address** {**email** *address* | **http** *url*} | **message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} | **transport-method** {**email** | **http**}}
no destination {**address** {**email** *address* | **http** *url*} | **message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} | **transport-method** {**email** | **http**}}

Syntax Description

address {**email** *address* | **http** *url*	Configures the address type and location to which Call Home messages are sent, where: • **email** *address* --Email address, up to 200 characters. • **http** *url* --URL, up to 200 characters. Starting from Cisco IOS XE 17.1, only a single URL is permitted for a profile. If you add a new URL, the old URL is replaced.
message-size-limit *size*	Displays maximum Call Home message size for this profile, in bytes. The range is from 50 to 3145728. The default is 3145728.
preferred-msg-format {**long-text** | **short-text** | **xml**}	Specifies the message format for this profile, where: • **long-text** --Format for use in standard e-mail providing a complete set of information in message. • **short-text** --Format for use with text pagers providing a smaller set of information in the message, including host name, timestamp, error message trigger, and severity level. • **xml** --Format that includes a complete set of information in the message, including XML tags. This is the default.
transport-method	Specifies the transport method for this profile, where: • **email** --Messages are sent using e-mail. This is the default. • **http** --Messages are sent using HTTP or HTTPS.

Command Default

No destination address type is configured. If you do not configure the **destination (call home)** command, the following defaults are configured for the profile:

- **message-size-limit** --3,145,728 bytes
- **preferred-msg-format** --XML
- **transport-method** --E-mail

Command Modes

Call home profile configuration (cfg-call-home-profile)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
12.2(52)SG	This command was integrated into Cisco IOS Release 12.2(52)SG.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

You can repeat the **destination (call home)** command in call home profile configuration mode to configure different message parameters for a profile. There is no default for the **destination address** form of the command, and an address must be configured for every profile.

For a user-defined profile, you can enable both e-mail and HTTP as accepted transport methods, by entering the **destination transport-method email** command and also the **destination transport-method http** command for the profile.

For the CiscoTAC-1 predefined profile, only one transport method can be enabled at a time. If you enable a second transport method, the existing method is automatically disabled. By default, e-mail can be used to send information to the Cisco Smart Call Home backend server, but if you want to use a secure HTTPS transport, you need to configure HTTP.

Examples

The following examples shows configuration of both transport methods for a user profile:

```
Router(config)# call-home
Router(cfg-call-home)# profile example
Router(cfg-call-home-profile)# destination transport-method email
Router(cfg-call-home-profile)# destination transport-method http
```

The following example shows a profile configuration for e-mail messaging using long-text format:

```
Router(config)# call-home
Router(cfg-call-home)# profile example
Router(cfg-call-home-profile)# destination address email username@example.com
Router(cfg-call-home-profile)# destination preferred-msg-format long-text
```

The following example shows part of a Syslog alert notification (when subscribed to receive syslog alerts) using long-text format on a Cisco ASR 1006 router:

```
TimeStamp : 2009-12-03 12:26 GMT+05:00
Message Name : syslog
Message Type : Call Home
Message Group : reactive
Severity Level : 2
Source ID : ASR1000
Device ID : ASR1006@C@FOX105101DH
Customer ID : username@example.com
Contract ID : 123456789
Site ID : example.com
Server ID : ASR1006@C@FOX105101DH
Event Description : *Dec  3 12:26:02.319 IST: %CLEAR-5-COUNTERS: Clear counter on all
interfaces by console
System Name : mcp-6ru-3
```

```
Contact Email : username@example.com
Contact Phone : +12223334444
Street Address : 1234 Any Street Any City Any State 12345
Affected Chassis : ASR1006
Affected Chassis Serial Number : FOX105101DH
Affected Chassis Part No : 68-2584-05
Affected Chassis Hardware Version : 2.1
Command Output Name : show logging
Attachment Type : command output
MIME Type : text/plain
Command Output Text :
Syslog logging: enabled (1 messages dropped, 29 messages rate-limited, 0 flushes, 0 overruns,
 xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 112 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
No active filter modules.
    Trap logging: level informational, 104 message lines logged
Log Buffer (1000000 bytes):
*Dec  3 07:16:55.020: ASR1000-RP HA: RF status CID 1340, seq 93, status
RF_STATUS_REDUNDANCY_MODE_CHANGE, op 0, state DISABLED, peer DISABLED
*Dec  3 07:17:00.379: %ASR1000_MGMTVRF-6-CREATE_SUCCESS_INFO: Management vrf Mgmt-intf
created with ID 4085, ipv4 table-id 0xFF5, ipv6 table-id 0x1E000001
*Dec  3 07:17:00.398: %NETCLK-5-NETCLK_MODE_CHANGE: Network clock source not available. The
 network clock has changed to freerun
*Dec  3 07:17:00.544: %LINEPROTO-5-UPDOWN: Line protocol on Interface LI-Null0, changed
state to up
*Dec  3 07:17:00.545: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
*Dec  3 07:17:00.545: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
*Dec  3 07:17:00.546: %LINK-3-UPDOWN: Interface LIIN0, changed state to up
*Dec  3 07:17:00.546: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to down
*Dec  3 07:17:01.557: %LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC0, changed state
 to up
*Dec  3 07:17:01.557: %LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi0, changed state
 to up
*Dec  3 07:17:01.558: %LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN0, changed state
 to up
*Dec  3 07:17:01.558: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0,
changed state to down
*Dec  3 07:17:01.818: %DYNCMD-7-CMDSET_LOADED: The Dynamic Command set has been loaded from
 the Shell Manager
*Dec  3 07:16:30.926: %CMRP-5-PRERELEASE_HARDWARE: R0/0: cmand:  2 is pre-release hardware
*Dec  3 07:16:24.147: %HW_IDPROM_ENVMON-3-HW_IDPROM_CHECKSUM_INVALID: F1: cman_fp:  The
idprom contains an invalid checksum in a sensor entry. Expected: 63, calculated: fe
*Dec  3 07:16:24.176: %CMFP-3-IDPROM_SENSOR: F1: cman_fp:  One or more sensor fields from
the idprom failed to parse properly because Success.
*Dec  3 07:16:27.669: %CPPHA-7-START: F1: cpp_ha:  CPP 0 preparing image
/tmp/sw/fp/1/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:27.839: %CPPHA-7-START: F1: cpp_ha:  CPP 0 startup init image
/tmp/sw/fp/1/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:28.659: %CPPHA-7-START: F0: cpp_ha:  CPP 0 preparing image
/tmp/sw/fp/0/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:28.799: %CPPHA-7-START: F0: cpp_ha:  CPP 0 startup init image
/tmp/sw/fp/0/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:32.557: %CPPHA-7-START: F1: cpp_ha:  CPP 0 running init image
/tmp/sw/fp/1/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:32.812: %CPPHA-7-READY: F1: cpp_ha:  CPP 0 loading and initialization complete
```

```
*Dec  3 07:16:33.532: %CPPHA-7-START: F0: cpp_ha:  CPP 0 running init image
/tmp/sw/fp/0/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:33.786: %CPPHA-7-READY: F0: cpp_ha:  CPP 0 loading and initialization complete
.
.
.
```

Example: Sample Message Using XML Format

The following example shows part of a Syslog alert notification using XML format on a Cisco ASR 1006 router when the **destination preferred-msg-format xml** command for a profile is configured:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M0:FOX105101DH:CEC1E73E</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2009-12-03 12:29:02 GMT+05:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>ASR1000</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G1:FOX105101DH:CEC1E73E</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2009-12-03 12:29:01 GMT+05:00</ch:EventTime>
<ch:MessageDescription>*Dec  3 12:29:01.017 IST: %CLEAR-5-COUNTERS: Clear counter on all
interfaces by console</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>ASR1000 Series Routers</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>username@example.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId>username@example.com</ch:CustomerId>
```

```
<ch:SiteId>example.com</ch:SiteId>
<ch:ContractId>123456789</ch:ContractId>
<ch:DeviceId>ASR1006@C@FOX105101DH</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>mcp-6ru-3</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>username@example.com</ch:ContactEmail>
<ch:ContactPhoneNumber>+12223334444</ch:ContactPhoneNumber>
<ch:StreetAddress>1234 Any Street Any City Any State 12345</ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>ASR1006</rme:Model>
<rme:HardwareVersion>2.1</rme:HardwareVersion>
<rme:SerialNumber>FOX105101DH</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="68-2584-05" />
<rme:AD name="SoftwareVersion" value="" />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.925" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, IOS-XE Software
(PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Experimental Version 12.2(20091118:075558)
[v122_33_xnf_asr_rls6_throttle-mcp_dev_rls6 102]
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 18-Nov-09 01:14 by " />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Syslog logging: enabled (1 messages dropped, 29 messages rate-limited, 0 flushes, 0 overruns,
 xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 114 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
No active filter modules.
    Trap logging: level informational, 106 message lines logged
Log Buffer (1000000 bytes):
*Dec  3 07:16:55.020: ASR1000-RP HA: RF status CID 1340, seq 93, status
RF_STATUS_REDUNDANCY_MODE_CHANGE, op 0, state DISABLED, peer DISABLED
*Dec  3 07:17:00.379: %ASR1000_MGMTVRF-6-CREATE_SUCCESS_INFO: Management vrf Mgmt-intf
created with ID 4085, ipv4 table-id 0xFF5, ipv6 table-id 0x1E000001
*Dec  3 07:17:00.398: %NETCLK-5-NETCLK_MODE_CHANGE: Network clock source not available. The
 network clock has changed to freerun
*Dec  3 07:17:00.544: %LINEPROTO-5-UPDOWN: Line protocol on Interface LI-Null0, changed
state to up
*Dec  3 07:17:00.545: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
*Dec  3 07:17:00.545: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
*Dec  3 07:17:00.546: %LINK-3-UPDOWN: Interface LIIN0, changed state to up
*Dec  3 07:17:00.546: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to down
```

```
*Dec  3 07:17:01.557: %LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC0, changed state
 to up
*Dec  3 07:17:01.557: %LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi0, changed state
 to up
*Dec  3 07:17:01.558: %LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN0, changed state
 to up
*Dec  3 07:17:01.558: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0,
changed state to down
*Dec  3 07:17:01.818: %DYNCMD-7-CMDSET_LOADED: The Dynamic Command set has been loaded from
 the Shell Manager
*Dec  3 07:16:30.926: %CMRP-5-PRERELEASE_HARDWARE: R0/0: cmand:  2 is pre-release hardware
*Dec  3 07:16:24.147: %HW_IDPROM_ENVMON-3-HW_IDPROM_CHECKSUM_INVALID: F1: cman_fp:  The
idprom contains an invalid checksum in a sensor entry. Expected: 63, calculated: fe
*Dec  3 07:16:24.176: %CMFP-3-IDPROM_SENSOR: F1: cman_fp:  One or more sensor fields from
the idprom failed to parse properly because Success.
*Dec  3 07:16:27.669: %CPPHA-7-START: F1: cpp_ha:  CPP 0 preparing image
/tmp/sw/fp/1/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:27.839: %CPPHA-7-START: F1: cpp_ha:  CPP 0 startup init image
/tmp/sw/fp/1/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:28.659: %CPPHA-7-START: F0: cpp_ha:  CPP 0 preparing image
/tmp/sw/fp/0/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:28.799: %CPPHA-7-START: F0: cpp_ha:  CPP 0 startup init image
/tmp/sw/fp/0/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:32.557: %CPPHA-7-START: F1: cpp_ha:  CPP 0 running init image
/tmp/sw/fp/1/0/fp/mount/usr/cpp/bin/cpp-mcplo-ucode
*Dec  3 07:16:32.812: %CPPHA-7-READY: F1: cpp_ha:  CPP 0 loading and initialization complete
.
.
.
```

Related Commands

Command	Description
call-home (global configuration)	Enters call home configuration mode for configuration of Call Home settings.
profile (call home)	Configures a destination profile to specify how alert notifications are delivered for Call Home and enters call home profile configuration mode.

diagnostic-signature

To enter diagnostic signature configuration mode on a device, use the **diagnostic-signature** command in call-home configuration mode. To set all diagnostic signature configurations to default, use the **no** form or the **default** form of this command. To disable the diagnostic signature configuration mode, use only the **no** form of this command.

diagnostic-signature
no diagnostic-signature
default diagnostic-signature

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Call-home configuration (cfg-call-home)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

Use the **call-home** command to enter call-home configuration mode. Then use the **diagnostic-signature** command to enter diagnostic signature configuration mode.

Example

The following example shows how to enter call-home diagnostic-signature mode using the **call-home** and **diagnostic-signature** commands:

```
Device> enable
Device# configure terminal
Device(config)# call-home
Device(cfg-call-home)# diagnostic-signature
Device(cfg-call-home-diag-sign)# end
```

Related Commands

Command	Description
call-home	Enters call-home configuration mode.

environment (diagnostic signature)

To set a value to an environment variable for a diagnostic signature that is available on a device, use the **environment** command in call-home diagnostic-signature configuration mode. To remove the value for an existing environment variable, use the **no** form of this command. To set default value to an environment variable, use the **default** form of this command.

environment ds_ *env-varname ds-env-varvalue*
no environment ds_ *env-varname*
default environment ds_ *env-varname*

Syntax Description

ds_ *env-varname*	Environment variable name for the diagnostic signature feature. The range is from 4 to 31 characters including the **ds_** prefix. **Note** The variable name must have a prefix **ds_**; for example, ds_env1.
ds-env-varvalue	Environment variable value for the diagnostic signature feature. The range is from 1 to 127 characters.

Command Default

The value for an environment variable for a diagnostic signature is not set.

Command Modes

Call-home diagnostic-signature configuration (cfg-call-home-diag-sign)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

If a diagnostic signature file requires embedding of the environment variable specific to a device, you must set a value for the environment variable by using the **environment** command. There are two special environment variables: ds_signature_id and ds_hostname. These environment variables are assigned a default value automatically when the diagnostic signature files are being installed.

Example

The following example shows how to specify the environment variable name (for example, ds_env1) and the environment variable value (for example, abc) for a diagnostic signature feature:

```
Device> enable
Device# configure terminal
Device(config)# call-home
Device(cfg-call-home)# diagnostic-signature
Device(cfg-call-home-diag-sign)# environment ds_env1 abc
Device(cfg-call-home-diag-sign)# end
```

Related Commands

Command	Description
active (diagnostic signature)	Activates the diagnostic signatures on a device.
call-home	Enters call-home configuration mode.

Command	Description
diagnostic-signature	Enters call-home diagnostic-signature configuration mode.

frame-relay redundancy auto-sync lmi-sequence-numbers

To configure automatic synchronization of Frame Relay Local Management Interface (LMI) sequence numbers, use the **frame-relay redundancy auto-sync lmi-sequence-numbers**command in global configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

frame-relay redundancy auto-sync lmi-sequence-numbers
no frame-relay redundancy auto-sync lmi-sequence-numbers

Syntax Description

This command has no arguments or keywords.

Command Default

Automatic synchronization of Frame Relay LMI sequence numbers is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced on Cisco 7500 and 10000 series Internet routers.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S on Cisco 7500 series routers.
12.2(20)S	Support was added for the Cisco 7304 router. The Cisco 7500 series router is not supported in Cisco IOS Release 12.2(20)S.
12.0(28)S	SSO support was added to the Multilink Frame Relay feature on the Cisco 12000 series Internet router and the Cisco 7500 series router.
12.2(25)S	SSO support was added to the Multilink Frame Relay feature on the Cisco 12000 series Internet router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Enabling the **frame-relay redundancy auto-sync lmi-sequence-numbers**command improves the chances of a clean switchover on Frame Relay DTE interfaces when the peer Frame Relay DCE is intolerant of LMI errors. Use this command to configure LMI if the DCE fails the line protocol after fewer than three LMI errors and if changing the DCE configuration is neither possible nor practical.

Examples

The following example enables synchronization of LMI DTE sequence numbers on a router that is running Frame Relay:

```
frame-relay redundancy auto-sync lmi-sequence-numbers
```

Related Commands

Command	Description
debug frame-relay redundancy	Debugs Frame Relay redundancy on the networking device.

http-proxy

To specify the HTTP proxy server and port for the HTTP request and prevent the device from connecting to Cisco or other destinations using HTTP directly, use the **http-proxy** command in call home configuration mode. To disable, use the **no** form of this command.

http-proxy {*ipv4-addressipv6-addressname*} **port** *port-number*
no http-proxy

Syntax Description

ipv4-address | *ipv6-address* | *name*	IP (ipv4 or ipv6) address or name of proxy server. Maximum length is 64.
port *port-number*	Port number. Range: 1 to 65535.

Command Default

No HTTP proxy server is used for Call-Home messages.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Examples

The following example specifies port 1 of proxy server 1.1.1.1 as the HTTP proxy server port for the HTTP request:

```
Router(cfg-call-home)# http-proxy 1.1.1.1 port 1
```

Related Commands

Command	Description
call-home	Enters call home configuration mode.

http resolve-hostname ipv4-first

To enable/disable ipv4-first resolution type of http. To disable, use the no form of this command.

Syntax

This command has no arguments or keywords.

Command Default

This command is disabled by default. When disabled, http resolves server hostname with ipv6-first.

Command Modes

Call home configuration (cfg-call-home)

Command History

Release	Modification
Cisco IOS XE 16.9.4	This command was introduced.
Cisco IOS XE Gibraltar 16.10.2	This command was integrated.
Cisco IOS XE Gibraltar 16.11.x	This command was integrated.

Examples

The following example specifies how to use **http resolve-hostname ipv4-first** command:

```
Device> enable
Device# configure terminal
Device(config)# call-home
Device(cfg-call-home)# http resolve-hostname ipv4-first
Device(cfg-call-home)# end
```

http secure server-identity-check

To enable/disable server identity check when HTTPS connection is established. To disable, use the no form of this command.

Syntax

This command has no arguments or keywords.

Command Default

This command is enabled by default. When http secure server-identity-check is enabled, the requested http address must included in http server certificate else the http connection will fail.

Note The **http secure server-identity-check** option was default in versions 16.7.2 or earlier, and was not configurable. For behavioral parity with images earlier than 16.7.3, ensure that you configure the **no http secure server-identity-check** option after upgrading. The default option is **http secure server-identity-check**.

Command Modes

Call home configuration (cfg-call-home)

Release	Modification
Cisco IOS XE Fuji 16.8	This command was introduced.

Command History

Release	Modification
15.2(2)T	This command was introduced.

Examples

The following example specifies how to use **http secure server-identity-check** command:

```
Device> enable
Device# configure terminal
Device(config)# call-home
Device(cfg-call-home)# http secure server-identity-check
Device(cfg-call-home)# end
```

issu abortversion

To cancel the In Service Software Upgrade (ISSU) upgrade or downgrade process in progress and restore the router to its state before the process had started, use the **issu abortversion**command in user EXEC or privileged EXEC mode. This command is also available in diagnostic mode on the Cisco ASR 1000 Series Routers.

General Syntax
issu abortversion *slot image*

Cisco ASR 1000 Series Router Syntax
issu abortversion [**verbose**]

Syntax Description

slot	The specified slot on the networking device. Refer to your hardware documentation for information on the number of slots on your networking device.
image	The new image to be loaded into the standby.
verbose	Displays verbose information, meaning all information that can be displayed on the console during the process will be displayed.

Command Default

This command is disabled by default.

Command Modes

User EXEC (>) Privileged EXEC (#) Diagnostic (diag)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	Enhanced Fast Software Upgrade (eFSU) support was added on the Cisco 7600 series routers. ISSU is not supported in Cisco IOS Release 12.2(33)SRB.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers and introduced in diagnostic mode.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **issu abortversion** command allows the user to stop the ISSU process at any time before the user commits to completing the process by issuing the **issu commitversion** command. Before any action is taken, a check is performed to ensure that both RPs are either in the run version (RV) or load version (LV) state.

When the **issu abortversion** command is issued before the **issu runversion** command, the standby RP is reset and reloaded. When the **issu abortversion** command is issued after the **issu runversion**command, the network switches to the former Cisco IOS software version.

On Cisco ASR 1000 Series Routers, the **issu** command set, including this command, can be used to upgrade individual sub-packages and consolidated packages. The **request platform software package** command set can also be used for ISSU upgrades on this platform, and generally offer more options for each upgrade.

Previously, when ISSU was in a state other than Init, either the **issu commitversion** or **issu runversion** command had been issued, and the image being loaded or run was not present, the only way to return to the ISSU Init state was to clear the state manually and reload the router. Now, if either thei**ssu commitversion** or the **issu runversion**command is issued and the image cannot be located, the ISSU state is cleared automatically, and the standby RP is reloaded with the image that existed before the i**ssu abortversion** or the **issu loadversion** command was issued.

Examples

In the following example, the **issu abortversion** command resets and reloads the standby RP:

```
Router# issu abortversion bootdisk:c10k2-p11-mz.2.20040830
```

In the following example, the **issu abortversion** command is entered to abort an ISSU upgrade of a consolidated package on a Cisco ASR 1000 Series Router:

```
Router# issu abortversion
--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting installation changes ---
Cancelling rollback timer
Finished installation changes
SUCCESS: Target RP will now reload
```

Related Commands

Command	Description
issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
issu commitversion	Allows the new Cisco IOS software image to be loaded into the standby RP.
issu loadversion	Starts the ISSU process.
issu runversion	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image.
show issu state	Displays the state and current version of theduring the ISSU process.

issu acceptversion

To halt the rollback timer and ensure the new Cisco IOS software image is not automatically aborted during the In Service Software Upgrade (ISSU) process, use the **issu acceptversion**command in user EXEC or privileged EXEC mode. This command is also available in diagnostic mode on the Cisco ASR 1000 Series Routers.

General Syntax
issu acceptversion {*active slot-number* | **active slot-name** *slot-name*}

Cisco ASR 1000 Series Routers syntax
issu acceptversion [**verbose**]

Syntax Description

active slot-number	The specified active slot on your networking device. Refer to your hardware documentation for information on the number of slots on your networking device.
active slot-name *slot-name*	Identifies a specific slot name.
verbose	Displays verbose information, meaning all information that can be displayed on the console during the process will be displayed.

Command Default

45 minutes from the time the **issu runversion** command is issued to the time the **issu acceptversion** is issued.

Command Modes

User EXEC (>) Privileged EXEC (#) Diagnostic (diag)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	Enhanced Fast Software Upgrade (eFSU) support was added on the Cisco 7600 series routers. ISSU is not supported in Cisco IOS Release 12.2(33)SRB.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers, and introduced in diagnostic mode.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use the issu acceptversion command to ensure that the active Route Processor (RP) is running the new image, that the standby RP is running the old image, and that both RPs are in the run version (RV) state. If the **issu acceptversion** command is not issued within 45 minutes from the time the **issu runversion** command is

issued, the new active RP is assumed to be unreachable, and the entire ISSU process is automatically rolled back to the previous version of the software. The rollback timer starts immediately after the user issues the **issu runversion** command.

If the rollback timer is set for a short period of time, such as 1 minute, and the standby RP is not yet in a hot standby state, you then have 15 1-minute extensions during which the router will wait for the standby state to become hot standby state. However, if the standby state becomes hot standby state within the 15-minute extension, the router will abort the ISSU process because the 1-minute rollback timer has expired. Therefore, it is not recommended to set the rollback timer shorter than the time required for the standby state to become hot standby state.

If the rollback timer is set to a long period of time, such as the default of 45 minutes, and the standby RP goes into the hot standby state in 7 minutes, you have 38 minutes (45 minus 7) to roll back if necessary.

Use the **configure issu set rollback timer** to configure the 45-minute default value on the rollback timer.

On Cisco ASR 1000 Series Routers, the **issu** command set, including this command, can be used to upgrade individual sub-packages and consolidated packages. The **request platform software package** command set can also be used for ISSU upgrades on this platform, and generally offer more options for each upgrade.

Examples

The following example shows how to halt the rollback timer and allow the ISSU process to continue:

```
Router# issu acceptversion b disk0:c10k2-p11-mz.2.20040830
```

The following example shows how to halt the rollback timer and allow the ISSU process to continue on a Cisco ASR 1000 Series Router:

```
Router# issu acceptversion
```

Related Commands

Command	Description
configure issu set rollback timer	Configures the rollback timer value.
issu abortversion	Cancels the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.
issu commitversion	Allows the new Cisco IOS software image to be loaded into the standby RP.
issu loadversion	Starts the ISSU process.
issu runversion	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image.
show issu state	Displays the state and current version of the RPs during the ISSU process.

issu changeversion

To perform a single-step complete In-Service Software Upgrade (ISSU) upgrade process cycle, use the **issu changeversion**command in privileged EXEC mode.

issu changeversion *active-image*

Cisco 7600 Series Routers

issu changeversion {*active-slot active-image* | *standby-slot active-image*}[{[**at** *hh*:*mm*] | **in** *hh*:*mm* | **quick**}]

Syntax Description

active-slot	The active slot on the networking device.
active-image	The active image on the networking device.
standby-slot	The standby slot on the networking devive
at *hh*:*mm*	(Optional) Specifies the exact time (hh:mm; 24 hour format), within the next 24 hours, at which the upgrade will occur.
in *hh*:*mm*	(Optional) Specifies the number of hours and minutes to elapse before the upgrade occurs.
quick	(Optional) When switchover happens, the standby boots up with the new image instead of the old image for faster upgrade.

Command Default

No upgrade has happened.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SCD2	This command was introduced.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S. This command is supported on the Cisco 7600 Series routers.

Usage Guidelines

The **issu changeversion** command starts a single-step complete upgrade process cycle. This command performs the logic for all four of the standard commands (**issu loadversion**, **issu runversion**, **issu acceptversion**, and **issu commitversion**) without any user intervention required to complete the next step.

The **issu changeversion** command allows the networking device to inform the system that the networking device is performing a complete upgrade cycle automatically, and allows the state transitions to move to the next step automatically.

Once the **issu changeversion** command is issued, the upgrade can be aborted using the **issu abortversion** command. An upgrade using the **issu changeversion** command may also be automatically aborted if the system detects any problems or an unhealthy system is determined during the upgrade.

The ISSU upgrade process consists of three states:

1. Initialization (INIT) state

2. Load version (LV) state
3. Run version (RV) state

Each of these states is defined by a set of variables, which are primary version (PV), secondary version (SV), current version (CV), and the ISSU state (IS). The transition of all these states is accomplished using the **issu changeversion** command, which automatically performs these state transitions.

Examples

The following example starts a single-step complete upgrade process cycle using the disk0:ubr10k4-k9p6u2-mz.122-33.SCC2 image from slot 0:

```
Router# issu changeversion
disk0:ubr10k4-k9p6u2-mz.122-33.SCC2
```

Related Commands

Command	Description
issu abortversion	Cancels the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.
issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
issu commitversion	Allows the new Cisco IOS software image to be loaded into the standby RP.
issu loadversion	Starts the ISSU process.
issu runversion	Forces a switchover from the active RP to the standby RP and causes the newly active RP to run the new image specified in the **issu loadversion** command.
show issu state	Displays the state and current version of the RPs during the ISSU process.

issu checkversion

To check In-Service Software Upgrade (ISSU) compatibility between the current and the target image, use the issu checkversion command in the privileged EXEC mode.

Using the mdr as a keyword, you can also verify the Minimal Disruptive Restart (MDR) compatibility of software upgrade.

issu checkversion *slot URL*

Syntax Description

slot	(Optional)Specified slot on the networking device. This slot is used when the subpackage software upgrade option is selected. For information about the number of slots on your networking device, refer to your hardware documentation.
URL	URL to the file. The URL contains the name of the file system, directories, and filename.

Command Default

This command is disabled by default

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced in the Cisco ASR 1000 Series Aggregation Services Routers.

Example

The following is sample output from the issu checkversion command that is used to check the MDR upgrade compatibility on the Cisco ASR 1000 Series Routers:

```
Router# issu checkversion rp 1 file stby-harddisk:RP2_XE38_20121101_080017_iso1 mdr

--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization

--- Starting local lock acquisition on R1 ---
Finished local lock acquisition on R1

--- Starting file path checking ---
Finished file path checking

--- Starting system installation readiness checking ---
Finished system installation readiness checking

--- Starting image verification ---
Compatibility check with running software on active RP

WARNING:
WARNING: Candidate software combination not found in compatibility database
```

```
WARNING:

Software sets are identified as compatible
Finished image verification

--- Starting mdr compatibility verification ---
Extracting consolidated package content
Checking and verifying packages contained in consolidated package
Creating candidate provisioning file
Processing candidate provisioning file

WARNING:

MDR for SPA type [0x55E] located at slot [2] bay [2] not supported by running package version
 [BLD_V153_1_S_XE38_THROTTLE_LATEST_20121101_080017_2]


WARNING:

MDR for SPA type [0x43F] located at slot [3] bay [1] not supported by running package version
 [BLD_V153_1_S_XE38_THROTTLE_LATEST_20121101_080017_2]


WARNING:

MDR for SPA type [0x43B] located at slot [5] bay [2] not supported by running package version
 [BLD_V153_1_S_XE38_THROTTLE_LATEST_20121101_080017_2]

WARNING:

MDR compatibility failed - proceeding with forced MDR-upgrade - some traffic will be impacted
 during the upgrade
Finished mdr compatibility verification

SUCCESS: Software is ISSU MDR compatible
```

The fields shown in the display are self-explanatory.

Related Commands

Command	Description
issu abortversion	Cancels the ISSU upgrade or downgrade process that is in progress and restores the router to its original state before the process had started.
issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically aborted during the ISSU process.
issu commitversion	Commits the new Cisco IOS software image to the file system of the standby RP and ensures that both the active RP and standby RP are in the run version (RV) state.
issu loadversion	Starts the ISSU process.
show issu state	Displays the state and current version of the RPs during the ISSU process.

issu commitversion

To allow the new Cisco IOS software image to be loaded into the standby Route Processor (RP), use the **issu commitversion**command in user EXEC or privileged EXEC mode. This command is also available in diagnostic mode on the Cisco ASR 1000 Series Routers.

General Syntax
issu commitversion *slot active-image*

Cisco ASR 1000 Series Routers Syntax
issu commitversion [**verbose**]

Syntax Description

slot	The specified slot on the networking device. Refer to your hardware documentation for information on the number of slots on your networking device.
active-image	The new image to be loaded into the active networking device.
verbose	Displays verbose information, meaning all information that can be displayed on the console during the process will be displayed.

Command Default

This command is disabled by default.

Command Modes

User EXEC (>) Privileged EXEC (#) Diagnostic (diag)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	Enhanced Fast Software Upgrade (eFSU) support was added on the Cisco 7600 series routers. In Service Software Upgrade (ISSU) is not supported in Cisco IOS Release 12.2(33)SRB.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was introduced on the ASR 1000 Series Routers, and introduced in diagnostic mode.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **issu commitversion**command verifies that the standby RP has the new Cisco IOS software image in its file system and that both RPs are in the run version (RV) state. If these conditions are met, then the following actions take place:

- The standby RP is reset and booted with the new version of Cisco IOS software.

- If both images are compatible, the standby RP moves into the stateful switchover (SSO) mode and is fully stateful for all clients and applications with which the standby RP is compatible.
- If both images are not compatible, the standby RP moves into Route Processor Redundancy Plus (RPR+) mode or RPR mode.
- If all conditions are correct, the RPs are moved into final state, which is the same as initial state.

Issuing the issu commitversion command completes the In Service Software Upgrade (ISSU) process. This process cannot be stopped or reverted to its original state without starting a new ISSU process.

Issuing the **issu commitversion** command at this stage is equivalent to entering both the **issu acceptversion** and the **issu commitversion** commands. Use the **issu commitversion** command if you do not intend to run in the current state for a period of time and are satisfied with the new software version.

On Cisco ASR 1000 series routers, the **issu** command set, including this command, can be used to upgrade individual subpackages and consolidated packages. The **request platform software package** command set can also be used for ISSU upgrades on this platform, and generally offer more options for each upgrade.

The **issu runversion** step can be bypassed on a Cisco ASR 1000 Series Router by using the **redundancy force-switchover** command to switchover between RPs and entering the **issu commitversion**command on the RP being upgraded. However, the **issu runversion** command is still available on this router and can still be used as part of the process for upgrading software using ISSU.

Previously, when ISSU was in a state other than Init, either the **issu commitversion** or **issu runversion** command had been issued, and the image being loaded or run was not present, the only way to return to the ISSU Init state was to clear the state manually and reload the router. Now, if either thei**ssu commitversion** or the **issu runversion**command is issued and the image cannot be located, the ISSU state is cleared automatically, and the standby RP is reloaded with the image that existed before the i**ssu abortversion** or the **issu loadversion** command was issued.

Examples

The following example shows how to reset the standby RP and reload it with the new Cisco IOS software version:

```
Router# issu commitversion a stby-disk0:c10k2-p11-mz.2.20040830
```

The following example shows how the standby RP or Cisco IOS process is reset and reloaded with the new Cisco consolidated package on the Cisco ASR 1000 Series Router:

```
Router# issu commitversion
--- Starting installation changes ---
Cancelling rollback timer
Saving image changes
Finished installation changes
Building configuration...
[OK]
SUCCESS: version committed: harddisk
:ASR1000rp1-advipservicesk9.01.00.00.12-33.XN.bin
```

Related Commands

Command	Description
issu abortversion	Cancels the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.

Command	Description
issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
issu loadversion	Starts the ISSU process.
issu runversion	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image.
show issu state	Displays the state and current version of the RPs during the ISSU process.

issu loadversion

To start the In-Service Software Upgrade (ISSU) process, use the **issu loadversion** command in user EXEC, privileged EXEC mode, or diagnostic mode.

General Syntax
issu loadversion *active-slot active-image standby-slot standby-image* [**force**]

Cisco ASR 1000 Series Routers Syntax
issu loadversion rp *identifier* **file** *disk-type image-file-name* [{**bay** *number* [**slot** *number*] | **slot** *number* [**bay** *number*]}] [**mdr**] [**force**]

Syntax Description

active-slot	The active slot on the networking device.
active-image	The active image on the networking device.
rp *identifier*	Specifies the Route Processor (RP) on Cisco ASR 1000 Series Aggregation Services Routers to verify the upgraded software version. Entering the **rp** *0* commad selects the RP in slot 0 and entering the **rp** *1* command selects the RP in slot 1.
file *disk-type image-file-name*	Specifies the path to the Cisco software image file that is used to perform the upgrade. The disk-type represents the type of storage disk where the image is available on Cisco ASR 1000 Series Aggregation Services Routers. The various disk-types are: • bootflash: • flash: • harddisk: • stby-bootflash: • stby-harddisk: • stby-obfl: • stby-usb0: • stby-usb1:
standby-slot	The standby slot on the networking device.
standby-image	The new image to be loaded into the standby networking device.
bay *number*	(Optional) Specifies the bay number within a shared port adapter interface processor (SIP) where a shared port adapter (SPA) is installed. Specifying the bay number restricts ISSU upgrades to the specified bay.
slot *number*	(Optional) Specifies the slot number where a SIP is installed. Specifying the slot number restricts ISSU upgrades to the specified slot.

mdr	(Optional) Performs ISSU upgrades using minimal disruptive restart (MDR). MDR upgrades can be performed on MDR-compatible SIPs (for example, SIP-40) and MDR-compatible SPAs.
force	(Optional) Performs automatic rollback overrides when ISSU upgrades are performed on MDR-incompatible SIPs (for example, SIP-10) or MDR-incompatible SPAs.

Command Default

If you do not enter the **issu loadversion** command, the ISSU upgrade or downgrade process is not initiated on devices.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	Enhanced Fast Software Upgrade (eFSU) support was added on the Cisco 7600 series routers. ISSU is not supported in Cisco IOS Release 12.2(33)SRB.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 Series Routers in Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco ASR 1000 Series Aggregation Services Routers in diagnostic mode.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.8S	This command was modified. The **mdr** keyword was added.

Usage Guidelines

Enabling the **issu loadversion** command causes the standby RP to be reset and booted with the new Cisco software image specified by the command. If both the active and standby RP images are ISSU-capable, ISSU-compatible, and have no configuration mismatches, then the standby RP moves into stateful switchover (SSO) mode, and both RPs move into the load version (LV) state.

It may take several seconds after the **issu loadversion** command is entered for Cisco software to load into the standby RP and the standby RP to transition to SSO mode.

Cisco ASR 1000 Series Aggregation Services Routers Usage Guidelines

On Cisco ASR 1000 Series Aggregation Services Routers, the **issu** command set, including the **issu loadversion** command, is used to upgrade individual subpackages and consolidated packages. The **request platform software package** command set can also be used for ISSU upgrades on this platform, and generally offer more options for each upgrade.

Use the **issu loadversion** command to start the ISSU rollback timer.

When ISSU is in a state other than Init, either the **issu commitversion** or **issu runversion** command had been issued, and the image being loaded or run is not present, the only way to return to the ISSU Init state is to clear the state manually and reload the device. Now, if either the **issu commitversion** or the **issu runversion** command is issued and the image cannot be located, the ISSU state is cleared automatically, and the standby RP is reloaded with the image that existed before the **issu abortversion** or the **issu loadversion** command is issued.

The **mdr** keyword is not usually configured with the **issu loadversion** command while performing consolidated package upgrades or SIPBase/SIPSPA subpackage upgrades. ISSU initiates MDR on a SIP when the following conditions are met:

- The chassis of Cisco ASR 1000 Series Aggregation Service Routers support hardware redundancy, that is, dual RPs and embedded services processors (ESPs) must be installed.
- The SIP type supports MDR. Currently, only SIP-40 supports MDR.
- All SPAs present in the SIP's SPA bays support MDR.
- All software versions are MDR-compatible with the subpackages available for each SPA and SIP types. Software versions are MDR-compatible if:
  - SIP base packages support MDR.
  - SIP base packages contain the same version of the SIP field programmable gate array (FPGA) or complex programmable logic device (CPLD) images.
  - SPA drivers for each SPA in a SIP support MDR.
  - Any existing SPA firmware has the same version.
  - Any existing SPA FPGA and CPLD images have the same version.

If any of the above mentioned conditions are not met, the MDR compatibility fails due to the presence of nonMDR-capable, nonMDR-compatible SPAs on MDR capable, or MDR-compatible SIPs, or due to the presence of an MDR-incompatible SIP. Use the **force** keyword to skip the MDR software compatibility checks and the MDR-incompatible SIP/SPAs are held from being reset during the upgrade process and brought online after a cold reboot when the upgrade is done.

Examples

The following example shows how to initiate the ISSU process by loading the active image into the active RP slot and loading the standby image into the standby RP slot:

```
Device# issu loadversion rp 0 file disk0:c10k2-p11-mz.2.20040830 b
stby-disk0:c10k2-p11-mz.2.20040830
```

The following is sample output when the **issu loadversion** command initiates an ISSU consolidated package upgrade on Cisco ASR 1000 Series Aggregation Services Routers.

```
Device# issu loadversion rp 1 file
stby-harddisk:ASR1000rp1-advipservicesk9.01.00.00.12-33.XN.bin

--- Starting installation state synchronization --- Finished installation state
synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting system installation readiness checking --- Finished system installation readiness
```

```
 checking
--- Starting installation changes ---
Setting up image to boot on next reset
Starting automatic rollback timer
Finished installation changes
SUCCESS: Software will now load.
```

The following is sample output when the **issu loadversion** command initiates an ISSU consolidated package upgrade using the **mdr** keyword on the standby RP of the Cisco ASR 1000 Series Aggregation Services Routers.

```
Device# issu loadversion rp 1 file stby-harddisk:issu_dir/xe38_iso1.bin mdr

--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization

--- Starting local lock acquisition on R1 ---
Finished local lock acquisition on R1

--- Starting file path checking ---
Finished file path checking

--- Starting system installation readiness checking ---
Finished system installation readiness checking

--- Starting image verification ---
Compatibility check with running software on active RP

WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:

Software sets are identified as compatible
Finished image verification

--- Starting mdr compatibility verification ---
Extracting consolidated package content
Checking and verifying packages contained in consolidated package
Creating candidate provisioning file
Processing candidate provisioning file

WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard format.
Skipping MDR Software Compatibility checks.
WARNING:

WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard format.
Skipping MDR Software Compatibility checks.
WARNING:


WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard format.
Skipping MDR Software Compatibility checks.
WARNING:

MDR for SPA type [0x46F] located at slot [1] bay [1] not supported by running package version

[BLD_V153_1_S_XE38_THROTTLE_LATEST_20121004_080020_2]
```

```
WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard format.
Skipping MDR Software Compatibility checks.
WARNING:

MDR for SPA type [0x507] located at slot [1] bay [3] not supported by running package version

[BLD_V153_1_S_XE38_THROTTLE_LATEST_20121004_080020_2]

WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard format.
Skipping MDR Software Compatibility checks.
WARNING:

MDR for CC type [0x515] located at slot [2] not supported by running package version
[BLD_V153_1_S_XE38_THROTTLE_LATEST_20121004_080020_2]
As SIP2 does not support MDR none of the SPA's within in may be upgraded using MDR
FAILED: MDR compatibility failed - alternatively run with 'force' option to proceed.
However not all FRU's may be upgraded using MDR
```

Note In the output displayed above, although an MDR-compatible SIP-40 is available on Cisco ASR 1000 Series Aggregation Services Routers, the MDR compatibility check fails due to the presence of an MDR-incompatible SIP-10.

The following is sample output when the **issu loadversion** command initiates an ISSU consolidated package upgrade using the **mdr** and **force** keywords on the standby RP of the Cisco ASR 1000 Series Aggregation Services Routers:

```
Device# issu loadversion rp 1 file stby-harddisk:issu_dir/xe38_iso1.bin mdr force

--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization

--- Starting local lock acquisition on R1 ---
Finished local lock acquisition on R1

--- Starting file path checking ---
Finished file path checking

--- Starting system installation readiness checking ---
Finished system installation readiness checking

--- Starting image verification ---
Compatibility check with running software on active RP

WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:

Software sets are identified as compatible
Finished image verification

--- Starting mdr compatibility verification ---
Extracting consolidated package content
Checking and verifying packages contained in consolidated package
```

```
Creating candidate provisioning file
Processing candidate provisioning file

WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard format.
Skipping MDR Software Compatibility checks.
WARNING:


WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard format.
Skipping MDR Software Compatibility checks.
WARNING:


WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard format.
Skipping MDR Software Compatibility checks.
WARNING:

MDR for SPA type [0x46F] located at slot [1] bay [1] not supported by running package version

[BLD_V153_1_S_XE38_THROTTLE_LATEST_20121004_080020_2]

WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard format.
Skipping MDR Software Compatibility checks.
WARNING:

MDR for SPA type [0x507] located at slot [1] bay [3] not supported by running package version

[BLD_V153_1_S_XE38_THROTTLE_LATEST_20121004_080020_2]

WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard format.
Skipping MDR Software Compatibility checks.
WARNING:

MDR for CC type [0x515] located at slot [2] not supported by running package version
[BLD_V153_1_S_XE38_THROTTLE_LATEST_20121004_080020_2]
As SIP2 does not support MDR none of the SPA's within in may be upgraded using MDR
MDR compatibility failed - proceeding with forced MDR-upgrade - some traffic will be impacted
 during the upgrade
Finished mdr compatibility verification

--- Starting installation changes ---
Setting up image to boot on next reset
Starting automatic rollback timer
Finished installation changes

SUCCESS: Software will now load.

*Oct 10 07:21:36.032: %IOSXE_OIR-6-OFFLINECARD: Card (rp) offline in slot R1
*Oct 10 07:21:36.065: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_NOT_PRESENT)
*Oct 10 07:21:36.065: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN)
*Oct 10 07:21:36.065: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
*Oct 10 07:21:38.273: %RF-5-RF_RELOAD: Peer reload. Reason: EHSA standby down
*Oct 10 07:21:38.284: % Redundancy mode change to SSO
```

Note In the output displayed above, despite the presence of an MDR-incompatible SIP-10, software upgrade is forced on Cisco ASR 1000 Series Aggregation Services Routers.

Related Commands

Command	Description
issu abortversion	Cancels the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.
issu acceptversion	Halts the rollback timer and ensures that the new Cisco IOS software image is not automatically aborted during the ISSU process.
issu commitversion	Allows the new Cisco IOS software image to be loaded into the standby RP.
issu runversion	Forces a switchover of the active to the standby processor and causes the newly active processor to run the new image.
request platform software package install file	Upgrades a consolidated package or an individual subpackage on devices.
show issu state	Displays the state and current version of the RPs during the ISSU process.

issu runversion

To force a switchover from the active Route Processor (RP) to the standby RP and cause the newly active RP to run the new image specified in the **issu loadversion** command, use the **issu runversion**command in user EXEC or privileged EXEC mode. This command is also available in diagnostic mode on the Cisco ASR 1000 Series Routers.

General Syntax
issu runversion *slot image*

Cisco ASR 1000 Series Routers Syntax
issu runversion [**verbose**]

Syntax Description

slot	The specified slot on the networking device. Refer to your hardware documentation for information on the number of slots on your networking device.
image	The new image to be loaded into the standby RP.
verbose	Displays verbose information, meaning all information that can be displayed on the console during the process will be displayed.

Command Default

No default behavior or values.

Command Modes

User EXEC (>) Privileged EXEC (#) Diagnostic (diag)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(31)SGA	This command was integrated into Cisco IOS Release 12.2(31)SGA.
12.2(33)SRB	Enhanced Fast Software Upgrade (eFSU) support was added on the Cisco 7600 series routers. ISSU is not supported in Cisco IOS Release 12.2(33)SRB.
12.2(33)SRB1	ISSU is supported on the Cisco 7600 series routers in Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers, and introduced in diagnostic mode.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

When a user enables the **issu runversion** command, a switchover is performed, and the standby RP is booted with the old image version following the reset caused by the switchover. As soon as the standby RP moves into the standby state, the rollback timer is started.

On Cisco ASR 1000 Series Routers, the **issu** command set, including this command, can be used to upgrade individual sub-packages and consolidated packages. The **request platform software package** command set can also be used for ISSU upgrades on this platform, and generally offer more options for each upgrade.

The **issu runversion** step can be bypassed on a Cisco ASR 1000 Series Router by using the **redundancy force-switchover** command to switchover between RPs and entering the **issu commitversion** command on the RP being upgraded. However, **issu runversion** is still available on this router and can still be used as part of the process for upgrading software using ISSU.

Previously, when ISSU was in a state other than Init, either the **issu commitversion** or **issu runversion** command had been issued, and the image being loaded or run was not present, the only way to return to the ISSU Init state was to clear the state manually and reload the router. Now, if either thei**ssu commitversion** or the **issu runversion**command is issued and the image cannot be located, the ISSU state is cleared automatically, and the standby RP is reloaded with the image that existed before the i**ssu abortversion** or the **issu loadversion** command was issued.

Examples

In the following example, the **issu runversion** command is used to switch to the redundant RP with the new Cisco IOS software image:

```
Router# issu runversion b stby-disk0:c10k2-p11-mz.2.20040830
```

In the following example, the **issu runversion** command is used to switch to the standby RP with the new Cisco IOS-XE consolidated package on the Cisco ASR 1000 Series Routers:

```
Router# issu runversion
--- Starting installation state synchronization ---
Finished installation state synchronization
Initiating active RP failover
SUCCESS: Standby RP will now become active
```

Related Commands

Command	Description
issu abortversion	Cancels the ISSU upgrade or downgrade process in progress and restores the router to its state before the process had started.
issu acceptversion	Halts the rollback timer and ensures the new Cisco IOS software image is not automatically aborted during the ISSU process.
issu commitversion	Commits the new Cisco IOS software image in the file system of the standby RP and ensures that both the active and standby RPs are in the RV state.
issu loadversion	Starts the ISSU process.
show issu state	Displays the state and current version of the RPs during the ISSU process.

issu set rollback-timer

To set the rollback timer for the software image to revert to the previous software image after an unfinished or unsuccessful in-service software upgrade (ISSU), use the **issu set rollback-timer** command in global configuration mode. To disable the timer, use the **no** form of this command.

issu set rollback-timer {*seconds hh:mm:ss*}
no issu set rollback-timer

Syntax Description

seconds	Rollback timer value in seconds.
hh:mm:ss	Rollback timer value in hours:minutes:seconds.

Command Default

The default rollback timer value is 2700 seconds (45 minutes).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

If the rollback timer expires during an ISSU, the software image reverts to the previous software image. To stop the timer, you must either accept or commit the new software image.

The timer duration can be set with one number (seconds), indicating the number of seconds, or as hours, minutes, and seconds with a colon as the delimiter (hh:mm:ss). The range is 0 to 7200 seconds (2 hours); the default is 2700 seconds (45 minutes). A setting of 0 disables the rollback timer.

Examples

This example shows how to set the rollback timer to 3600 seconds (one hour) using both command formats:

```
Router(config)# issu set rollback-timer 3600
% Rollback timer value set to [ 3600 ] seconds
Router(config)# issu set rollback-timer 01:00:00
% Rollback timer value set to [ 3600 ] seconds
```

The following examples shows how to disable the rollback timer:

```
Router(config) no issu set rollback-timer
```

Related Commands

Command	Description
show issu	Displays eFSU information.
show issu rollback-timer	Displays eFSU rollback timer value.