New and Changed Information for Cisco Unified Communications Manager Release 8.6(1)

New and Changed Information for Cisco Unified Communications Manager Release 8.6(1) contains information about the following topics:

• Installation, Upgrade, and Migration, page 1
• Command Line Interface, page 5
• Cisco Unified Communications Manager Administration, page 23
• Cisco Unified Communications Manager Features and Applications, page 26
• Security, page 66
• Cisco Unified IP Phones, page 77
• Cisco Unified Serviceability, page 86
• Cisco Unified Real-Time Monitoring Tool, page 93
• APIs, page 97

Installation, Upgrade, and Migration

This section contains information about the following topics:

• Unified CM on Virtualized Servers with Small Hard Drives, page 3
• VMware Specs-based Support, page 3
• Performing Failed RAID Disk Replacement With Single Restart for Linux Software RAID, page 3
• Software Upgrades, page 4
• Upgrading the Cisco Intercompany Media Engine Server, page 4
• Installing Cisco Unified Communications Manager on a VM, page 5
Caution

When you upgrade to Cisco Unified Communications Manager (Unified CM) 8.6(1) the system will reboot as part of the upgrade process. Therefore, you may want to perform the upgrade during a scheduled down time for your organization to avoid service interruptions.

Caution

If you are upgrading your software on HP 7825H3 or HP 7828H3 hardware, there is no option to revert to the previous version of Unified CM. To perform an upgrade on one of these machines you must use a 16 GB USB key to migrate data from the old system to the new installation.

You must back up your system before you begin the upgrade. This is particularly important if you are upgrading software on HP 7825H3 or HP 7828H3 hardware as there is no option to revert to the previous version.

If you are upgrading software on HP 7825H3 or HP 7828H3 hardware, ensure that you have a 16 GB USB device available to migrate your data to the new system. For Unity Connection and Business Edition 5000, a 128 GB external USB device is required.

Note

When you upgrade to Cisco Unified Communications Manager 8.6(1), the system reboots several times as part of the upgrade process and the service outage period is longer than with traditional upgrades. Therefore, you may want to perform the upgrade during a scheduled down time for your organization to avoid service interruptions. Once the upgrade begins, (either from the command line or graphical user interface) the data is migrated, the system reboots automatically, and the temporary server outage begins. The duration of this outage depends on your configuration and the amount of data that needs to be migrated.

When the upgrade is complete, you can choose to activate the partition with the new upgrade software or return to using the partition with the previous version of the software. With the exception of HP 7825H3 and HP 7828H3 hardware upgrades, the previous software remains in the inactive partition until the next upgrade. Your configuration information migrates automatically to the upgraded version in the active partition.

If for any reason you decide to back out of the upgrade, you can restart the system to the inactive partition that contains the older version of the software. However, any configuration changes that you made since you upgraded the software will get lost.

Note

You can only make changes to the database on the active partition. The database on the inactive partition does not get updated. If you make changes to the database after an upgrade, you must repeat those changes after switching the partition.

Caution

Be sure to back up your system data before starting the software upgrade process. For more information, see the Disaster Recovery System Administration Guide. If you are upgrading your software on HP 7825H3 or HP 7828H3 hardware, there is no option to revert to the previous version of Unified CM. If you do not back up your system data before starting the software upgrade process your data will be lost.

Before you proceed with the installation, consider the following recommendations (in addition to the existing ones):
• You will face a problem during RAID creation when you install Cisco Unified Communications Manager 8.5 or an earlier version on 7825 H3 and 7528 H3 servers that currently have Cisco Unified Communications Manager 8.6 installed on it. To resolve the issue:
  a. Boot the Unified CM server with the Unified CM 8.6 recovery disc.
  b. When prompted, choose option C to wipe off all data from the system. Option C indicates “Cleaning the system to set to bare metal state.”

You can now proceed with the installation of the earlier versions of Unified CM.

• When you insert or remove a USB drive, you might see error messages on the console similar to “sdb: assuming drive cache: write through.” You can safely ignore these messages.

Unified CM on Virtualized Servers with Small Hard Drives

Unified CM can be installed on virtual servers with smaller hard drives to support deployments with fewer users.

For deployments of 2500 users with a small disk (55 GB), if the administrator modifies the number of logs or the size of log files, for any service from the default they will need to clean up the log files before an upgrade. Alternately, the administrator can modify the thresholds of Lpm so that log files are cleaned up automatically more often.

Caution

A deployment of 2500 users with a small disk (55 GB) should only be used for a deployment where the total number of users on the cluster is less than 2500. If this deployment option is used, each node in the cluster must use the same deployment. Migration from this deployment to the large deployments is not supported.

VMware Specs-based Support

Cisco supports Unified Communications applications running in a virtual environment which meet certain criteria. For information on VMware specs-based support, see http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment.

Performing Failed RAID Disk Replacement With Single Restart for Linux Software RAID

Perform the following procedure to replace a failed RAID disk for these specific servers:

• MCS-7825-H3
• MCS-7828-H3

Procedure

Step 1 Log in to the console as an administrator and enter the CLI command show hardware.

Step 2 Check the status of the logical drives:
  – If the logical drive state is active or clean, you need not perform any further action.
  – If the logical drive state is degraded, check the physical disk status, as described in Step 3.
Step 3 Enter the CLI command **show hardware**, again and check the physical disk status:

- If none of the physical disks displays the state as “Removed”, you need not perform any further action.
- If the logical drive state is degraded, and any physical disk displays the state as “Removed”, identify the physical disk on the server as follows—The LED color of the failed disk will be amber or red.

You must perform Step 2 to verify the logical RAID drive Status and then perform Step 3 to verify the physical disk status.

To replace the failed drive and rebuild the RAID, continue with Step 4.

Step 4 Shut down the server using the CLI command **utils system shutdown**.

Step 5 After the system shuts down, replace the faulty hard disk with a new disk that is of the same type and size as the original disk and that comes from the same manufacturer—for example, Western Digital.

Step 6 Ensure that the new replacement disk is fully inserted.

Step 7 Power up the system.

Step 8 After the system is powered up, log in to the CLI and enter the CLI command **show hardware**.

In the **show hardware** command output, in the Logical Drive section, the Current Operation field will display Rebuild.

The status on the new, replaced hard disk will display spare rebuilding during the course of rebuilding. Rebuilding will take eight to 10 hours to complete. The duration depends on the size and I/O activity of the disk.

After the failed RAID disk replacement is complete, the status of both the logical drive and the new physical disk will display as clean and active.

---

**Warning**

If the failed disk is the first disk in the array, then replace it with a blank new disk that does not contain any partitions. However, if you replace the failed disk with a disk that was previously configured using HP RAID, the system will not be able to boot and this will result in a kernel panic.

---

**Software Upgrades**

**Note**

If you upgrade to the U.S. export unrestricted version of Unified CM, you will not be able to later upgrade to or be able to perform a fresh install of the U.S. export restricted version of this software. Note that IP phone security configurations will be modified to disable signaling and media encryption (including encryption provided by the VPN phone feature).

---

**Upgrading the Cisco Intercompany Media Engine Server**

When you upgrade the Cisco Intercompany Media Engine (Cisco IME) server from the Local Upgrade Directory, the system removes the ISO file from the local directory on your hard drive after the upgrade is complete. If you need to perform another upgrade using the same load, you must copy the ISO file to your local directory again or select a different source.
Installing Cisco Unified Communications Manager on a VM

During the installation process, the VM displays a message to indicate that the guest operating system has locked the CD-ROM door, and prompts you to disconnect and override the lock. This message displays twice during the installation process. Click No on each occurrence and continue the installation.

Command Line Interface

This section contains information about the following topics:

- delete dscp, page 6
- set accountlocking, page 6
- set accountlocking count, page 7
- set cli session timeout, page 7
- set dscp defaults, page 7
- set dscp disable, page 8
- set dscp enable, page 8
- set dscp marking, page 9
- set password change-at-login, page 9
- set password complexity character, page 10
- set password complexity character difference, page 11
- set password complexity character max-repeat, page 13
- set password expiry user maximum-age configure, page 12
- set webapp session timeout, page 13
- show cli session timeout, page 14
- show dscp all, page 14
- show dscp marking, page 14
- show dscp defaults, page 15
- show dscp status, page 15
- show password, page 16
- show password change-at-login, page 17
- show webapp session timeout, page 17
- utils create report, page 17
- utils os secure, page 18
- utils fips disable, page 18
- utils fips enable, page 18
- utils fips status, page 19
- utils sso enable, page 19
- utils os kernaldump enable, page 19
**delete dscp**

This command deletes a DSCP port tag.

**Command Syntax**

delete dscp port_tag

**Parameters**

- `port_tag` represents a DSCP port tag, which is a string that is mapped to a TCP or UDP port to identify the application that uses the port. It is the value of the portTag field displayed in the output of the command `show dscp defaults`. The set of port tags is predefined.

**Usage Guidelines**

When you delete an enabled port tag, DSCP marking on that port tag stops. You can recreate a deleted port tag by using the `set dscp marking` command; enter the name of the port tag that you previously deleted.

**set accountlocking**

This command enables and disables account locking after a user incorrectly enters his or her credentials.

**Note**

When you enable `set accountlocking`, account lockout notification gets automatically enabled when the audit logging function is also enabled. For more information, see the `utils auditd` command.

**Command Syntax**

set accountlocking [disable | enable | unlocktime seconds]

**Parameters**

- `disable`—Disables account locking for the current Unified CM administrator accounts
- `enable`—Enables account locking for the current Unified CM administrator accounts
- `unlocktime`—Configures the unlock time for the current Unified CM administrator accounts
- `seconds`—Specifies the unlock time in seconds.
  - Value range: 30—3600 seconds. (60 minutes).

**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes
set accountlocking count

This command sets the global consecutive failed login attempt count that triggers locking a user account.

**Note**

This command is only valid when account locking is enabled. If account locking is disabled, the system does not remember the account locking value and will use the default value, 3, when you enable account locking.

**Command Syntax**

```
set accountlocking count n
```

**Parameters**

- `n` specifies the number of consecutive failed login attempts before the system locks the user account.
  - Value range: 2—5
  - Default value: 3

**Usage Guidelines**

To change the global value for consecutive failed login attempts before the system locks a user account, execute this command.

set cli session timeout

This command sets the time, in minutes, after which an active CLI session times out and disconnects. Be aware that the new session timeout value becomes effective immediately for a new CLI session; however, existing sessions retain their original timeout value. Also the show cli session timeout command reflects the new value, even if the current session is not using it.

**Note**

This setting gets preserved through a software upgrade and does not get reset to the default value.

**Command Syntax**

```
set cli session timeout minutes
```

**Parameters**

- `minutes` specifies the time, in minutes, that can elapse before an active CLI session times out and disconnects.
  - Value range: 5—99999 minutes
  - Default value: 30 minutes

**Requirements**

- Command privilege level: 1
- Allowed during upgrade: No

set dscp defaults
This command sets the factory default DSCP settings for all of the port tags.

**Command Syntax**

set dscp defaults

**Usage Guidelines**

All non-default DSCP settings get removed when you run this command.

You can use the command `show dscp defaults` to see the factory default DSCP settings.

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

---

**set dscp disable**

This command disables DSCP marking on outgoing TCP or UDP packets. You can disable DSCP on a single port tag, or on all port tags at once.

**Command Syntax**

set dscp disable [all | port_tag]

**Parameters**

- `all` disables all DSCP port tags.
- `port_tag` represents a DSCP port tag, which is a string that is mapped to a TCP or UDP port to identify the application that uses the port. It is the value of the portTag field displayed in the output of the command `show dscp defaults`. The set of port tags is predefined.

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

---

**set dscp enable**

This command enables DSCP marking on outgoing TCP or UDP packets. You can enable DSCP on a single port tag, or on all port tags at once.

**Command Syntax**

set dscp enable [all | port_tag]

**Parameters**

- `all` enables all DSCP port tags.
- `port_tag` represents a DSCP port tag, which is a string that is mapped to a TCP or UDP port to identify the application that uses the port. It is the value of the portTag field displayed in the output of the command `show dscp defaults`. The set of port tags is predefined.
**Requirements**
Command privilege level: 1
Allowed during upgrade: No

**set dscp marking**

This command sets DSCP markings on port tags by using well-known DSCP classes and numeric values.

**Command Syntax**

```
set dscp marking port_tag value
```

**Parameters**
- `port_tag` represents a DSCP port tag, which is a string that is mapped to a TCP or UDP port to identify the application that uses the port. It is the value of the portTag field displayed in the output of the command `show dscp defaults`. The set of port tags is predefined.
- `value` is a DSCP value. You can enter the name of a well-known DSCP class, or a numeric value in decimal or hexadecimal format. Precede hexadecimal values with 0x or 0X.

**Usage Guidelines**
The valid class names as defined by DSCP are:
- **Class Selector:** values `CS0`, `CS1`, `CS2`, `CS3`, `CS5`, `CS6`, `CS7`
  The class selector (CS) values correspond to IP Precedence values and are fully compatible with IP Precedence.
- ** Expedited Forwarding:** value `EF`
  EF PHB is ideally suited for applications such as VoIP that require low bandwidth, guaranteed bandwidth, low delay, and low jitter.
- ** Best Effort:** value `BE`
  Also called default PHB, this value essentially specifies that a packet be marked with 0x00, which gets the traditional best-effort service from the network router.
- ** Assured Forwarding:** values `AF11`, `AF12`, `AF13`, `AF21`, `AF22`, `AF23`, `AF41`, `AF42`, `AF43`
  There are four types of Assured Forwarding classes, each of which has three drop precedence values. These precedence values define the order in which a packet will dropped (if needed) due to network congestion. For example packets, in AF13 class will be dropped before packets in the AF12 class.

**Requirements**
Command privilege level: 1
Allowed during upgrade: No

**set password change-at-login**

Use this command to force new or existing users to change their password when they log in to the system the next time.
Note: By default, this command is enabled for new users, so users will have to change their password the first time they log in to the system.

**Command Syntax**

`set password change-at-login {enable|disable} userid`

**Parameters**

- `enable` forces users to change their password when they log in to the system the next time.
- `disable` does not force users to change their password.
- `userid` specifies the affected user account.

**Requirements**

- Command privilege level: 4
- Allowed during upgrade: No

---

**set password complexity character**

This command enables password complexity rules for the type of characters in a password.

**Command Syntax**

`set password complexity character {enable|disable} [num-chars]`

**Parameters**

- `enable` turns on password complexity for types of characters.
- `disable` turns off password complexity for types of characters.

---

**Note**

Disabling password complexity also turns off password character difference, password character max repeat, and password history.

- `num-chars` specifies the number of characters required from each of the four character sets: lowercase, uppercase, numbers, and special characters.
  - Value range: 0—8
  - Default value: 1

---

**Note**

When you enable password complexity, this command also enables password history if it has not already been enabled (for more information, see the set password history command). If you had not previously enabled password history, the password history number parameter value gets set to 10. If you previously enabled password history with a value of less than 10, the value gets reset to 10 when you execute this command. If you previously enabled password history with a value of 10 or greater, the value remains unchanged when you execute this command.
Usage Notes

- When you enable password complexity, you must follow these guidelines when assigning a password:
  - It must have at least the current setting, num-chars, of lower-case character.
  - It must have at least the current setting, num-chars, of uppercase characters.
  - It must have at least the current setting, num-chars, of digit characters.
  - It must have at least the current setting, num-chars, of special characters.
  - You cannot use adjacent characters on the keyboard; for example, qwerty.
  - You cannot reuse any of the previous passwords that match the passwords retained by password history.
  - By default, the admin user password can only be changed only once during a 24-hour day.

Requirements

Command privilege level: 1
Allowed during upgrade: No

**set password complexity character max-repeat**

This command specifies the number of times you can consecutively repeat a single character in a new password.

**Command Syntax**

```
set password complexity character max-repeat num-repeat
```

**Parameters**

- `num-repeat` specifies the number of times you can consecutively repeat a single character in a new password.
  - Value range: 0—10
  - Default value: 0

Requirements

Command privilege level: 1
Allowed during upgrade: No

**set password complexity character difference**

This command specifies the number of characters that the character sequence in a new password must differ from the character sequence in the old password.

**Command Syntax**

```
set password complexity character difference num-chars
```


Parameters

`num-chars` specifies the number of characters that the character sequence in a new password must differ from the character sequence in the old password

- Value range: 0—31

Note

The maximum password length is 31 characters.

Usage Notes

Enter 0 to indicate no difference.

Requirements

Command privilege level: 1

Allowed during upgrade: No

---

**set password expiry user maximum-age configure**

This command sets the maximum number of days that a user password is valid.

Note

Before using this command, you must enable password maximum aging by using the `set password expiry maximum-age enable` command.

Command Syntax

```
set password expiry user maximum-age configure userid days
```

Parameters

- `userid` specifies the user account you want to configure
- `days` specifies the number of days that the user password is valid
  - Value range: 10—3650 days

Usage Notes

- To display the value for the maximum password age for a specific user account, enter the command `show password expiry user maximum-age`.
- If you disable password maximum aging by using the `set password expiry maximum-age disable` command, the system loses the password maximum-age values for specific user accounts.
- If you set the password maximum-age value on a system-wide basis by using the `set password age maximum` command, the password maximum-age values for specific user accounts get changed to the new system-wide default value.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes
**set password complexity character max-repeat**

This command specifies the number of times you can consecutively repeat a single character in a new password.

**Command Syntax**

`set password complexity character max-repeat num-repeat`

**Parameters**

`num-repeat` specifies the number of times you can consecutively repeat a single character in a new password.

- Value range: 0—10
- Default value: 0

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

**set webapp session timeout**

This command sets the time, in minutes, that can elapse before a web application, such as Unified CM Administration, times out and logs off the user.

For the new webapp session timeout setting to become effective, you must restart the Cisco Tomcat service. This command prompts you to restart the service.

⚠️ **Caution**

Restarting the Cisco Tomcat service ends all active sessions and can affect system performance. Cisco recommends that you only execute this command during off-peak traffic hours.

🔍 **Tip**

Until you restart the Cisco Tomcat service, the show webapp session timeout command reflects the new values, but system will continue to use the old values.

⚠️ **Note**

This setting gets preserved through a software upgrade and does not get reset to the default value.

**Command Syntax**

`set webapp session timeout minutes`

**Parameters**

`minutes` specifies the time, in minutes, that can elapse before a web application times out and logs off the user.

- Value range: 5—99999 minutes
- Default value: 30 minutes
show cli session timeout

This command displays the CLI session timeout value, which is the amount of time, in minutes, that can elapse before a CLI session times out and disconnects.

**Command Syntax**
show cli session timeout

**Parameters**
None

**Requirements**
Command privilege level: 1
Allowed during upgrade: No

show dscp all

This command displays the current DSCP traffic markings on all of the ports. It displays the DSCP markings in decimal and hexadecimal. If the value corresponds to a class then it displays the correct class. If the value does not correspond to a class then it displays N/A.

**Command Syntax**
show dscp all

**Requirements**
Command privilege level: 0
Allowed during upgrade: No

show dscp marking

This command displays the current DSCP traffic markings for a particular DSCP value.

**Command Syntax**
show dscp marking value

**Parameters**
value is a DSCP value. You can enter the name of a well-known DSCP class, or a numeric value in decimal or hexadecimal format. Precede hexadecimal values with 0x or 0X.

**Usage Guidelines**
The valid class names as defined by DSCP are:
Class Selector: values CS0, CS1, CS2, CS3, CS5, CS6, CS7
The class selector (CS) values correspond to IP Precedence values and are fully compatible with IP Precedence.

Expedited Forwarding: value EF
EF PHB is ideally suited for applications such as VoIP that require low bandwidth, guaranteed bandwidth, low delay, and low jitter.

Best Effort: value BE
Also called default PHB, this value essentially specifies that a packet be marked with 0x00, which gets the traditional best-effort service from the network router.

Assured Forwarding: values AF11, AF12, AF13, AF21, AF22, AF23, AF41, AF42, AF43
There are four types of Assured Forwarding classes, each of which has three drop precedence values. These precedence values define the order in which a packet will dropped (if needed) due to network congestion. For example packets, in AF13 class will be dropped before packets in the AF12 class.

Requirements
Command privilege level: 1
Allowed during upgrade: No

show dscp defaults

This command displays the default factory DSCP settings. These values will take effect if the set dscp defaults command is executed.

Command Syntax
show dscp defaults

Requirements
Command privilege level: 0
Allowed during upgrade: No

show dscp status

This command displays the current DSCP traffic markings.

Command Syntax
show dscp status [enabled | disabled]

Parameters
- enabled filters the output to show only DSCP traffic markings that are enabled. If you do not specify a status, this is the default filter.
- disabled filters the output to show only DSCP traffic markings that are disabled

Requirements
Command privilege level: 0
show password

This command displays the information about the configured password.

Command Syntax

show password

- age—displays information about the configured password age parameters
- complexity [character | length]—displays password complexity or length parameters for OS accounts.
- expiry [minimum-age | maximum-age]—displays the configured password expiration parameters.
- expiry user [minimum-age | maximum-age]—displays the configured password expiration parameters for the specified user.
- expiry user list—Displays both the password maximum age and password minimum age for each CLI user defined in the system.
- history—displays the number of passwords that will be maintained in the history for OS administration accounts.
- inactivity—displays the status of the password inactivity for OS accounts. Password inactivity is the number of days of inactivity after a password has expired before the account is disabled.

Parameters

- `character`—Displays the status of the password complexity as enabled or disabled
- `length`—Displays the minimum length of passwords that get used for OS accounts. The default specifies 6.
- `minimum-age`—Displays the minimum number of days set for password expiry
- `maximum-age`—Displays the maximum number of days for set password expiry

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Usage Notes

When password complexity is enabled, you must follow these guidelines when assigning a password:

- It must have at least one lower-case character.
- It must have at least one uppercase, one digit, and one special character.
- You cannot use adjacent characters on the keyboard.
- You cannot reuse any of the previous ten passwords.
- The admin user password can only be changed only once in 24 hours.
**show password change-at-login**

This command displays whether a user will be forced to change passwords when the user logs in to the system the next time.

**Command Syntax**
```
show password change-at-login userid
```

**Parameters**
- `userid` specifies the user account you want to display

**Requirements**
- Command privilege level: 1
- Allowed during upgrade: No

**show webapp session timeout**

This command displays the webapp session timeout value, which is the amount of time, in minutes, that can elapse before a web application times out and logs off the user.

**Command Syntax**
```
show webapp session timeout
```

**Parameters**
- None

**Requirements**
- Command privilege level: 0
- Allowed during upgrade: Yes

**utils create report**

For SELinux, this command creates reports about the server in the platform/log directory.

**Command Syntax**
```
utils create report [security]
```

**Parameters**
- `security`—collects the diagnostic reports and creates a TAR file that you can download for troubleshooting purposes. You can retrieve this file by using the `file get` command.

**Usage Guidelines**
- You are prompted to continue after you enter the command.
- After creating a report, use the command `file get activelog platform/log/filename`, where `filename` specifies the report filename that displays after the command completes, to get the report.
**utils os secure**

This command monitors and controls SELinux.

**Command Syntax**

```
utils os secure [status | enforce | permissive]
```

**Parameters**

- **status**—displays SELinux mode (enforcing or permissive) to the CLI user.
- **enforce** allows the CLI user to change the SELinux mode from permissive to enforce. SELinux will block actions or events based on the defined policies when it is in enforce mode.
- **permissive** allows the CLI user to change the SELinux mode from enforce to permissive. SELinux will log, but not block, actions or events when it is in permissive mode.

**Usage Guidelines**

If SELinux is enabled, you do not have to reboot when you use `utils os secure enforce` or `utils os secure permissive`.

If SELinux is disabled, you can use `utils os secure enforce` or `utils os secure permissive` to enable it. If you do this; however, you must reboot before SELinux becomes enabled.

**utils fips disable**

This command disables FIPS mode.

**Command Syntax**

```
utils fips disable
```

**Requirements**

- Command privilege level: 0
- Allowed during upgrade: No

**utils fips enable**

This command enables FIPS mode.

**Caution**

Before enabling FIPS mode, a system backup should be performed.
Command Syntax
utils fips enable [reboot]

Requirements
Command privilege level: 0
Allowed during upgrade: No

**utils fips status**

This command lets you check the status of FIPS mode.

Command Syntax
utils fips status

Requirements
Command privilege level: 0
Allowed during upgrade: No

**utils sso enable**

This command lets you to enable and configure SSO-based authentication.

Command Syntax
utils sso enable

Parameters
enable—Enables SSO-based authentication. This command starts a single sign on configuration wizard.

**utils os kerneldump enable**

*Note*
The netdump commands have been removed from release 8.6(1) and have been replaced with the kerneldump commands.

This command configures kerneldump to provide a kernel crash dumping mechanism. The kernel captures the dump to the local disk, in case of a kernel crash.

*Note*
The MCS-7835-H2 and MCS-7845-H2 models do not support this command.

Command Syntax
utils os kerneldump enable
Parameters
None

Usage Guidelines
If a kernel crash occurs, the capture kernel dumps the core on the local disk of the server. The primary kernel reserves 128MB of physical memory that the capture kernel uses to boot. The kerneldump uses kexec command to boot into a capture kernel whenever the kernel crashes.
This command reboots the system for the changes to come into effect.

Requirements
Command privilege level: 1
Allowed during upgrade: true

Example
admin:utils os kerneldump enable
***************WARNING*****************
Enabling kerneldump requires system reboot
Would you like to reboot the machine(y/n):y

kerneldump enable operation succeeded
System going for a reboot

Retrieving core files
The core files are dumped to /var/log/install/crash location. You can collect these files by using the file get install command.

Example
admin: file get install crash/127.0.0.1-2011-03-15-13:59:02/vmcore

where
- 127.0.0.1-2011-03-15-13:59:02 is the crash directory indicating the time of kernel crash
- vmcore is the dump file that contains the system information during kernel crash.

utils os kerneldump disable

This command disables the kerneldump service; dumps are not captured after this.

Note
The MCS-7835-H2 and MCS-7845-H2 models do not support this command.

Command Syntax
utils os kerneldump disable

Parameters
None
Usage Guidelines
This command frees the memory reserved for the crash kernel and the dumps are not collected in case of a kernel panic. This command reboots the system for the changes to come into effect.

Requirements
Command privilege level: 1
Allowed during upgrade: true

Example
admin:utils os kerneldump disable
***************WARNING***************
Disabling kerneldump requires system reboot
Would you like to continue(y/n):y

kerneldump disable operation succeeded
System going for a reboot.

utils os kerneldump status
This command states if the kerneldump service is enabled or disabled.

Note
The MCS-7835-H2 and MCS-7845-H2 models do not support this command.

Command Syntax
utils os kerneldump status

Parameters
None

Usage Guidelines
User can query the status of the kerneldump service.

Requirements
Command privilege level: 1
Allowed during upgrade: true

Example
admin: utils os kerneldump status
kerneldump is enabled

utils os kerneldump ssh enable
This command configures an external SSH server as a kerneldump server to collect kernel dumps.

Command Syntax
utils os kerneldump ssh enable
Parameters

ip_address

Usage Guidelines
If a kernel crash occurs, the capture kernel dumps the core on the external server that is configured to collect the dump. This command reboots the system for the changes to come into effect.

Requirements
Command privilege level: 1
Allowed during upgrade: true

Example
admin:utils os kerneldump ssh enable 10.77.31.60

******************WARNING******************
Enabling kerneldump requires system reboot
Would you like to reboot the machine(y/n): y
Enter server username: root
Enter server password:
Do you wish to change dump location ?(y/n):y
Enter new dump location: /root/abc
Your core will be dumped to /root/abc on 10.77.31.60
kerneldump enable operation succeeded
System going for a reboot

utils os kerneldump ssh disable

This command removes support of the external SSH server that is configured to collect kernel dumps.

Command Syntax
utils os kerneldump ssh disable

Parameters

ip_address

Usage Guidelines
If a kernel panic occurs, the capture kernel does not dump the core to external server. This command reboots the system for the changes to come into effect.

Requirements
Command privilege level: 1
Allowed during upgrade: true

Example
admin:utils os kerneldump ssh disable 10.77.31.60

******************WARNING******************
Disabling kerneldump requires system reboot
Would you like to continue(y/n):y
kerneldump disable operation succeeded
System going for a reboot

**utils os kerneldump ssh status**

This command states if an external SSH server is configured or not, to collect kernel dumps.

**Command Syntax**

tools os kerneldump ssh status

**Parameters**

None

**Usage Guidelines**

User can query the status of the kerneldump service for external SSH server. If an external server is configured to collect dumps, the output of the command is *enabled*; if not, the output is *disabled*.

**Requirements**

Command privilege level: 1
Allowed during upgrade: true

**Example**

admin:utils os kerneldump ssh status

Dumping to external server is disabled

---

**Cisco Unified Communications Manager Administration**

This section contains information about the following topics:

- New and Updated Enterprise and System Parameters, page 23
- Menu Changes, page 24

**New and Updated Enterprise and System Parameters**

**Enterprise Parameters**

No new or updated enterprise parameters exist in Cisco Unified Communications Manager 8.6(1).

**Service Parameters**

To access the service parameters in Cisco Unified Communications Manager Administration, choose System > Service Parameters. Choose the server and the service name that the parameter supports. For some parameters, you may need to click Advanced to display the service parameter. To display the help for the service parameter, click the name of the service parameter in the window.
• Enable Source IP Address Verification for Software Media Devices—Use this parameter to
determine whether the source IP address of the An nunciator and Music On Hold servers are verified
to be registered Cisco Unified Communications Manager nodes in the cluster. This parameter is
applicable only when the enterprise parameter Cluster Security Mode is set to 1 (mixed mode).
• Disable G.711u-law (64 kb/s and 56 kb/s) and G.711a-law (64 kb/s and 56 kb/s) codecs—Disable
these parameters to minimize use of transcoders during Consult Conference/Transfer when you use
BIB Recording. When you disable both codecs, Cisco Unified Communications Manager will
reference the Static Selection Table and select the next available codec that devices and applications
support.
• Locations-based Maximum Bandwidth Enforcement Level for MLPP Calls—Use this parameter to
determine the level of bandwidth restriction that Cisco Unified Communications Manager enforces
for a location when bandwidth reaches the threshold of becoming oversubscribed.
• SIP V.150 Outbound SDP Offer Filtering—Use this parameter to set the SIP V.150 outbound SDP
offer filtering option. This parameter determines whether the SIP trunk performs filtering on
transmitted SDP offers to remove MER or pre-MER V.150 content. Valid values specify No Filtering
(the SIP trunk does not perform any filtering on outbound V.150 SDP lines); Remove MER V.150
(the SIP trunk removes MER lines in outbound SDP offers; use this value to reduce ambiguity when
a trunk is connected to a pre-MER V.150 Unified CM); or Remove Pre-MER V.150 (the SIP trunk
removes any non-MER-compliant lines in outbound SDP offers; if your cluster is contained within
a network of MER-compliant devices that are incapable of processing an offer with pre-MER lines,
choose this value). This is a required field and the default is No Filtering.

Menu Changes

Main Window
No changes exist for the main window.

System
The System menu contains the following updates:

• Region—In the Modify Relationships to Other Regions area of the Region Configuration window,
there is a new Max Audio Bit Rate selection in the drop-down list box. This new rate is 128 kb/s
(AAC-LD[LATM]). This new rate supports the AAC-LD (MP4A-LATM) codec. AAC-LD
(MP4A-LATM) is supported for SIP devices including Tandberg and some third-party endpoints.
• Region—In the Region Configuration window, there are two new codecs included in the Max Audio
Bit Rate drop-down list box, the AMR and AMR-WB codecs. Both codecs support SIP devices.
AMR-WB is preferred by Unified CM over AMR and other supported codecs, G.711 in particular.
• Security—In the SIP Trunk Security Profile Configuration window, there is a new SIP V.150
Outbound SDP Offer Filtering drop-down list box that contains the following filtering options:
  – Use Default Filter—The SIP trunk uses the default filter that is indicated in the SIP V.150
Outbound SDP Offer Filtering service parameter. To locate the service parameter, go to System
> Service Parameters > Clusterwide Parameters (Device-SIP) in Cisco Unified
Communications Manager Administration.
  – No Filtering—The SIP trunk performs no filtering of V.150 SDP lines in outbound offers.
  – Remove MER V.150—The SIP trunk removes V.150 MER SDP lines in outbound offers. Select
this option to reduce ambiguity when the trunk is connected to a pre-MER V.150 Cisco Unified
Communications Manager.
- Remove Pre-MER V.150—The SIP trunk removes any non-MER compliant V.150 lines in outbound offers. Select this option to reduce ambiguity when your cluster is contained in a network of MER compliant devices that are incapable of processing offers with pre-MER lines.

- **Codec Enhancements for G.722.1 and AAC-LD (MP4A-LATM)**
  - **Region**—In the Region Configuration window in the Max Audio Bit Rate drop-down list box, the 32 kb/s bit rate includes the G.722.1 codec.

### Call Routing
No updates or new fields exist for this menu.

### Advanced Features
No updates or new fields exist for this menu.

### Media Resources

#### Media Resources > Conference Bridge
Four new options have been added to the Conference Bridge Type drop-down menu. When you select any of the four new Conference Bridge Types, a new menu page appears with configuration settings for that particular Conference Bridge Type. The four new options are as follows:

- Cisco IOS Heterogeneous Video Conference Bridge (see Conferencing with Cisco Integrated Services Routers Generation 2, page 39)
- Cisco IOS Homogeneous Video Conference Bridge (see Conferencing with Cisco Integrated Services Routers Generation 2, page 39)
- Cisco IOS Guaranteed Audio Video Conference Bridge (see Conferencing with Cisco Integrated Services Routers Generation 2, page 39)
- Cisco TelePresence MCU (see Cisco TelePresence MCU Conference Bridge, page 32)

#### Device
The Device menu contains the following updates:

- **Device > Device Settings > SIP Profile**—New fields were added to the SIP Profile configuration window:
  - SDP Session-level Bandwidth Modifier for Early Offer and Re-invites—This drop-down menu indicates which Session Level Bandwidth Modifier Unified CM includes in outbound offers. This configuration can be applied to both the SIP line side device and SIP trunk device. (see Session Level Bandwidth Modifiers, page 56.)
  - User-Agent and Server header information—This drop-down menu indicates how Unified CM handles the User-Agent and Server header information in a SIP message. (see User-Agent and Server Header Information, page 61.)
  - Require SDP Inactive Exchange for Mid-Call Media Change—This check box indicates how Cisco Unified Communications Manager handles mid-call updates to codecs or connection information such as IP address or port numbers. (see Require SDP Inactive Exchange for Mid-Call Media Change, page 53.)
  - Use Fully Qualified Domain Name in SIP Requests—This check box is checked to enable Unified CM relay an alphanumeric hostname of a caller by passing it through to the called device or outbound trunk as a part of the SIP header information. (see Use Fully Qualified Domain Name in SIP Requests, page 60.)
- Allow Presentation Sharing using BFCP—This check box is checked to enable presentation sharing using the Binary Floor Control Protocol. (see Binary Floor Control Protocol, page 28.)

- **Device > Device Settings > Feature Control Policy**—In the Feature Control Section area of the Feature Control Policy Configuration window, seven new features have been added:
  - Call PickUp
  - Group Call PickUp
  - Meet Me
  - Mobility
  - Other Call PickUp
  - Report Caller
  - Report Quality

**Application**

No updates or new fields exist for this menu.

**Bulk Administration**

No updates or new fields exist for this menu.

---

**Cisco Unified Communications Manager Features and Applications**

This section contains information about the following topics:

- BAT Changes, page 27
- Binary Floor Control Protocol, page 28
- Called Party Trace, page 29
- Certificate Management, page 31
- Cisco TelePresence MCU Conference Bridge, page 32
- Codec Enhancements for AMR and AMR-WB, page 33
- Codec Enhancements for G.722.1 and AAC-LD (MP4A-LATM), page 35
- Codec Enhancements for iLBC, page 38
- Conferencing with Cisco Integrated Services Routers Generation 2, page 39
- Destination Code Control, page 40
- Dynamic DSCP Tagging, page 41
- Federal Information Processing Standard (FIPS) 140-2, page 43
- iSAC Enable and Disable Support, page 44
- Mapping MLPP Precedence to DSCP Values, page 45
- Message Waiting Indicator for Route Lists with a SIP Trunk, page 46
- MLPP Location-Based CAC Enhancements, page 46
- Mobility Feature Enhancements, page 49
- P-Charging Vector (PCV) Support for Unified CM, page 52
- Require SDP Inactive Exchange for Mid-Call Media Change, page 53
- SRTP for Annunciator and Music On Hold, page 54
- Session Level Bandwidth Modifiers, page 56
- Single Sign On, page 57
- Transparency for REFER Without Replaces, page 58
- Use Fully Qualified Domain Name in SIP Requests, page 60
- User-Agent and Server Header Information, page 61
- V.150.1 MER SCIP 216, page 62
- Video Encryption, page 63
- Video and Interoperability Enhancements, page 65

**BAT Changes**

You can export the DCC details through the Import/Export menu in BAT.

To export DCC details through BAT, go to **Bulk Administration > Import/Export > Export**. Select the Route Pattern entity for export. The DCC details are found under Call Routing Data.

For more details about Import/Export, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

**GUI Changes**

No GUI changes exist for this feature.

**Service Parameter and Enterprise Parameter Changes**

No service or enterprise parameter changes exist for this feature.

**Installation/Upgrade (Migration) Considerations**

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

**Serviceability Considerations**

No serviceability considerations exist for this feature.

**CAR/CDR Considerations**

No CAR or CDR considerations exist for this feature.

**Security Considerations**

No security considerations exist for this feature.

**User Tips**

No user tips exist for this feature.
Binary Floor Control Protocol

Description
In this release, Cisco Unified Communications Manager introduces support for presentation sharing within an ongoing video conversation using the Binary Floor Control Protocol (BFCP).

BFCP is negotiated between two video endpoints using the SIP protocol. Cisco Unified Communications Manager aids in the negotiation of BFCP by relaying messages between the two endpoints until a session can be established. This negotiation involves establishing a floor, which is a temporary permission to access shared resources. The BFCP stream is a point-to-point stream between the endpoints. The BFCP stream itself never hits Cisco Unified Communications Manager.

The following example shows how presentation sharing works:
An ongoing video conversation exists between two video phones. User A decides to show User B a slide presentation that is saved on a laptop. User A attaches the laptop to a Cisco EX90 video phone and presses the Present button on the phone. The SIP INVITE message gets initiated to the other phone, forming the invitation for a BFCP stream. After the BFCP session is negotiated, an additional stream is added to the audio and video streams. The BFCP stream allows User B to see the desktop on User A’s laptop.

BFCP is only supported on SIP networks. The entire network, including the endpoints and all the intermediary devices and trunks, must be SIP. BFCP must be enabled on all trunks and lines.

Note
Cisco Unified Communications Manager does not support BFCP when it is used between Cisco Unified Communications Manager and a Cisco TelePresence MCU.

Cisco Unified Communications Manager will reject the BFCP stream in the following scenarios:
- The Allow Presentation Sharing using BFCP check box in the SIP Profile window is unchecked for one of the SIP lines or trunks in the network.
- One endpoint offers BFCP, but the other does not.
- The SIP line or SIP trunk uses MTP, TRP, or Transcoder. In this case, BFCP functionality is not supported.
- The stream is between a SIP and non-SIP endpoint. BFCP is supported only on SIP endpoints.

Cisco Unified Communications Manager Administration Configuration Tips
BFCP is enabled in Cisco Unified Communications Manager by checking the Allow Presentation Sharing using BFCP check box on the SIP Profile Configuration window. If the check box is unchecked, all BFCP offers will be rejected. By default, the check box is unchecked.

BFCP is supported only on full SIP networks. For presentation sharing to work, BFCP must be enabled for all SIP endpoints as well as all SIP lines and SIP trunks between the endpoints.

GUI Changes
The Allow Presentation Sharing using BFCP check box has been added to the SIP Profile window.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.
**Installation/Upgrade (Migration) Considerations**
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.6(1), you can use this feature.

**Serviceability Considerations**
No serviceability considerations exist for this feature.

**BAT Considerations**
No BAT considerations exist for this feature.

**CAR/CDR Considerations**
No CAR or CDR considerations exist for this feature.

**Security Considerations**
No security considerations exist for this feature.

**AXL and CTI Considerations**
No AXL or CTI considerations exist for this feature.

**User Tips**
No user tips exist for this feature.

---

**Called Party Trace**

**Description**
Called Party Trace allows you to configure a directory number or list of directory numbers that you want to trace. You can request on-demand tracing of calls by using the Session Trace Tool.

The Called Party Trace feature provides information about the calling party number in addition to the called party number within a node. You can use the information from each node to trace a call back to the originator.

**Unified CM Administration Configuration Tips**
Use the Advanced Features menu in Cisco Unified Communications Manager Administration to add DNs. Once the call log information has been generated, you can use the Real Time Monitoring Tool to view logs for specific DNs.

**GUI Changes**
No GUI changes exist for this feature.

**Service Parameter and Enterprise Parameter Changes**
No service or enterprise parameter changes exist for this feature.

**Installation/Upgrade (Migration) Considerations**
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.
Serviceability Considerations

Note
You must be an authorized administrator to access the directory number logs. To grant authorization to a specific role using Role Configuration, the “Called Party Tracing” resource must have read permission enabled for the role.

Procedure

To access the DN Trace report in the Real Time Monitoring Tool (RTMT), follow these steps:

1. From the RTMT menu, choose CallManager > Callprocess > Called Party Trace. Or, Click the CallManager tab; then, click Called Party Trace.

2. Choose the start time of the report using the drop-down box list.

   Note
   The start time cannot be older than five years from the current date.

3. The report shows the following information
   - Start time
   - Calling directory number
   - Original called directory number
   - Called directory number
   - Calling device name
   - Called device name

   Note
   When 5 megabytes of trace file entries have been written to the log files being accessed by RTMT, the oldest log information is overwritten by new trace entries as they are recorded. The RTMT will only list a maximum of 500 entries for any given search.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.
Certificate Management

Description
The following certificate management features have been added for this release:

- The Cisco Unified Communications Manager certificate management backend has been migrated to a Federal Information Processing Standards (FIPS) compliant cryptographic library that meets the United States government security standards. No additional configuration is required by the user to access this feature.

- The certificate management feature has been extended to support multiple levels of certificates rather than the two levels previously supported. In this release, certificate management supports a PKCS #7 format certificate chain that can contain leaf certificates and all its issuer certificates as well as the X509 format certificates for the leaf certificate and the immediate issuer certificate.

- You can configure Cisco Unified Communications Manager so that the revocation status of the certificate is checked using the online certificate status protocol (OCSP) during the certificate upload. The revocation status gets reported to Cisco Unified Communications Manager. You can use RTMT or the file list activelog/platform/certMgmt CLI command to view the revocation status of a certificate. If you use the CLI command, you can search for “OCSP status” to find the information that you need.

Note
Before you enable OCSP, you must upload the OCSP Responder certificate in Certificate Management’s tomcat-trust.

Unified CM Administration Configuration Tips
No Cisco Unified Communications Manager configuration tips exist for this feature.

GUI Changes
In the Cisco Unified Communications Operating System, the following changes exist:


- The Upload Certificate dialog box no longer contains a root certificate field as you no longer need to identify the root certificate when uploading the signed certificate.

- The Certificate Revocation window (Security > Certificate Revocation) has been added to allow you to enable or disable OCSP. To configure OCSP, you must upload the OCSP Responder certificate in Certificate Management's tomcat-trust. Then, you check the OCSP and enter the OCSP configured URI on the Certificate Revocation window.

Service Parameter and Enterprise Parameter Changes
No Service Parameter and Enterprise Parameter Changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
You can use the Real Time Monitoring Tool (RTMT) to check a certificate revocation status. Use the following alarms in RTMT under the SysLog Viewer menu:

- CertificateRevoked—A revoked certificate is found during upload of Certificate/Certificate chain
• CertificateRevocationStatusByOCSP—One of the following messages appear with this alarm:
  – Could not determine certificate revocation status.
  – OCSP responder certificate is not found in tomcat-trust.
  – Cannot contact OCSP Responder.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No Security Considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

Cisco TelePresence MCU Conference Bridge

Description
Cisco TelePresence MCU refers to a set of hardware conference bridges for Cisco Unified Communications Manager.

The Cisco TelePresence MCU is a high-definition (HD) multipoint video conferencing bridge. It delivers up to 1080p at 30 frames per second, full continuous presence for all conferences, full transcoding, and is ideal for mixed HD endpoint environments.

The Cisco TelePresence MCU supports SIP as the signaling call control protocol. It has a built-in Web Server that allows for complete configuration, control and monitoring of the system and conferences. The Cisco TelePresence MCU provides XML management API over HTTP.

Cisco TelePresence MCU allows both ad hoc and meet-me voice and video conferencing. Each conference bridge can host several simultaneous, multiparty conferences.

GUI Changes
A new Conference Bridge Type has been added to the drop down menu on the Conference Bridge Configuration window of Cisco Unified Communications Manager. When you select Cisco TelePresence MCU from the Conference Bridge Type drop down menu, a new window appears with configuration settings for Cisco TelePresence MCU conference bridge.

For more detailed information about how to configure the Cisco TelePresence MCU conference bridge, see the Cisco Unified Communications Manager Administration Guide.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.
Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

Codec Enhancements for AMR and AMR-WB

Description
AMR—Adaptive Multi-Rate (AMR) codec is the required standard codec for 2.5G/3G wireless networks based on GSM (WDMA, EDGE, GPRS). This codec encodes narrowband (200-3400 Hz) signals at variable bit rates ranging from 4.75 to 12.2 kb/s with toll quality speech starting at 7.4 kb/s.

AMR is supported only for SIP devices.

AMR-WB—Adaptive Multi-Rate Wideband (AMR-WB) is codified as G.722.2, an ITU-T standard speech codec, formally known as Wideband coding of speech for about 16 kb/s. This codec is preferred since it provides excellent speech quality due to a wider speech bandwidth of 50 Hz to 7000 Hz compared to other narrowband speech codecs.

AMR-WB is supported only for SIP devices.

Note
AMR-WB is preferred by Unified CM over AMR and other supported codecs, G.711 in particular.

The audio codec preference feature orders the audio preference table (Table 1) for the default low-loss case by sound quality, and the table adds a separate preference list for the lossy case. For audio and video calls, Cisco Unified Communications Manager uses the preference order of codecs in Table 1. When you configure the maximum audio bit rate setting in the Region Configuration window (or use the service parameter in the Service Parameter Configuration window), this setting serves as a filter. When an audio codec is selected for a call, Cisco Unified Communications Manager takes the matching codecs from both sides of a call leg, filters out the codecs that exceed the configured maximum audio bit rate, and then picks the preferred codec among the codecs that are remaining in the list.
Bandwidth Calculations

In performing location bandwidth calculations for purposes of call admission control, Unified CM assumes that each call stream consumes the following amount of bandwidth:

- AMR call uses 12.2 kb/s.
- AMR-WB call uses 23.85 kb/s.

Table 1 describes the various supported audio media types:

<table>
<thead>
<tr>
<th>Type</th>
<th>Encoding Name</th>
<th>Payload Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMR</td>
<td>AMR</td>
<td>Dynamically</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>AMR-WB</td>
<td>AMR-WB</td>
<td>Dynamically</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
</tbody>
</table>
Table 3  Codec Types

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>97</td>
<td>AMR</td>
</tr>
<tr>
<td>98</td>
<td>AMR-WB</td>
</tr>
</tbody>
</table>

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

Codec Enhancements for G.722.1 and AAC-LD (MP4A-LATM)

Description
The G.722.1 codec is a low-complexity wideband codec operating at 24 and 32 kb/s. The audio quality approaches that of G.722 while using at most half the bit rate. As it is optimized for both speech and music, G.722.1 has slightly lower speech quality than the speech-optimized iSAC codec. G.722.1 is supported for calls between SIP and H.323 endpoints.

The Advanced Audio Coding-Low Delay (AAC-LD) Low-overhead MPEG-4 Audio Transport Multiplex (LATM) codec is a super-wideband audio codec that provides superior sound quality for voice and music. This codec provides equal or improved sound quality over older codecs, even at lower bit rates.

AAC-LD (MP4A-LATM) is supported for SIP devices including Tandberg and some third-party endpoints.

Note
AAC-LD (mpeg4-generic) and AAC-LD (MPA4-LATM) are not compatible.

Unified CM Administration Configuration Tips
The following tables are helpful when using Region Configuration.

The total bandwidth that is used per call stream depends on the audio codec type as well as factors such as data packet size and overhead (packet header size), as indicated in Table 4.

Note
Each call includes two streams, one in each direction.

Note
For information about bandwidth usage for each codec, see the Cisco Unified Communications Solution Reference Network Design (SRND) for the current release of Cisco Unified Communications Manager.
The audio codec preference feature orders the audio preference table (Table 4) for the default low-loss case by sound quality, and the table adds a separate preference list for the lossy case. For audio and video calls, Cisco Unified Communications Manager uses the preference order of codecs in Table 4. When you configure the maximum audio bit rate setting in the Region Configuration window (or use the service parameter in the Service Parameter Configuration window), this setting serves as a filter. When an audio codec is selected for a call, Cisco Unified Communications Manager takes the matching codecs from both sides of a call leg, filters out the codecs that exceed the configured maximum audio bit rate, and then picks the preferred codec among the codecs that are remaining in the list.

### Table 4 Audio Codec Preference Order for Cisco Unified Communications Manager 8.6(1)

<table>
<thead>
<tr>
<th>If Low Loss Is Configured for Link Loss Type</th>
<th>If Lossy Is Configured for Link Loss Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAC-LD (MP4A-LATM)—128 kb/s</td>
<td>AAC-LD (MP4A-LATM)—128 kb/s</td>
</tr>
<tr>
<td>AAC-LD (mpeg4-generic)—256 kb/s</td>
<td>AAC-LD (mpeg4-generic)—256 kb/s</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)—64 kb/s</td>
<td>AAC-LD (MP4A-LATM)—64 kb/s</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)—56 kb/s</td>
<td>AAC-LD (MP4A-LATM)—56 kb/s</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)—48 kb/s</td>
<td>AAC-LD (MP4A-LATM)—48 kb/s</td>
</tr>
<tr>
<td>iSAC—32 kb/s</td>
<td>AAC-LD (MP4A-LATM)—32 kb/s</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)—32 kb/s</td>
<td>G.722 64k—64 kb/s</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)—24 kb/s</td>
<td>AAC-LD (MP4A-LATM)—24 kb/s</td>
</tr>
</tbody>
</table>

For audio calls that involve H.323 intercluster trunks, Cisco Unified Communications Manager uses the preference list of codecs in Table 4 only if both sides of the call run Cisco Unified Communications Manager 8.6(1). If both sides of the call do not run Cisco Unified Communications Manager 8.6(1), the codec list from Table 5 gets used.

### Table 5 Audio Codec Preference Order for H.323 Intercluster Trunks If Both Sides of Call Do Not Support Cisco Unified Communications Manager 8.6(1)

<table>
<thead>
<tr>
<th>If Low Lossy Is Configured for Link Loss Type</th>
<th>If Lossy Is Configured for Link Loss Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAC-LD (mpeg4-generic)—256 kb/s</td>
<td>AAC-LD (mpeg4-generic)—256 kb/s</td>
</tr>
</tbody>
</table>

Table 6 describes the various supported audio media types:

### Table 6 Supported Audio Media Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Encoding Name</th>
<th>Payload Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.722.1</td>
<td>G7221</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>AAC-LD (mpeg4-generic)</td>
<td>mpeg4-generic</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)</td>
<td>MP4A-LATM</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
</tbody>
</table>
GUI Changes
In the Region Configuration window in the Max Audio Bit Rate drop-down list box, the 32 kb/s bit rate includes the G.722.1 codec.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
Table 7 contains the compression and payload types that may appear in the codec fields.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>AAC-LD (mpeg4-generic)</td>
</tr>
<tr>
<td>43</td>
<td>AAC-LD (MP4A-LATM) 128K</td>
</tr>
<tr>
<td>44</td>
<td>AAC-LD (MP4A-LATM) 64K</td>
</tr>
<tr>
<td>45</td>
<td>AAC-LD (MP4A-LATM) 56K</td>
</tr>
<tr>
<td>46</td>
<td>AAC-LD (MP4A-LATM) 48K</td>
</tr>
<tr>
<td>47</td>
<td>AAC-LD (MP4A-LATM) 32K</td>
</tr>
<tr>
<td>48</td>
<td>AAC-LD (MP4A-LATM) 24K</td>
</tr>
</tbody>
</table>

The following are CDR examples for AAC-LD calls.
Advanced Audio Coding-Low Delay (AAC-LD) is a super-wideband codec that provides excellent speech and music quality at various bit rates. The audio quality scales up with the bit rate. Two mutually incompatible RTP payload formats are supported: mpeg4-generic and MP4A-LATM.

For AAC-LD (mpeg4-generic) calls, the codec type (payload capability) value 42 is used.

For AAC-LD (MP4A-LATM) calls, a separate codec type value is used for each supported bit rate. The codec type values are 43 (128K), 44 (64K), 45 (56K), 46 (48K), 47 (32K), and 48 (24K).

The system adds an audio bandwidth field to the CDR for AAC-LD calls.
The system populates the bandwidth fields based on the following table:
Codec Enhancements for iLBC

The Internet Low Bit Rate Codec (iLBC) provides audio quality between that of G.711 and G.729 at bit rates of 15.2 and 13.3 kb/s, while allowing for graceful speech quality degradation in a lossy network due to the speech frames being encoded independently. By comparison, G.729 does not handle packet loss, delay, and jitter well, due to the dependence between speech frames. iLBC is supported for SIP, SCCP, H323, and MGCP devices.

GUI Changes
No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.
**BAT Considerations**
No BAT considerations exist for this feature.

**CAR/CDR Considerations**
No CAR or CDR considerations exist for this feature.

**Security Considerations**
No security considerations exist for this feature.

**AXL and CTI Considerations**
No AXL or CTI considerations exist for this feature.

**User Tips**
No user tips exist for this feature.

---

**Conferencing with Cisco Integrated Services Routers Generation 2**

Cisco Integrated Services Routers Generation 2 (ISR G2) can be enabled to act as an IOS-based conference bridge that supports ad hoc and meet-me audio and video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge.

Within Cisco Unified Communications Manager, the ISR G2 can be configured as one of three Conference Bridge Types:

- **Cisco IOS Homogeneous Video Conference Bridge**—This conference bridge type supports homogeneous video conferences. A homogeneous video conference is a video conference in which all participants connect to the conference bridge using the same video format attributes. The conference bridge sends the same data stream format to all the video participants.

- **Cisco IOS Heterogeneous Video Conference Bridge**—This conference bridge type supports heterogeneous video conferences. In a heterogeneous video conference, conference participants connect to the conference bridge with phones that use different video format attributes. The DSP provides transcoding and transsizing features to convert the signal between the various formats.

- **Cisco IOS Guaranteed Audio Video Conference Bridge**—This conference bridge type reserves DSP resources for audio conferencing, but does not reserve DSP resources for video conferencing. Callers on video phones may have video service if DSP resources are available at the start of the conference. Otherwise, the callers connect to the conference as audio participants.

**GUI Changes**
Three new Conference Bridge Types have been added to the drop down menu on the Conference Bridge Configuration page of Cisco Unified Communications Manager. When you select either of the three Conference Bridge Types, a new menu page appears with configuration settings for that particular type.

For more detailed information about how to configure conference bridges, see the *Cisco Unified Communications Manager Administration Guide*.

**Service Parameter and Enterprise Parameter Changes**
No service or enterprise parameter changes exist for this feature.
Destination Code Control

Description
Destination Code Control (DCC) limits the number of lower precedence calls that are allowed to a particular destination while allowing an unlimited number of calls for Flash, Flash Override, and Executive Override precedence calls (Flash or higher precedence calls) to that same destination.

A DCC-enabled route pattern allows each Flash or higher precedence calls to proceed, but regulates the percentage of lower precedence calls that are allowed by allowing or disallowing them based on the blocked percentage that is set by the administrator for that destination. The DCC-enabled route pattern limits Immediate, Priority and Routine (lower precedence than Flash) calls in accordance with the call blocking percentage that the administrator configures. In emergency situations, DCC enables the administrator to control the amount of call traffic to a particular destination. At any given time, the number of outgoing low priority calls through the DCC-enabled route pattern are less than or equal to the number of maximum allowed calls configured on that route pattern.

You can set the call blocking percentage on the Route Pattern Configuration window of Cisco Unified Communications Manager.

To access the Apply Call Blocking Percentage check box on the Route Pattern Configuration window, go to Call Routing > Route Hunt > Route Pattern.

Each node on the Cisco Unified Communications Manager independently tracks the number of calls to be blocked through it. The following nodes independently track the number of calls being routed through them, without synchronizing the tracking with any other node.

After you enable DCC by selecting the Apply Call Blocking Percentage and setting the call blocking percentage to a certain value, if you then make changes to the Gateway/Route List or Route Class, or any other fields on the Route Pattern window, without changing the blocked call percentage value, then the
DCC counters do not get reset, but continue counting based on the number of calls attempted through the route pattern prior to the change. For the DCC counter to reset, there must be a change in the Apply Call Blocking Percentage field.

**Note**

You cannot configure the MLPP level on the Route Pattern window to Flash, Flash Override, or Executive Override levels if you want to enable the DCC feature. You must set these MLPP levels at the translation pattern instead.

**Configuration Requirements**

To enable DCC, you must update the following fields:

**Apply Call Blocking Percentage**

Check this check box to enable the DCC feature. When DCC is enabled, all calls other than Flash and higher precedence calls that are made to the destination are filtered and allowed or disallowed based on the call blocking percentage quota that is set for the destination. Flash and higher precedence calls are allowed at all times. DCC is disabled by default.

**Call Blocking Percentage (%)**

Enter the percentage of calls to be blocked for this destination in numerals. This value specifies the percentage of lower precedence calls that are made to this destination that get blocked by the route pattern. This percentage limits the lower precedence calls only; the Flash and higher precedence calls that are made to this destination are allowed at all times.

**Note**

Cisco Unified Communications Manager calculates the maximum number of low priority calls to be allowed through this route pattern based on the call blocking percentage that you set for this destination.

**Note**

The Call Blocking Percentage (%) field gets enabled only if the Apply Call Blocking Percentage check box is checked.

**Dynamic DSCP Tagging**

**Description**

Cisco Unified Communications Manager maps the MLPP precedence levels to the Differentiated Services Control Point (DSCP) values in the ToS field of the IP Header to prioritize calls in an IP network. You can map the following precedence levels to DSCP values:

- Executive Override
- Flash
- Flash Override
- Immediate
- Priority
Unified CM Administration Configuration Tips

To map MLPP precedence levels to DSCP values, choose the DSCP value that you want mapped to each precedence level in the Clusterwide Parameters (System-QoS) section of the service parameters. Click the Save button to save the changes.

The DSCP values that you configure are also applicable to the SCCP phones.

Choose Enterprise Parameters > MLPP Parameters and set the MLPP indication status to MLPP Indication On.

For SCCP phones, choose Phone Configuration > MLPP Information > MLPP Indication and set to MLPP Indication On.

If MLPP indication is not set to On in the preceding cases, then the DSCP value corresponding to DSCP for audio calls will be used.

The DSCP values that you specify for audio calls are also applicable for Media Termination Points, Transcoders, Music on Hold, Annunciators, and Built in bridges on stations. The DSCP is set to the value of the service parameter corresponding to the MLPP for the call.

Use the following CLI commands to set DSCP marking:

- delete dscp
- set dscp defaults
- set dscp disable
- set dscp enable
- set dscp marking
- show dscp all
- show dscp markings
- show dscp defaults
- show dscp status

For more information about these CLI commands, see the Command Line Interface Reference Guide for Cisco Unified Solutions.

GUI Changes

No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.
CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

Federal Information Processing Standard (FIPS) 140-2

Description
For Federal Information Processing Standard (FIPS) 140-2 content, see Federal Information Processing Standard (FIPS) 140-2, page 72

Unified CM Administration Configuration Tips
No tips.

GUI Changes
No GUI changes.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can enable this feature via CLI.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.
User Tips
No user tips exist for this feature.

iSAC Enable and Disable Support

iSAC (Internet Speech Audio Codec) is a proprietary wideband speech and audio codec with an adaptive bit rate from 10 to 32 kb/s.

Codecs for recording calls match the codecs for agent-customer calls, therefore you may need to insert transcoders if the recorder does not support the matching codecs.

Cisco Unified IP Phones add new codecs that Cisco transcoders do not support.

Unified CM Administration Configuration Tips
No tips.

GUI Changes

The iSAC service parameters can be found in the Clusterwide Parameters (System - Location and Region) section of the Service Parameter Configuration window.

You can set the iSAC service parameters with the following values:
• Enabled for All Devices
• Enabled for All Devices Except Recording-Enabled Devices
• Disabled

Service Parameter and Enterprise Parameter Changes
• No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.
Mapping MLPP Precedence to DSCP Values

Description
Cisco Unified Communications Manager maps the MLPP precedence levels to the DSCP values in the ToS field of the IP Header to prioritize calls in an IP network. You can map the following precedence levels to DSCP values:

- Executive Override
- Flash Override
- Flash
- Immediate
- Priority

You must map the MLPP precedence levels to the DSCP values identically for every Cisco Unified Communications Manager cluster within your network.

Unified CM Administration Configuration Tips
No tips.

GUI Changes
No GUI changes.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.
Message Waiting Indicator for Route Lists with a SIP Trunk

Unified CM supports outbound Message Waiting Indicator (MWI) notification on a SIP trunk that is assigned to a Route List or a Route Group.

MLPP Location-Based CAC Enhancements

Description
Prior to Cisco Unified Communications Manager 8.6(1), Cisco Unified Communications Manager randomly selected a call with a precedence level that was lower than the new call request. If two calls existed that had a precedence of Routine and Priority, the Priority call could be preempted instead of the Routine call when a Flash call was attempted for that location.

In Cisco Unified Communications Manager 8.6(1) and later, Cisco Unified Communications Manager always preempts the Routine call before the Priority call.

Precedence-Based MLPP Preemption
Prior to Cisco Unified Communications Manager 8.6(1), Cisco Unified Communications Manager randomly chose calls to preempt that had lower precedence levels than the new request. If there are two existing calls with precedence levels of Routine and Priority and a Flash call comes in for that location, Cisco Unified Communications Manager might preempt the Routine call or the Priority call. With Cisco Unified Communications Manager 8.6(1) and later, Cisco Unified Communications Manager always preempts the Routine call before the Priority call.

CAC Call-State-Based MLPP Preemption
If two calls are in the same location, have the same precedence level, and are using the same media type (audio or video), Cisco Unified Communications Manager preempts the call that is in setup phase before selecting the call that has already completed.

Because location CAC counts bandwidth, when media is established, the bandwidth is being used, therefore, Cisco Unified Communications Manager considers the call setup to be completed.

Minimize Number of Calls to Preempt
For calls with the same precedence level, call state, and that use the same media type (audio or video), Cisco Unified Communications Manager attempts to minimize the number of calls to be preempted; that is, Cisco Unified Communications Manager selects a call with larger bandwidth, rather than several calls with less bandwidth.

Note
Cisco Unified Communications Manager always preempts calls with lower precedence levels if a call with a higher precedence level gets selected. This rule applies even when the higher precedence call can satisfy the required bandwidth.

Because each call connects two devices in different locations, each location could result in calls to be preempted. For example, in one location, a Flash call could be preempted while a Priority call is not preempted in the other location.
Preempt Video Calls When Allocating or Adjusting Bandwidth

Cisco Unified Communications Manager 8.6(1) and later preempts lower precedence video calls when allocating or adjusting video bandwidth for high priority calls if there is not enough bandwidth for the new request. When preempting a video call, Cisco Unified Communications Manager clears the call and plays a preemption tone to the party that is preempted.

Preempt Bandwidth Allocated for Annunciator or Music On Hold

Cisco Unified Communications Manager 8.6(1) and later preempts the bandwidth that is allocated for Annunciator and Music On Hold (MOH) when preempting calls. If media resource bandwidth is needed for a higher priority call, an entire call is cleared, rather than simply removing the Annunciator or MOH. When Annunciator or MOH is inserted into a call, such as to play music on hold or a ringback for MLPP Calls, preemption, or reorder tone, the media is streaming; therefore, Cisco Unified Communications Manager considers the call connected and preempts the call after all alerting calls with the same precedence level. However, when Annunciator or MOH is requested but not enough bandwidth is available at neither the media user location or the media resource location, the request for Annunciator or MOH fails and Cisco Unified Communications Manager does not preempt other calls for Annunciator or MOH.

As with all preempted calls, the bandwidth that is allocated for those calls is immediately released and then allocated for another call. When Annunciator is played for preemption tone, or any other tone that causes a call to disconnect, the tone continues to play for a short while even though the bandwidth has already released. That is, when Cisco Unified Communications Manager selects an Annunciator tone to be used for a preemption or reorder tone, the bandwidth might be over-subscribed (over-budget) for a short while before the call is completely cleared.

Enforcing Maximum Bandwidth

Cisco Unified Communications Manager 8.6(1) and later enforces configured maximum bandwidth for locations, which can result in calls being cleared when a call is resumed or transferred. In addition, multiple calls could be cleared when new bandwidth requests occur and the bandwidth is over-subscribed. To enforce maximum bandwidth for locations, the service parameters Locations-based Maximum Bandwidth Enforcement Level for MLPP Calls and Locations-based MLPP Enable must be set to Strict Enforcement.

When the value for the Locations-based Maximum Bandwidth Enforcement Level for MLPP Calls service parameter is changed from Lenient to Strict, the result could be more calls than the maximum bandwidth that is allowed. However, Cisco Unified Communications Manager does not immediately preempt calls to bring the bandwidth within the allowed budget, but rather, when new bandwidth is requested for the same type of audio or video call. When the preemption occurs, one possible result is a large amount of difference between bandwidth usage and the maximum allowed.

When handling preemption in over-subscription situations, Cisco Unified Communications Manager considers all existing calls, beginning with the lowest precedence level. Although this preemption is triggered by a bandwidth request, the preempted call could have a higher precedence level than the requesting call.

Preempt Audio Calls When Adjusting Bandwidth

Cisco Unified Communications Manager adjusts bandwidth for audio calls when bandwidth usage is changed after a call is presented to the called party, as in the case of called party answer, shared line hold and resume, transfer, and other feature interactions. Cisco Unified Communications Manager attempts to preempt other calls, if possible, but allows the new bandwidth request to proceed even when there is not enough bandwidth for the call to be preempted.
Note
If the service parameter Enforce Maximum Bandwidth for MLPP is set to True, the bandwidth request fails, which causes the call to be cleared. The requesting call is cleared as if it is preempted as any other location preemption with the same cause code and preemption tone.

Update Bandwidth After Joining Call Legs

Prior to Cisco Unified Communications Manager 8.6(1), real bandwidth usage was not reflected accurately. For example, when user B transferred user A and user C, the bandwidth that was reserved for the primary call (A and B) was allocated but the bandwidth reserved for the secondary call (B and C) was released.

Cisco Unified Communications Manager 8.6(1) and later updates bandwidth immediately after the Join operation, which reflects the correct bandwidth usage for calls. Updating bandwidth preserves the existing bandwidth that has been allocated to the two call legs. Once the media has connected, Cisco Unified Communications Manager adjusts to the correct bandwidth usage. That is, when the bandwidth is updated after the Join operation, one side of the call leg could have a bandwidth reservation for video and the other side for audio, which results in a call with two types of bandwidth reservation; however, the bandwidth is adjusted to the correct usage after the media connects.

Note
Because the update for bandwidth does not request additional bandwidth in either location, Cisco Unified Communications Manager does not preempt any calls.

Unified CM Administration Configuration Tips
No configuration tips exist for this feature.

GUI Changes
No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes
The service parameter Locations-based Maximum Bandwidth Enforcement Level for MLPP Calls determines whether to restrict the bandwidth usage for a location to be within its configured maximum.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.
AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

Mobility Feature Enhancements

The following mobility features were added:
- Toll Bypass Optimization for Handoff
- Unified Application Dial Rule Configuration for Mobility
- Single Registration
- Additional Device Types

Toll Bypass Optimization for Handoff

The Least Cost Routing (LCR) and Dialed Number Identification Service (DNIS) pool features were introduced as part of the Unified CM 8.5 release. These features led to reduced costs for Dial Via Office (DVO) calls by providing call routing based on the area, location, and region. Unified CM release 8.6(1) leverages the LCR-DNIS feature to invoke Handoff. Toll Bypass Optimization for Handoff uses the Enterprise Feature Access Number configured in the Mobility Profile associated with the Mobile Identity. Using this feature eliminates the need for a separate Handoff DID to be configured, which can also result in cost savings. When a user needs to invoke legacy Handoff, the client must dial the administrator configured Handoff DID number, which would be an international call placed to the Handoff DID number in roaming scenarios, which incurs additional costs to the enterprise.

Cisco Mobile Clients that are registered with a release previous to 8.6(1) of Unified CM will continue to have the legacy Handoff invocation.

GUI Changes
No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.
Unified Application Dial Rule Configuration for Mobility

Unified CM 8.5 and earlier versions, required that Application Dial Rules be configured locally on the client side for VoIP calls and separately in Unified CM for DVO calls. To simplify configuration for both VoIP and DVO calls, Unified CM 8.6(1) allows Application Dial Rule configuration to apply to DVO as well as VoIP calls, so that there is no separate client configuration required. This allows mobile users to make calls with both the enterprise dial plan or service provider dial plan regardless of the transports and provides a consistent way to manage dial plans. When a client makes a call in either VOIP or DVO mode, the same rule applies. Mobility uses the Application Dial Rules in such a way that the client can dial a 10-digit number in VoIP mode to call an external number as it does in DVO mode.

**Note**

VoIP mode is applicable to only SIP based mobile clients using en bloc dialing and cannot be applied to SCCP based mobile clients using overlap dialing.

This feature uses existing Application Dial Rule configuration and Mobility is treated as an application. Application Dial rules are shared by all applications. Ensure that the Application Dial rules you configure for Mobility do not conflict with Application Dial rules shared among other applications.

**GUI Changes**

No GUI changes exist for this feature.

**Service Parameter and Enterprise Parameter Changes**

No service or enterprise parameter changes exist for this feature.

**Installation/Upgrade (Migration) Considerations**

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

**Serviceability Considerations**

No serviceability considerations exist for this feature.

**BAT Considerations**

No BAT considerations exist for this feature.

**CAR/CDR Considerations**

No CAR or CDR considerations exist for this feature.

**Security Considerations**

No security considerations exist for this feature.
Single Registration

This feature enables a client to maintain a single connection to Cisco Unified Communication Manager while registered to both WLAN and Cellular Networks. It provides a seamless user experience and consistent enterprise features independent of the transport and registration modes.

For dual-registration of a dual mode device, the known limitation is that the registration status on the configuration page shows as registered only when it is registered to a WLAN Network. The registration status does not reflect whether the device is actually registered to a cellular network or not.

With the 8.6(1) release of Cisco Unified Communication Manager a single registration feature was added that displays the registration status on the single-registration dual mode device configuration page to reflect the actual registration status. When it shows registered, it indicates that the device has successfully registered to both a WLAN and a cellular network.

GUI Changes
The single-registration dual mode device configuration page in Cisco Unified Communication Manager now reflects the actual registration status of a device.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.
Additional Device Types

Two dual mode device types are have been made available as built-in. The Nokia S60 and Cisco Dual Mode for Android no longer require external COP files to enable these two device types.

GUI Changes
When adding a phone, both Nokia S60 and Cisco Dual Mode for Android devices will show up in the Phone Type drop-down list.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

P-Charging Vector (PCV) Support for Unified CM

Description
Unified CM 8.6(1) supports pass through of a SIP header called P-Charging-Vector (PCV) in network deployment. This PCV header is used to convey mobile or PSTN charging related information, such as the globally unique IP Multimedia Subsystem (IMS) charging identifier (ICID) value to the service providers.

A new SIP Normalization script, HCS-PCV-PAI-passthrough, is introduced as part of this feature. This script would be pre-installed on the Unified CM and has to be associated with all the SIP trunks that point to the network.
For any calls that originate from a network, the Unified CM passes through the PCV header received from a network in the INVITE, UPDATE and 200 OK to the other side. Unified CM would additionally pass through the PCV header from a network via 200 OK SIP for the calls terminating in the Unified CM. Because these calls are routed back to the Cisco network via the same SIP trunk, the 200 OK message received by the Unified CM is passed as-is through the PCV header in the outgoing calls.

**AXL and CTI Considerations**
No AXL or CTI considerations exist for this feature.

**BAT Considerations**
No BAT considerations exist for this feature.

**CAR/CDR Considerations**
No CAR or CDR considerations exist for this feature.

**GUI Changes**
No GUI changes exist for this feature.

**Installation/Upgrade (Migration) Considerations**
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

**Service Parameter and Enterprise Parameter Changes**
No service or enterprise parameter changes exist for this feature.

**Serviceability Considerations**
No serviceability considerations exist for this feature.

**Security Considerations**
No security considerations exist for this feature.

**User Tips**
No user tips exist for this feature.

**Require SDP Inactive Exchange for Mid-Call Media Change**

**Description**
This feature designates how Cisco Unified Communications Manager handles mid-call updates to codecs or connection information such as IP address or port numbers. The feature is selected by checking the **Require SDP Inactive Exchange for Mid-Call Media Change** check box on the SIP Profile Configuration window.

If the box is checked, then during mid-call codec or connection updates Cisco Unified Communications Manager sends an INVITE a=inactive SDP message to the endpoint to break the media exchange. This is required if an endpoint is not capable of reacting to changes in the codec or connection information without disconnecting the media. This applies only to audio and video streams within SIP-SIP calls.
If the box is unchecked, Cisco Unified Communications Manager passes the mid-call SDP to the peer leg without sending a prior Inactive SDP to break the media exchange. This is the default behavior.

**Note**
For early offer enabled SIP trunks, this feature is overridden by the *Send send-receive SDP in mid-call INVITE* feature.

**GUI Changes**
The feature is selected by checking the **Require SDP Inactive Exchange for Mid-Call Media Change** check box on the SIP Profile Configuration window.

**Service Parameter and Enterprise Parameter Changes**
No service or enterprise parameter changes exist for this feature.

**Installation/Upgrade (Migration) Considerations**
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

**Serviceability Considerations**
No serviceability considerations exist for this feature.

**BAT Considerations**
No BAT considerations exist for this feature.

**CAR/CDR Considerations**
No CAR or CDR considerations exist for this feature.

**Security Considerations**
No security considerations exist for this feature.

**AXL and CTI Considerations**
No AXL or CTI considerations exist for this feature.

**User Tips**
No user tips exist for this feature.

---

**SRTP for Annunciator and Music On Hold**

**Description**
Cisco Unified Communications Manager 8.6(1) and later enhances the Cisco IP Voice Media Streaming application service to support Secure Real-Time Protocol (SRTP); therefore, when the Cisco Unified Communications Manager cluster is enabled for security, the Annunciator and Music On Hold server registers with the Cisco Unified Communications Manager as SRTP capable devices. If the receiving device is also SRTP capable, the announcement or music media is encrypted before streaming to the receiving device.
In a secure mode, the Cisco Unified Communications Manager Administration Device Configuration window for Annunciator Configuration window and Music On Hold displays a Device is trusted message with a check box, indicating that it is a trusted device.

When the Cisco Unified Communications Manager is configured in a secure deployment environment (the Cluster Security Mode enterprise parameter is set to mixed mode), Cisco Unified IP Phones, voice gateways, and other secure capable endpoints are set to encrypted mode. The media streaming between the devices is done through SRTP. When calls are secure, a locked icon displays on the Cisco Unified IP Phone, indicating that the call is protected for both signaling and media.

When Cisco Unified Communications Manager interrupts the media of an encrypted call, such as when call features are activated, the locked icon is removed from the Cisco Unified IP Phone. The icon is restored when the phone reconnects with the encrypted media. The duration of the media interruption and restoration is short when encrypted Music On Hold is activated.

Unified CM Administration Configuration Tips
No configuration tips exist for this feature.

GUI Changes
No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes
Cisco Unified Communications Manager 8.6(1) adds the service parameter Enable Source IP Address Verification for Software Media Devices that determines whether the source IP address of the Annunciator and Music On Hold servers are verified to be registered Cisco Unified Communications Manager nodes in the cluster. This parameter is applicable only when the enterprise parameter Cluster Security Mode is set to 1 (mixed mode).

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.
**Session Level Bandwidth Modifiers**

**Description**

In previous releases, Cisco Unified Communications Manager inconsistently used incoming SDP session level bandwidth values to reserve bandwidth, causing Cisco Unified Communications Manager to occasionally over or under reserve bandwidth.

In this release, Cisco Unified Communications Manager provides location call admission control support for handling session level bandwidth modifiers. Session level bandwidth modifiers are communicated as part of the parameters in the SDP portion of the initial SIP signaling. These parameters indicate the maximum amount of bandwidth each endpoint will support for that type of call. These parameters are used, along with Cisco Unified Communications Manager region and locations settings to set the bandwidth for each call.

During the initial call setup, both parties communicate their maximum allowed bandwidth for the call to Cisco Unified Communications Manager. Cisco Unified Communications Manager passes on this communication to the other endpoint, but if the bandwidth specified by the endpoint is greater than the region setting, Cisco Unified Communications Manager replaces the value with the regional bandwidth value.

For information about the rules that Cisco Unified Communications Manager uses to determine the amount of bandwidth to allocate to a specific call, see the *Cisco Unified Communications Manager System Guide*.

**Unified CM Administration Configuration Tips**

No configuration tips exist for this feature.

**GUI Changes**

The **SDP Session-level Bandwidth Modifier for Early Offer and Re-invites** drop box has been added to the SIP Profile Configuration window.

**Service Parameter and Enterprise Parameter Changes**

No service or enterprise parameter changes exist for this feature.

**Installation/Upgrade (Migration) Considerations**

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

**Serviceability Considerations**

No serviceability considerations exist for this feature.

**BAT Considerations**

No BAT considerations exist for this feature.

**CAR/CDR Considerations**

No CAR or CDR considerations exist for this feature.
Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

Single Sign On

Description
The single sign on feature allows end users to log into a Windows client machine on a Windows domain, then use certain Unified CM applications without signing on again. For this release, the single sign on feature has been extended to include the Cisco Unified Communications Manager Administration application and the Real Time Monitoring Tool (RTMT) application in addition to the User Options pages and the Cisco Unified Communication interface for Microsoft Office Communicator that were previously supported.

Unified CM Administration Configuration Tips
Use the following procedure to configure the Single Sign On feature:

1. Ensure that your environment meets the requirements described in the “Single Sign On” section of the Cisco Unified Communications Manager Features and Services Guide 8.6(1). Refer to this document online at:


2. Provision the OpenAM server in Active Directory, then generate keytab files.

   Note
   If your Windows version does not include the ktpass tool for generating keytab files, then you must obtain it separately.

3. Import the OpenAM server certificate into the Cisco Unified Communications Manager tomcat-trust store.

4. Configure Windows single sign on with Active Directory and OpenAM.

5. (For Unified CM Administration only) Verify that the user is provisioned in the Active Directory.

6. (For Unified CM Administration only) Synchronize the user data to the Cisco Unified Communications Manager database using the DirSync service.

7. (For Unified CM Administration only) Add the user to the CCM Super User group to enable access to Cisco Unified Communications Manager Administration.

8. Configure client browsers for single sign on.

9. Enable single sign on in Cisco Unified Communications Manager.

   Note
   For more detailed information about this procedure, see the Cisco Unified Communications Manager Features and Services Guide 8.6(1). Refer to this document online at

GUI Changes
No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

Transparency for REFER Without Replaces

Description
In previous releases, Cisco Unified Communications Manager acted upon any REFER request (such as a blind transfer) sent by an endpoint. This functionality caused a problem in call center applications, where the agent sending the REFER (initiating the transfer) resides in a geographic area remote from both of the other call parties. The call signaling remained connected through the Cisco Unified Communications Manager of the agent that initiated the transfer. The load associated with the call and continued used of MTP devices (if allocated during the initial call), remained with the Cisco Unified Communications Manager of the agent initiating the transfer, resulting in signaling delays between the parties in the new call.

In this release Cisco Unified Communications Manager allows you to enable REFER transparency for blind transfers, so that the local Cisco Unified Communications Manager drops from the call when the local agent gets removed.
Unified CM Administration Configuration Tips
You enable REFER transparency by associating the refer-passthrough script or a custom REFER transparency script with one or more SIP trunks. For information about creating customer scripts, see the Developer Guide for SIP Transparency and Normalization. To upload custom scripts in Cisco Unified Communications Manager, use the SIP Normalization Script Configuration window (Device > Device Settings > SIP Normalization Script).

You cannot modify or delete the refer-passthrough script in Cisco Unified Communications Manager Administration. If you want to use the content of the refer-passthrough script in a custom script, display the script in the SIP Normalization Script window. Copy the information from the Content field, click the Add New button to create a new script record, and paste the information from the refer-passthrough script into the new record.

To associate the refer-passthrough script or a customer REFER transparency script with a SIP trunk, configure the Normalization Script fields on the Trunk Configuration window (Device > Trunk).

GUI Changes
The refer-passthrough script has been included in the Cisco Unified Communications Manager database. To view the script, choose Device > Device Settings > SIP Normalization Script.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 8.6(1), you can use this feature.

Serviceability Considerations
The following alarms introduced in Cisco Unified Communications Manager Release 8.5(1) apply to the REFER transparency feature:
- SIPNormalizationScriptOpened
- SIPNormalizationScriptClosed
- SIPNormalizationResourceWarning
- SIPNormalizationScriptError
- SIPNormalizationAutoResetDisabled

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.
**User Tips**

No user tips exist for this feature.

---

**Use Fully Qualified Domain Name in SIP Requests**

**Description**

This feature enables Unified CM to relay an alphanumeric hostname of a caller by passing it through to the called device or outbound trunk as a part of the SIP header information. The feature is set with the **Use Fully Qualified Domain Name in SIP Requests** check box on the SIP Profile Configuration window.

- If the box is unchecked, the IP address for Cisco Unified Communications Manager is passed to the line device or outbound trunk instead of the user’s hostname. This is the default behavior.
- If the box is checked, Cisco Unified Communications Manager relays the alphanumeric hostname of a caller by passing it through to the called endpoint as a part of the SIP header information. This enables the called endpoint to return the call using the received or missed call list.

If the call is originating from a line device on Cisco Unified Communications Manager and is being routed on a SIP trunk, then the configured Organizational Top-Level Domain (e.g., cisco.com) is used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID.

If the call is originating from a trunk on Cisco Unified Communications Manager and is being routed on a SIP trunk, then:

- If the inbound call provides a host or domain in the caller’s information, the outbound SIP trunk messaging preserves the hostname in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID
- If the inbound call does not provide a host or domain in the caller’s information, the configured Organizational Top-Level Domain (e.g. cisco.com) is used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID

**Unified CM Administration Configuration Tips**

No configuration tips exist for this feature.

**GUI Changes**

The **Use Fully Qualified Domain Name in SIP Requests** check box has been added to the SIP Profile Configuration window.

**Service Parameter and Enterprise Parameter Changes**

No service or enterprise parameter changes exist for this feature.

**Installation/Upgrade (Migration) Considerations**

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

**Serviceability Considerations**

No serviceability considerations exist for this feature.

**BAT Considerations**

No BAT considerations exist for this feature.
**User-Agent and Server Header Information**

**Description**

This feature indicates how Unified CM handles the User-Agent and Server header information in a SIP message. The feature is configured by selecting one of the following three options from the User-Agent and Server header information drop-down list on the SIP Profile Configuration window:

- **Send Unified CM Version Information as User-Agent Header**—For INVITE requests, the User-Agent header is included with the CM version header information. For responses, the Server header is omitted. Unified CM passes through any contact headers untouched. This is the default behavior.

- **Pass Through Received Information as Contact Header Parameters**—If this option is selected, the User-Agent/Server header information is passed as Contact header parameters. The User-Agent/Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent/Server headers.

- **Pass Through Received Information as User-Agent and Server Header**—If this option is selected, the User-Agent/Server header information is passed as User-Agent/Server headers. The User-Agent/Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent/Server headers.

**Unified CM Administration Configuration Tips**

No configuration tips exist for this feature.

**GUI Changes**

The User-Agent and Server header information drop-down list has been added to the SIP Profile Configuration window.

**Service Parameter and Enterprise Parameter Changes**

No service or enterprise parameter changes exist for this feature.

**Installation/Upgrade (Migration) Considerations**

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

**Serviceability Considerations**

No serviceability considerations exist for this feature.
V.150.1 MER SCIP 216

Description
Cisco Unified Communications Manager supports legacy V.150.1 and V.150.1 MER (Minimal Essential Requirements) based secure Modem over IP (MoIP) communications between an IP STE and legacy (BRI or analog) Secure Terminal Equipment (STE) across a SIP trunk and an intercluster SIP trunk. SIP trunks transport the Session Description Protocol (SDP) information for outbound calls and signal Cisco Unified Communications Manager when MoIP SDP information is received for inbound calls. Devices can call between clusters by using SIP to negotiate a V.150.1 or V.150.1 MER secure call.

Unified CM Administration Configuration Tips
If you want a trunk to support Non secure Modem over IP (MOIP) calls, you must enable the V150 (subset) check box in Cisco Unified Communications Manager Administration for digital access PRI/T1 port configuration on the gateway. For more information, see the Cisco Unified Communications Manager Administration Guide.

GUI Changes
The following GUI changes were implemented for the V.150.1 MER feature:

- **Security**—In the SIP Trunk Security Profile Configuration window, there is a new SIP V.150 Outbound SDP Offer Filtering drop-down list box that contains the following filtering options:
  - Use Default Filter—The SIP trunk uses the default filter that is indicated in the SIP V.150 Outbound SDP Offer Filtering service parameter. To locate the service parameter, go to System > Service Parameters > Clusterwide Parameters (Device-SIP) in Cisco Unified Communications Manager Administration.
  - No Filtering—The SIP trunk performs no filtering of V.150 SDP lines in outbound offers.
  - Remove MER V.150—The SIP trunk removes V.150 MER SDP lines in outbound offers. Select this option to reduce ambiguity when the trunk is connected to a pre-MER V.150 Cisco Unified Communications Manager.
  - Remove Pre-MER V.150—The SIP trunk removes any non-MER compliant V.150 lines in outbound offers. Select this option to reduce ambiguity when your cluster is contained in a network of MER compliant devices that are incapable of processing offers with pre-MER lines.

Service Parameter and Enterprise Parameter Changes
The SIP V.150 Outbound SDP Offer Filtering service parameter was added for this feature. Use this parameter to set the SIP V.150 outbound SDP offer filtering option. This parameter determines whether the SIP trunk performs filtering on transmitted SDP offers to remove MER or pre-MER V.150 content. Valid values specify No Filtering (the SIP trunk does not perform any filtering on outbound V.150 SDP lines); Remove MER V.150 (the SIP trunk removes MER lines in outbound SDP offers; use this value to reduce ambiguity when a trunk is connected to a pre-MER V.150 Unified CM); or Remove Pre-MER V.150 (the SIP trunk removes any non-MER-compliant lines in outbound SDP offers; if your cluster is contained within a network of MER-compliant devices that are incapable of processing an offer with pre-MER lines, choose this value). This is a required field and the default is No Filtering.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
This release of Cisco Unified Communications Manager supports V.150.1 MER (Minimal Essential Requirements) based secure Modem over IP (MoIP) communications between an IP STE and legacy (BRI or analog) Secure Terminal Equipment (STE) across a SIP trunk and an intercluster SIP trunk.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

Video Encryption

Description
Cisco Unified Communications Manager supports encryption of audio, video and other media streams so long as the individual endpoints involved in the communication also support encryption. Cisco Unified Communications Manager uses the Secure Real-Time Transport Protocol (SRTP) to encrypt the media streams. Some of the features include:

- Support for SIP and H.323 endpoints
- Support for encryption of main audio and video line while operating in MTP passthru mode
- Support for multiple encryption methods
- Support for SDP crypto-suite session parameters as per RFC 4568
In order to provide encrypted communications, encryption keys are exchanged between the endpoints and Cisco Unified Communications Manager during the SIP call setup. For this reason, the SIP signaling should be encrypted using TLS. During the initial call setup, the video endpoints will exchange a list of encryption methods that they support, select an encryption suite supported by both endpoints, and exchange encryption keys. If the endpoints cannot agree on a common encryption suite, then the media streams will be unencrypted and transported using the Real-Time Transport Protocol (RTP).

**Note**
If the individual endpoints do not support encryption, then the communication will take place using RTP.

For a list of encryption suites supported by Cisco Unified Communications Manager and a list of encryption methods that Cisco Unified Communications Manager supports for specific signaling methods, see the *Cisco Unified Communications Manager System Guide*.

**Unified CM Administration Configuration Tips**
No configuration tips exist for this feature.

**GUI Changes**
No GUI changes exist for this feature.

**Service Parameter and Enterprise Parameter Changes**
No service or enterprise parameter changes exist for this feature.

**Installation/Upgrade (Migration) Considerations**
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

**Serviceability Considerations**
No serviceability considerations exist for this feature.

**BAT Considerations**
No BAT considerations exist for this feature.

**CAR/CDR Considerations**
No CAR or CDR considerations exist for this feature.

**Security Considerations**
No security considerations exist for this feature.

**AXL and CTI Considerations**
No AXL or CTI considerations exist for this feature.

**User Tips**
No user tips exist for this feature.
Video and Interoperability Enhancements

Description
With the growing business need for video capability the list of video endpoints that are supported by Cisco Unified communications Manager has been expanded and enhanced. As of the 8.6 release, the Cisco portfolio of video endpoints is comprised of the following:

- Cisco IP Video Phone E20
- Cisco TelePresence Quick Set C20
- Cisco TelePresence Codec C40
- Cisco TelePresence Codec C60
- Cisco TelePresence Codec C90
- Cisco TelePresence EX60
- Cisco TelePresence EX90
- Cisco Unified IP Phone 7985
- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945
- Cisco Unified IP Phone 9971
- Cisco Unified IP Phone 9951

Unified CM Administration Configuration Tips
No configuration tips exist for this feature.

GUI Changes
Administrators configure video endpoints in the Phone Configuration window of Cisco Unified Communications Manager Administration.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.
Security

This section contains information about the following topics:

- Automatic Phone Synchronization with latest ITL File, page 66
- Configure Security for 3rd Party SIP phones, page 69
- Configuring Preferred Vendor SIP Phone Security Profile with Per-Device Certificates, page 69
- Configuring Preferred Vendor SIP Phone Security Profile with Shared Certificates, page 70
- CTL Client Installation on Windows 7, page 70
- Federal Information Processing Standard (FIPS) 140-2, page 72
- SELinux, page 75

Automatic Phone Synchronization with latest ITL File

Cisco Unified Communications Manager 8.6(1) and later automatically restarts applicable phones when the ITL File is updated.

Refresh Upgrade from Cisco Unified Communications Manager Release 7.x to Release 8.6(1) or later

To upgrade your cluster from Release 7.x to Release 8.6(1) or later, follow this procedure:

Procedure

Step 1  Follow the normal procedure for upgrading a cluster. For more information, see “Software Upgrades,” in the Cisco Unified Communications Operating System Administration Guide.

Tip  After you finish upgrading all nodes in the cluster to Cisco Unified Communications Manager Release 8.6(1) or later, you must also follow all the steps in this procedure to ensure that your Cisco Unified IP Phones register with the system.

Step 2  If you are running one of the following releases in mixed mode, you must run the CTL client:

- Cisco Unified Communications Manager Release 7.1(2)
  - All regular releases of 7.1(2)
  - All ES releases of 712 prior to 007.001(002.32016.001)
Cisco Unified Communications Manager Release 7.1(3)

- All regular releases of 713 prior to 007.001(003.21900.003) = 7.1(3a)su1a
- All ES releases of 713 prior to 007.001(003.21005.001)

**Note** For more information about running the CTL client, see “Configuring the CTL Client,” in the *Cisco Unified Communications Manager Security Guide*.

**Step 3** Wait ten minutes for the Cisco Unified IP Phones to automatically restart and register with Cisco Unified Communications Manager.

**Caution** You must back up your cluster using the Disaster Recovery System (DRS) to be able to recover the cluster. To backup your cluster using DRS, see the *Disaster Recovery System Administration Guide*.

---

**Rolling Back the Cluster to a Pre-8.0 Release**

Before you roll back a cluster to a pre-8.0 release of Cisco Unified Communications Manager, you must prepare the cluster for rollback using the Prepare Cluster for Rollback to pre-8.0 enterprise parameter.

To prepare the cluster for rollback, follow this procedure on each server in the cluster:

**Procedure**

**Step 1** From Cisco Unified Communications Manager Administration, choose System > Enterprise Parameters.

The Enterprise Parameters Configuration window displays.

Set the **Prepare Cluster for Rollback to pre-8.0** enterprise parameter to **True**.

**Note** Enable this parameter only if you are preparing to rollback your cluster to a pre-8.6(1) release of Cisco Unified Communications Manager. Phone services that use https (for example, extension mobility) will not work while this parameter is enabled. However, users will be able to continue making and receiving basic phone calls while this parameter is enabled.

**Step 2** Wait ten minutes for the Cisco Unified IP Phones to automatically restart and register with Cisco Unified Communications Manager.

**Revert the Cluster to the Previous Release**

**Step 3** Revert each server in the cluster to the previous release. For more information about reverting a cluster to a previous version, see “Software Upgrades” in the *Cisco Unified Communications Operating System Administration Guide*.

**Step 4** Wait until the cluster finishes switching to the previous version.

**Step 5** If you are running one of the following releases in mixed mode, you must run the CTL client:

- **Cisco Unified Communications Manager Release 7.1(2)**
  - All regular releases of 7.1(2)
• All ES releases of 712 prior to 007.001(002.32016.001)

Cisco Unified Communications Manager Release 7.1(3)
• All regular releases of 713 prior to 007.001(003.21900.003) = 7.1(3a)su1a
• All ES releases of 713 prior to 007.001(003.21005.001)

Note For more information about running the CTL client, see “Configuring the CTL Client,” in the Cisco Unified Communications Manager Security Guide.

Switching Back to Release 8.6(1)

If you decide to switch back to the Release 8.6(1) partition after you revert the cluster to Release 7.x, follow the procedure in this section.

Procedure

Step 1 Follow the procedure for switching the cluster back to the inactive partition. For more information, see the Cisco Unified Communications Operating System Administration Guide.

Step 2 If you were running one of the following releases in mixed mode, you must run the CTL client:

Cisco Unified Communications Manager Release 7.1(2)
• All regular releases of 7.1(2)
• All ES releases of 712 prior to 007.001(002.32016.001)

Cisco Unified Communications Manager Release 7.1(3)
• All regular releases of 713 prior to 007.001(003.21900.003) = 7.1(3a)su1a
• All ES releases of 713 prior to 007.001(003.21005.001)

Note For more information about running the CTL client, see “Configuring the CTL Client,” in the Cisco Unified Communications Manager Security Guide.

Step 3 From Cisco Unified Communications Manager Administration, choose System > Enterprise Parameters.

The Enterprise Parameters Configuration window displays.

Set the Prepare Cluster for Rollback to pre-8.6(1) enterprise parameter to False.

Step 4 Wait ten minutes for the Cisco Unified IP Phones to automatically restart and register with Cisco Unified Communications Manager.
Configure Security for 3rd Party SIP phones

There are two categories of phone models which support security in Unified CM: Secure Cisco phones and Secure Preferred Vendor phones. Secure Cisco phones are pre-installed with a Manufacture-Installed Certificate (MIC) and support automatic generation and exchange of Locally-Significant Certificates (LSC) using the Certificate Authority Proxy Function (CAPF). Secure Cisco phones immediately register with Unified CM using the MIC without any certificate management. For additional security, you can create and install an LSC on the phone using CAPF.

Secure Preferred Vendor phones do not come pre-installed with a MIC, and do not support CAPF for generating LSCs. In order for Secure Preferred Vendor phones to connect to Unified CM, a certificate must be provided with the device, or generated by the device. The phone supplier must provide the details on how to acquire or generate a certificate for the phone. Once you obtain the certificate, you must upload the certificate to the Unified CM using the OS Administration Certificate Management interface.

For a list of security features that are supported on your phone, see the phone administration and user documentation that supports this Cisco Unified Communications Manager release or the firmware documentation that supports your firmware load.

Cisco Unified Communications Manager can provide security for a preferred vendor SIP phone. In order to support security, you must enable Security Encryption or Security Authentication for the preferred vendor SIP phone.

Secure Preferred Vendor phones are phone types that are manufactured by 3rd-party vendors but are installed in the Unified CM database via a COP file. Unified CM provides security for a preferred vendor SIP phone. In order to support security, you must enable Security Encryption or Security Authentication for the preferred vendor SIP phone in the COP file. These phone types appear in the drop-down list in the Add a New Phone window. While all preferred vendor phones support Digest Authorization, not all preferred vendor phones support TLS security. Security capabilities is based on the phone model. If the Phone Security Profile includes a “Device Security Mode” field, then it supports TLS security.

If the preferred vendor phone supports TLS security, there are two modes that are possible: per-device certificate and shared certificate. The phone supplier must specify which mode is applicable for the phone as well as instructions on generating or acquiring a certificate for the phone.

Configuring Preferred Vendor SIP Phone Security Profile with Per-Device Certificates

To configure the preferred vendor SIP phone security profile with per-device certificates, perform the following procedure:

Procedure

Step 1 Upload the certificate for each phone using the OS Administration Certificate Management interface.
Step 2 In the Unified CM Administration, choose System > Security > Phone Secure Profile.
Step 3 Configure a new Phone Security Profile for the device type of this phone and in the Device Security Mode drop-down list box, choose Encrypted or Authenticated.
Step 4 To configure the new SIP phone in the Unified CM Admin interface, choose Device > Phone > Add New Phone.
Step 5 Select Phone type.
Configuring Preferred Vendor SIP Phone Security Profile with Shared Certificates

To configure the preferred vendor SIP phone security profile with shared certificates, perform the following procedure:

Procedure

Step 1 Using instructions from the phone vendor, generate a certificate with a Subject Alternate Name (SAN) string. The SAN must be of type DNS. Make a note of the SAN specified in this step. For example, X509v3 extensions:
X509v3 Subject Alternative Name:
DNS:AscomGroup01.acme.com

Note The SAN must be of type DNS or security will not be enabled.

Step 2 Upload the shared certificate using the OS Administration Certificate Management interface.

Step 3 In the Unified CM Administration, choose System > Security > Phone Secure Profile.

Step 4 In the Name field, enter the name of the Subject Alt Name (SAN), which is the name on the certificate provided by the preferred vendor or if there is no SAN enter the Certificate Name.

Note The name of the security profile must match the SAN in the certificate exactly or security will not be enabled.

Step 5 In the Device Security Mode drop-down list box, choose Encrypted or Authenticated.

Step 6 In the Transport type drop-down list box, choose TLS.

Step 7 To configure the new SIP phone in the CCMAadmin interface, choose Device > Phone > Create a New Phone.

Step 8 Select Phone type.

Step 9 Fill in the required fields

Step 10 In the Device Security Profile drop-down list box, select the profile you just created.

CTL Client Installation on Windows 7


To install the Cisco CTL Client for Windows 7 32-bit and Windows 7 64-bit, perform the following procedure:
Procedure

Step 1 From the Windows workstation or server where you plan to install the client, browse to Cisco Unified Communications Manager Administration, as described in the Cisco Unified Communications Manager Administration Guide.

Step 2 In Cisco Unified Communications Manager Administration, choose Application > Plugins. The Find and List Plugins window displays.

Step 3 From the Plugin Type equals drop-down list box, choose Installation and click Find.

Step 4 Locate the Cisco CTL Client (Windows 7) file.

Step 5 To download the file, click Download on the left side of the window, directly opposite the Cisco CTL Client plug-in name.

Step 6 Click Save and save the file to a location that you will remember.

Step 7 To begin the installation, double-click CiscoCTLClient_win7.exe (icon or executable depending on where you saved the file).

Note You can also click Open from the Download Complete box.

Step 8 The version of the Cisco CTL Client displays; click Next.

Step 9 The installation wizard displays. Click Next.

Step 10 Accept the license agreement and click Next.

Step 11 Choose a folder where you want to install the client. If you want to do so, click Browse to change the default location; after you choose the location, click Next.

Step 12 To begin the installation, click Next.

Step 13 After the installation completes, click Finish.

Changing the Security Token Password (Etoken) on a Windows 7 Server or Workstation

To change the security token password on a Windows 7 server or workstation, perform the following procedure:

Procedure

Step 1 Verify that you have installed the Cisco CTL Client on a Windows server or workstation.

Step 2 If you have not already done so, insert the security token into the USB port on the Windows server or workstation where you installed the Cisco CTL Client.

Step 3 Choose Start > Programs > Safenet > Safenet Authentication Client tools, right-click etoken, and choose Change etoken password.

Step 4 In the Current Password field, enter the password that you originally created for the token.

Step 5 Enter a new password.

Step 6 Enter the new password again to confirm it.

Step 7 Click OK.
Disable VPN for Unrestricted Unified CM

When employing a U.S. export unrestricted version of Unified CM, the following notes apply:

**Note**
You cannot export VPN details through Import/Export if you are employing the U.S. export unrestricted version of Unified CM.

**Note**
The check boxes: VPN Profile, VPN Gateway, VPN Group, and VPN Feature Configuration do not display if you are using the U.S. export unrestricted version of Unified CM. You cannot export VPN details through Import/Export if you are using the U.S. export unrestricted version of Unified CM.

Federal Information Processing Standard (FIPS) 140-2

FIPS, or Federal Information Processing Standard, is a U.S. and Canadian government certification standard that defines requirements that cryptographic modules must follow.

Cisco Unified Communications Manager 8.6 is FIPS 140-2 compliant, in accordance with the U.S. National Institute of Standards (NIST), and can operate in FIPS mode, level 1 compliance.

When you enable FIPS 140-2 mode, Cisco Unified Communications Manager reboots, runs certification self-tests at startup, performs the cryptographic modules integrity check, and then regenerates the keying materials. At this point, Cisco Unified Communications Manager operates in FIPS 140-2 mode.

Cisco Unified Communications Manager 8.6 meets FIPS requirements, including the following: it performs startup self-tests and restricts to a list of approved cryptographic functions.

Cisco Unified Communications Manager FIPS mode uses the following FIPS 140-2 level 1 validated cryptographic modules:

- OpenSSL 0.9.8l with FIPS Module 1.2
- RSA CryptoJ 4.1
- Red Hat Open SSL
- Red Hat Open Sw an
- NSS

In Cisco Unified Communications Manager, you can perform the following FIPS-related tasks:

- Enable FIPS 140-2 mode
- Disable FIPS 140-2 mode
- Check the status of FIPS 140-2 mode

**Note**
By default, Cisco Unified Communications Manager is in non-FIPS mode. The administrator must enable FIPS mode.

Enabling FIPS 140-2 Mode

FIPS 140-2 is enabled through the CLI. For more information, see Command Line Interface Reference Guide for Cisco Unified Communications Solutions.
Consider the following information before you enable FIPS 140-2 mode on Cisco Unified Communications Manager:

- In single server clusters, because certificates get regenerated, you need to run the CTL Client or apply the “Prepare Cluster for Rollback to pre 8.0” enterprise parameter before enabling FIPS mode. If either of these steps is not performed, the administrator must manually delete the ITL File after enabling FIPS mode.

- After FIPS mode is enabled on a server, please wait until the server reboots and the phones re-register successfully before enabling FIPS on the next server.

**Caution**

Before you enable FIPS mode, we strongly recommend that you perform a system backup. If FIPS checks fail at start-up, the system halts and requires a recovery CD to be restored.

To enable FIPS 140-2 Mode, perform the following procedure:

**Procedure**

**Step 1**

Start a CLI session.

For more information, see Starting a CLI Session in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

**Step 2**

In the CLI, enter `utils fips enable`.

The following prompts appear:

```
Security Warning: The operation will regenerate certificates for
1) CallManager
2) Tomcat
3) IPsec
4) TVS
5) CAPF
6) SSH
Any third party CA signed certificates that have been uploaded for the above components
will need to be re-uploaded.
If the system is operating in mixed mode, then the CTL client needs to be run again to
update the CTL file.
******************************************************************************
This will change the system to FIPS mode and will reboot.
******************************************************************************
Do you want to continue (yes/no) ?
```

**Step 3**

Enter yes.

The following message appears:

```
Generating certificates...
Setting FIPS mode in operating system.
FIPS mode enabled successfully.
******************************************************************************
It is highly recommended that after your system restarts
that a system backup is performed.
******************************************************************************
The system will reboot in a few minutes.

Cisco Unified Communications Manager reboots automatically.
```

**Note**

Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.
If you have a single server cluster and applied the “Prepare Cluster for Rollback to pre 8.0” enterprise parameter prior to enabling FIPS 140-2 mode, disable this enterprise parameter after making sure that all the phones registered successfully to the server.

In FIPS mode, Cisco Unified Communications Manager uses RedHat Openswan (FIPS validated) in place of Racoon (non-FIPS validated). If the security policies in Racoon contain functions that are not FIPS approved, the CLI command will ask you to redefine the security policies with FIPS approved functions and abort. For more information, see the Cisco Unified Communications Operating System Administration Guide.

Disabling FIPS 140-2 Mode

FIPS 140-2 is disabled through the CLI. For more information, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Consider the following information before you disable FIPS 140-2 mode on Cisco Unified Communications Manager:

- In single or multiple server clusters, we strongly recommend that you run the CTL Client. If the CTL Client is not run on a single server cluster, the administrator must manually delete the ITL File after disabling FIPS mode.
- In multiple server clusters, each server must be disabled separately, because FIPS mode is disabled not cluster-wide but rather per server basis.

To disable FIPS 140-2 mode, perform the following procedure:

**Procedure**

**Step 1**
Start a CLI Session.

For more information, see the Starting a CLI Session section in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

**Step 2**
In the CLI, enter `utils fips disable`

Cisco Unified Communications Manager reboots and is restored to non-FIPS mode.

Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.

Checking the Status of FIPS 140-2 Mode

To confirm that FIPS 1402 mode is enabled, you can check the status from the CLI.

To check the status of FIPS 140-2 mode, perform the following procedure:
Procedure

Step 1  Start a CLI Session.
For more information, see the Starting a CLI Session section in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Step 2  In the CLI, enter `utils fips status`
The following message appears to confirm that FIPS 140-2 mode is enabled.

```
admin:utils fips status
The system is operating in FIPS mode. Self test status:
- S T A R T ---------------------
  Executing FIPS selftests
  runlevel is N 3
  Start time: Thu Apr 28 15:59:24 PDT 2011
  NSS self tests passed.
  Kernel Crypto tests passed.
  Operating System OpenSSL self tests passed.
  Openswan self tests passed.
  OpenSSL self tests passed.
  CryptoJ self tests passed...
```

Rebooting a Server in FIPS 140-2 Mode

When a Cisco Unified Communications Manager server reboots in FIPS 140-2 mode, it will trigger FIPS startup self-tests in each of the FIPS 140-2 modules after rebooting.

Caution
If any of these self-tests fail, the CUCM server halts.

Note
A Cisco Unified Communications Manager server is automatically rebooted when FIPS is enabled or disabled with the corresponding CLI command. A user can also initiate a reboot.

Caution
If the startup self-test failed because of a transient error, restarting the Cisco Unified Communications Manager server fixes the issue. However, if the startup self-test error persists, it indicates a critical problem in the FIPS module and the only option is to use a recovery CD.

SELinux

SELinux is an integrated security enhancement to the Linux operating system. SELinux is integrated with Red Hat Enterprise Linux (RHEL) as a standard feature.

Linux has two forms of access control:
• **Discretionary Access Control (DAC)** — The standard Linux owner-group-world permission mode.

• **Mandatory Access Control (MAC)** — The SELinux security enhancement. MAC adds additional labels, or a categories, to all file system objects and restricts the level of control that users have over those system objects.

Both standard Linux (DAC) and SELinux (MAC) access controls must be satisfied in order to access an object. SELinux uses policies, in a manner similar to Cisco Security Agent (CSA), to refer to the set of rules that are loaded into the kernel for access enforcement. The SELinux policies defined on the system are specific to the installed version of the Cisco Unified Communication application.

Table 9 on page 76 illustrates the differences between SELinux and CSA.

### Table 9  **Supported Policies**

<table>
<thead>
<tr>
<th>Security policies supported by CSA</th>
<th>Supported by SELinux</th>
</tr>
</thead>
<tbody>
<tr>
<td>File access control</td>
<td>Yes</td>
</tr>
<tr>
<td>Application access control</td>
<td>Yes</td>
</tr>
<tr>
<td>Network control</td>
<td>Yes</td>
</tr>
<tr>
<td>Connection rate limit (DoS protection)</td>
<td>No (see Note)</td>
</tr>
<tr>
<td>Network shield</td>
<td>No (see Note)</td>
</tr>
<tr>
<td>Misc (for example: root kit, symbolic link protection)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note**  Connection Rate Limit and Network Shield protection are now provided by IPTables

Table 10 on page 76 illustrates feature comparisons for Cisco Security Agent (CSA) and SELinux.

### Table 10  **Feature Comparison**

<table>
<thead>
<tr>
<th>Feature</th>
<th>CSA</th>
<th>SELinux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled / disabled from CLI</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Deliver policy patches through COP file</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note**  SELinux can be changed to “permissive” mode using the CLI. Completely disabling it requires remote support access. Changing SELinux mode to “permissive” does not require a reboot, but disabling it via root access does.

**Troubleshooting SELinux**

If you suspect SELinux is the root cause for an issue, perform the following procedure to isolate the issue:
Procedure

Step 1
Enter the CLI command `utils os secure permissive`.

Step 2
Attempt to reproduce the issue.

If the issue disappears when SELinux is in permissive mode, then it is most likely a policy issue. Collect all relevant logs using the `utils create report [security]` CLI command and then contact TAC for assistance in resolving the issue.

Cisco Unified IP Phones

This section contains information about the following topics:

- Cisco Unified IP Phone 8941 and 8945, page 77
- Cisco Unified IP Phone Firmware 9.2(1) Features, page 77

Cisco Unified IP Phone 8941 and 8945

The Cisco Unified IP Phone 8941 and 8945 are new, easy-to-use IP Phones that provide high-quality voice services over IP. The phones offer a variety of features including:

- Integrated camera
- Color graphics display
- Full duplex speakerphone
- Rich media support
- Power over Ethernet (PoE)—IEEE 802.3af Class 1 (Cisco Unified IP Phone 8941) and IEEE 802.3af Class 2 (Cisco Unified IP Phone 8945)
- Built-in Gigabit Ethernet Switch (Cisco Unified IP Phone 8945 only)
- Bluetooth headset (Cisco Unified IP Phone 8945 only)

Cisco Unified IP Phone Firmware 9.2(1) Features

The following table lists the new features and the Cisco Unified IP Phone families affected by the Cisco Unified IP Phone 9.2(1) firmware release. In some cases, features are only applicable to part of a phone family, and these restrictions are noted in the table. For more information about each feature and the phones that support the feature, see the sections that follow the table.
## Assisted Directed Call Park

The Assisted Directed Call Park feature enables users to park a call by pressing only one button using the Direct Park feature. This feature requires administrators to configure a Busy Lamp Field (BLF) Assisted Directed Call Park button. When users press an idle BLF Assisted Directed Call Park button for an active call, the active call is parked at the Direct Park slot associated with the Assisted Directed Call Park button.

Support for this feature has been added to the following Cisco Unified IP Phones for Cisco Unified Communications Manager 8.6(1) and later:

- Cisco Unified IP Phone 6921 (SIP)
- Cisco Unified IP Phone 6941 (SIP)
- Cisco Unified IP Phone 6945 (SIP)
- Cisco Unified IP Phone 6961 (SIP)

### Where to Find More Information

- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6(1)
- Cisco Unified IP Phone User Guide for Cisco Unified Communications Manager 8.6(1)
- Cisco Unified Communications Manager Features and Services Guide
Classic Ringtones

The Classic Ringtones feature supports 29 ring tones: 2 embedded in the phone firmware and 27 downloaded from the Cisco Unified Communications Manager. The feature makes the available ring tones common with other Cisco Unified IP Phones.

The following phone models support the Classic Ringtones feature:
- Cisco Unified IP Phone 6921 (SCCP)
- Cisco Unified IP Phone 6941 (SCCP)
- Cisco Unified IP Phone 6945 (SCCP)
- Cisco Unified IP Phone 6961 (SCCP)

Where to Find More Information
Cisco Unified Communications Manager Features and Services Guide

CME Version Negotiation

The Cisco Unified Communications Manager Express (Unified CME) Version Negotiation feature supports a SIS version in the supported tag. The Cisco Unified IP Phones use the supported tag to interact with Cisco Unified Communications Manager Express and its supported SIS version.

The following phone models support the CME Version Negotiation feature:
- Cisco Unified IP Phone 6901 (SIP)
- Cisco Unified IP Phone 6911 (SIP)
- Cisco Unified IP Phone 6921 (SIP)
- Cisco Unified IP Phone 6941 (SIP)
- Cisco Unified IP Phone 6945 (SIP)
- Cisco Unified IP Phone 6961 (SIP)

Where to Find More Information
Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6(1)

EnergyWise

Cisco EnergyWise program promotes company-wide sustainability by monitoring, reporting, and reducing energy consumption across an entire corporate infrastructure. In the Cisco Unified IP Phone firmware, the EnergyWise feature allows phones to participate in an EnergyWise-enabled system. The phones can report power usage to the EnergyWise domain to allow the tracking and control of power within the customer premise.

In the Cisco Unified IP Phones, the EnergyWise feature enables the phone to sleep (power down) and wake (power up). A sleeping phone reduces energy consumption, typically into the 0 to 1 watt range. The administrator sets a working schedule of days, power up times, and power down times for each phone. At the scheduled power down time, the phone automatically powers down, and at the scheduled power up time, the phone automatically powers up.

The following Cisco Unified IP Phones support EnergyWise in this release:
- Cisco Unified IP Phone 6901 (SCCP)
EnergyWise in the Cisco Unified IP Phone 7900 Series

The Cisco Unified IP Phone 7900 series can be configured to automatically sleep and wake at specific times. When these phones are sleeping, users cannot wake them up.

EnergyWise in the Cisco Unified IP Phone 6900, 8900, and 9900 Series

The Cisco Unified IP Phone 6900, 8900, and 9900 series support EnergyWise by using configured sleep and wake times. In addition, users can wake a sleeping phone using the Select button. This feature allows the phone to participate in an EnergyWise enabled system. The phone reports its power usage to an EnergyWise compliant switch to allow the tracking and control of power within the customer premise. The phone provides alternate reduced power modes including an extremely low, off mode. The Unified CM administrator configures and exclusively manages the phones power state through vendor specific configuration on the Unified CM Admin pages.

When the phone turns off power after negotiation with an EnergyWise switch, it unregisters from Unified CM and enters Deep Sleep/PowerSavePlus mode.

For Cisco Unified IP Phone 9900 and 6900 Series, press the Select button on the phone to wake up the phone from the Deep Sleep/PowerSavePlus mode, but there is no way to register Cisco Unified IP Phone 7900 Series back to the Unified CM during Deep Sleep. This is the limitation for the Cisco Unified IP Phone 7900 Series. However, both types of phones automatically re-register with the Unified CM once
the Deep Sleep mode configured PowerON time occurs. You configure Deep Sleep mode on the Device page of the Unified CM. Configure Deep Sleep mode for the phones at least 10 minutes before the actual power off time to allow the information to synchronize between the switch and the phone.

The configured power off idle timer enables only in the case when there is physical interaction on the phone. If you do not physically interact with the phone such as call disconnection using an application, then the power idle timer defaults to 10 minutes.

**Enhanced Call Forward Notification**

The Enhanced Call Forward Notification feature provides additional call information to display in the notification window when a call forwards. This additional information includes the name or number of phone that forwarded the call. The type of information displayed is set by the system administrator.

The Enhanced Call Forward Notification feature is supported on the following phones:

- Cisco Unified IP Phone 6921 (SCCP)
- Cisco Unified IP Phone 6941 (SCCP)
- Cisco Unified IP Phone 6945 (SCCP)
- Cisco Unified IP Phone 6961 (SCCP)
- Cisco Unified IP Phone 8961 (SIP)
- Cisco Unified IP Phone 9951 (SIP)
- Cisco Unified IP Phone 9971 (SIP)

**Where to Find More Information**

- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6(1)
- Cisco Unified IP Phone User Guide for Cisco Unified Communications Manager 8.6(1)

**Forced Authentication Code and Client Matter Code Support**

The Forced Authentication Code (FAC) and Client Matter Code (CMC) Support features extends the FAC and CMC features to additional Cisco Unified IP Phones.

- FAC controls the types of calls that certain users can place. When placing a call, a user receives a prompt to enter a valid authorization code before the call is made.
- CMC enables a user to specify that a call relates to a specific client matter. When placing a call, a user can enter a code to indicate the type of call being placed (for example, to a specific customer).

The Forced Authentication Code and Client Matter Code Support feature is now supported on the following phones:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

**Where to Find More Information**

- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6(1)
- Cisco Unified IP Phone User Guide for Cisco Unified Communications Manager 8.6(1)
HTTP Download

The HTTP Download feature enhances the file download process to the phone. By default, the phone uses HTTP. If the HTTP download fails, the phone reverts to using the TFTP download.

This feature is supported on the following Cisco Unified IP Phones (SCCP and SIP):

- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961

Where to Find More Information

- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6(1)
- Cisco Unified IP Phone User Guide for Cisco Unified Communications Manager 8.6(1)

Missed Call Logs

The Missed Call Logs feature allows a user to specify whether missed calls are logged in the missed calls directory for a given line appearance.

This feature is supported on the following Cisco Unified IP Phones (SCCP and SIP):

- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961

Where to Find More Information

- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6(1)
- Cisco Unified IP Phone User Guide for Cisco Unified Communications Manager 8.6(1)

Multiple Calls per Line Appearance

The Multiple Calls Per Line feature supports multiple calls for each line. By default, your phone supports two active calls per line, and a maximum of six active calls per line. You can adjust this number of active calls (not exceeding six calls) according to your need using the Cisco Unified Communications Manager Assistant. Only one call can be connected at any time; other calls are automatically placed on hold.

This feature is supported on the following Cisco Unified IP Phones (SCCP and SIP):

- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961
Limitations
1. The system supports up to a maximum of 6 calls per line.
2. For phones with SCCP, the Cisco Unified Communications Manager must be running Release 8.6 or later to support the feature.

Where to Find More Information
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6(1)
- Cisco Unified IP Phone User Guide for Cisco Unified Communications Manager 8.6(1)
- Cisco Unified Communications Manager Features and Services Guide

Next Generation Power over Ethernet
The Next Generation Power over Ethernet (NGPoE+) feature enhances the ability of the phones to exceed the industrial standard IEEE 802.at. NGPoE+ provides up to 60 Watts (PSE) or 51 Watts (PD) to phones. On the Cisco Unified IP Phone side, the models support a maximum of 50.333 Watts (PSE) or 44 Watts (PD).

The phones self-adapt to the increased power. No user configuration is required.
This feature is supported on the following Cisco Unified IP Phones:
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

PLKs as Softkeys
The PLKs as Softkeys feature enables you to provide certain features to users as either softkeys or programmable line buttons on the phone.
The following features are now available as softkeys:
- Call PickUp
- Other Call PickUp
- Group Call PickUp
- Mobility
- Malicious Call Trace
- Meet Me
- Quality Reporting

This feature is supported on the following Cisco Unified IP Phones:
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Where to Find More Information
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6(1)
SSH Access

The SSH Access settings option allows you to enable or disable the SSH port on the phone using Unified CM Administration. When enabled, the option allows the phone to accept the SSH connections. Disabling the SSH server functionality of the phone blocks the SSH access to the phone. This setting is disabled by default.

This feature is supported on the following Cisco Unified IP Phones:

- Cisco Unified IP Phone 6901 (SCCP and SIP)
- Cisco Unified IP Phone 6911 (SCCP and SIP)
- Cisco Unified IP Phone 6921 (SCCP and SIP)
- Cisco Unified IP Phone 6941 (SCCP and SIP)
- Cisco Unified IP Phone 6945 (SCCP and SIP)
- Cisco Unified IP Phone 6961 (SCCP and SIP)
- Cisco Unified IP Phone 7906G (SCCP and SIP)
- Cisco Unified IP Phone 7911G (SCCP and SIP)
- Cisco Unified IP Phone 7931G (SCCP and SIP)
- Cisco Unified IP Phone 7941G (SCCP and SIP)
- Cisco Unified IP Phone 7941G-GE (SCCP and SIP)
- Cisco Unified IP Phone 7942G (SCCP and SIP)
- Cisco Unified IP Phone 7945G (SCCP and SIP)
- Cisco Unified IP Phone 7961G (SCCP and SIP)
- Cisco Unified IP Phone 7961G-GE (SCCP and SIP)
- Cisco Unified IP Phone 7962G (SCCP and SIP)
- Cisco Unified IP Phone 7965G (SCCP and SIP)
- Cisco Unified IP Phone 7970G (SCCP and SIP)
- Cisco Unified IP Phone 7975G (SCCP and SIP)
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Where to Find More Information

- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6(1)
- Cisco Unified IP Phone User Guide for Cisco Unified Communications Manager Guide 8.6(1)

Toast Timer

The Toast Timer feature controls the time that the Call Notification Pop-up Window (toast) remains visible for an incoming call. You select a time for all phones. The user cannot alter the timer.
This feature is supported on the following Cisco Unified IP Phones:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

**Where to Find More Information**

- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6(1)
- Cisco Unified IP Phone User Guide for Cisco Unified Communications Manager 8.6(1)

### UCR 2008 Support

The UCR 2008 feature provides the following functions:

- Support for Federal Information Processing Standard (FIPS) 104-2 Level 1—The phone requires the following functions:
  - Power On Self Testing, to ensure that the appropriate encryption algorithms are available. If the phone does not have the correct modules in the firmware, the phone will fail to boot.
  - Use of HTTPS for all internet communications.
  - Cisco Unified Communications Manager to be set up for FIPS compliance (for example, disabling 802.1x EAP-MD5).
- Support of IPv4 and IPv6 addressing
- Support of TVS IPv6—The phone displays the IPv6 address of a Trust Verification Service (TVS) server, if an IPv6 address is available. The Cisco Unified Communications Manager sends the additional IPv6 address, if available, to the phone.
- Support of 80-bit SRTCP Tagging—The phone handles both 32-bit and 80-bit SRTCP tags
- DSCP tagging for network management traffic
- Multilevel Precedence and Preemption (MLPP)—When placing a call, users can select a precedence level and have the call preempt an existing call of a lower priority.

The UCR 2008 feature is supported on the following Cisco Unified IP Phones:

- Cisco Unified IP Phone 6901 (SCCP)
- Cisco Unified IP Phone 6911 (SCCP)
- Cisco Unified IP Phone 6921 (SCCP)
- Cisco Unified IP Phone 6941 (SCCP)
- Cisco Unified IP Phone 6945 (SCCP)
- Cisco Unified IP Phone 6961 (SCCP)
- Cisco Unified IP Phone 7906G (SCCP)
- Cisco Unified IP Phone 7911G (SCCP)
- Cisco Unified IP Phone 7931G (SCCP)
- Cisco Unified IP Phone 7941G (SCCP)
- Cisco Unified IP Phone 7941GE (SCCP)
- Cisco Unified IP Phone 7942G (SCCP)
Cisco Unified Serviceability

- Cisco Unified IP Phone 7945G (SCCP)
- Cisco Unified IP Phone 7961G (SCCP)
- Cisco Unified IP Phone 7961G-GE (SCCP)
- Cisco Unified IP Phone 7962G (SCCP)
- Cisco Unified IP Phone 7965G (SCCP)
- Cisco Unified IP Phone 7970G (SCCP)
- Cisco Unified IP Phone 7971G-GE (SCCP)
- Cisco Unified IP Phone 7975G (SCCP)

Where to Find More Information
- Cisco Unified IP Phone User Guide for Cisco Unified Communications Manager 8.6(1)
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6(1)

Widescreen Video Enhancements

The Widescreen Video Enhancement feature provides support for the w360p Video Resolution. During video calls with a Cisco Camera, the phones negotiate the video resolution. The video window dimensions adjust according to the remote video resolution.

This feature is supported on the following Cisco Unified IP Phones:
- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Where to Find More Information
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager 8.6(1)
- Cisco Unified IP Phone User Guide for Cisco Unified Communications Manager 8.6(1)

Cisco Unified Serviceability

This section contains information about the following topics:
- Configuring Unified CM Call Home, page 86

Configuring Unified CM Call Home

Note

The Call Home feature introduced in Unified CM 8.6(1) requires back-office support from Smart Call Home (SCH) 3.2 planned for release in 2HCY2011. Please do not enable the feature in Unified CM serviceability until SCH 3.2 is released. Please check http://cisco.com/go/smartcall to confirm availability of SCH 3.2 prior to configuring Unified CM Call Home.
This section provides an overview of the Unified CM Call Home service and describes how to configure the Unified CM Call Home feature. The Call Home feature allows to communicate and send the diagnostic alerts, inventory, and other messages to the Smart Call Home back-end server.

**Understanding Smart Call Home**

Smart Call Home provides proactive diagnostics, real-time alerts, and remediation on a range of Cisco devices for higher network availability and increased operational efficiency. It accomplishes the same by receiving and analyzing the diagnostic alerts, inventory, and other messages from Smart Call Home enabled Cisco Unified Communications Manager. This particular capability of Unified CM is called as Unified CM Call Home.

Smart Call Home offers:

- Higher network availability through proactive, fast issue resolution by:
  - Identifying issues quickly with continuous monitoring, real-time, proactive alerts, and detailed diagnostics.
  - Making you aware of potential problems by providing alerts that are specific to only those types of devices in the network. Resolving critical problems faster with direct, automatic access to experts at Cisco Technical Assistance Center (TAC).

- Increased operational efficiency by providing customers the ability to:
  - Use staff resources more efficiently by reducing troubleshooting time.
  - Generate Service Requests to Cisco TAC automatically and route it to the appropriate support team that provides detailed diagnostic information and speedy resolution.

- Fast, web-based access to needed information that provides customers the ability to:
  - Review all Call Home messages, diagnostics, and recommendations in one place.
  - Check Service Request status quickly.
  - View the most up-to-date inventory and configuration information for all Call Home devices.
Figure 1 illustrates the Cisco Smart Call Home service.

**Figure 1  Cisco Smart Call Home Overview**

Smart Call Home contains modules that perform the following tasks:

- Raise Service Requests with Cisco TAC.
- Notify Customer of Call Home messages.
- Provide impact analysis and remediation steps.

For more information about Smart Call Home, see the Smart Call Home page at this location: http://www.cisco.com/en/US/products/ps7334/serv_home.html

**Smart Call Home Interaction with Unified CM Call Home**

If you have a service contract directly with Cisco Systems, you can register Unified CM for the Cisco Smart Call Home service. Smart Call Home provides fast resolution of system problems by analyzing Call Home messages that are sent from Unified CM and providing background information and recommendations.

The Unified CM Call Home feature delivers the following messages to the Smart Call Home back–end server:

- Alerts—Contain alert information for various conditions related to environment, hardware failure, and system performance. The alerts can be generated from any node within the Cisco Unified Communications Manager cluster. The alert details contain the node and other information required for troubleshooting purposes, depending on the alert type.

Table 12 lists the alerts that are sent to the Smart Call Home back–end server.
New and Changed Information for Cisco Unified Communications Manager Release 8.6(1)

Note

To control flooding of alert e-mails, you can change the default frequency of specific alert in RTMT. For more information about alerts, see the Cisco Unified Real Time Monitoring Tool Administration Guide.

- Configuration messages—Contain information about the row count for each database table that is related to a configuration. The configuration data consists of table name and row count for each table across the cluster.
- Inventory messages—Contain information about the cluster, nodes, and license.
- Telemetry messages—Contain information about the number of devices (IP phones, gateways, conference bridge, and so on) for each device type that is available on a Unified CM cluster. The telemetry data contains the device count for the entire cluster.

The configuration, inventory, and telemetry messages are sent periodically (first day of every month) to the Smart Call Home back–end server. The information in these messages enables TAC to provide timely and proactive service to help customers manage and maintain their network.

Pre-requisites for Unified CM Call Home

To support the Unified CM Call Home service, you require the following:
- A Cisco.com user ID associated with a corresponding Cisco Unified Communications Manager service contract.

Table 12  Alerts

<table>
<thead>
<tr>
<th>Alert Name</th>
<th>Default Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance Alerts</strong></td>
<td></td>
</tr>
<tr>
<td>CallProcessingNodeCPUPegging</td>
<td>Trigger up to 3 alerts within 30 minutes</td>
</tr>
<tr>
<td>CodeYellow</td>
<td>Trigger alert on every poll</td>
</tr>
<tr>
<td>CPUPegging</td>
<td>Trigger up to 3 alerts within 30 minutes</td>
</tr>
<tr>
<td>LowActivePartitionAvailableDiskSpace</td>
<td>Trigger up to 3 alerts within 30 minutes</td>
</tr>
<tr>
<td>LowAvailableVirtualMemory</td>
<td>Trigger up to 3 alerts within 30 minutes</td>
</tr>
<tr>
<td>LowSwapPartitionAvailableDiskSpace</td>
<td>Trigger up to 3 alerts within 30 minutes</td>
</tr>
<tr>
<td><strong>Database–Related Alerts</strong></td>
<td></td>
</tr>
<tr>
<td>DBReplicationFailure</td>
<td>Trigger up to 1 alert within 60 minutes</td>
</tr>
<tr>
<td><strong>Failed Calls Alerts</strong></td>
<td></td>
</tr>
<tr>
<td>MediaListExhausted</td>
<td>Trigger alert on every poll</td>
</tr>
<tr>
<td>RouteListExhausted</td>
<td>Trigger alert on every poll</td>
</tr>
<tr>
<td><strong>Crash–Related Alerts</strong></td>
<td></td>
</tr>
<tr>
<td>Coredumpfilefound</td>
<td>Trigger alert on every poll</td>
</tr>
<tr>
<td>CriticalServiceDown</td>
<td>Trigger alert on every poll</td>
</tr>
<tr>
<td><strong>Environment–Related Alert</strong></td>
<td></td>
</tr>
<tr>
<td>HardwareFailure</td>
<td>Trigger alert on every poll</td>
</tr>
</tbody>
</table>

To control flooding of alert e-mails, you can change the default frequency of specific alert in RTMT. For more information about alerts, see the Cisco Unified Real Time Monitoring Tool Administration Guide.

- Configuration messages—Contain information about the row count for each database table that is related to a configuration. The configuration data consists of table name and row count for each table across the cluster.
- Inventory messages—Contain information about the cluster, nodes, and license.
- Telemetry messages—Contain information about the number of devices (IP phones, gateways, conference bridge, and so on) for each device type that is available on a Unified CM cluster. The telemetry data contains the device count for the entire cluster.

The configuration, inventory, and telemetry messages are sent periodically (first day of every month) to the Smart Call Home back–end server. The information in these messages enables TAC to provide timely and proactive service to help customers manage and maintain their network.

Pre-requisites for Unified CM Call Home

To support the Unified CM Call Home service, you require the following:
- A Cisco.com user ID associated with a corresponding Cisco Unified Communications Manager service contract.
• Internet Explorer (IE) 6.0 or later, Mozilla Firefox, or Safari browsers.
• It is highly recommended that both the Domain Name System (DNS) and Simple Mail Transfer Protocol (SMTP) servers are setup for the Unified CM Call Home feature.
  – DNS setup is required to send the Call Home messages using Secure Web (HTTPS).
  – SMTP setup is required to send the Call Home messages to Cisco TAC or to send a copy of the messages to a list of recipients through email.

**Accessing Unified CM Call Home**

To access Unified CM Call Home, go to Cisco Unified Serviceability Administration and choose CallHome (Cisco Unified Serviceability > CallHome > Call Home Configuration).

**Default Unified CM Call Home Settings**

Table 13 lists the default Unified CM Call Home settings.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Home feature status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Send Data to Cisco Technical Assistance Center (TAC) using</td>
<td>Secure Web (HTTPS)</td>
</tr>
</tbody>
</table>

**Configuring Unified CM Call Home**

In Cisco Unified Serviceability, choose CallHome > Call Home Configuration. The Call Home Configuration window appears.

Table 14 describes the settings to configure the Unified CM Call Home.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Home Message Schedule</td>
<td>Displays the date and time of the last Call Home messages sent and the next message scheduled.</td>
</tr>
<tr>
<td>Customer Contact Details</td>
<td></td>
</tr>
<tr>
<td>Enable Call Home</td>
<td>Check this check box to activate the Unified CM Call Home service. This setting is disabled by default.</td>
</tr>
</tbody>
</table>
Table 14  Unified CM Call Home Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Address</td>
<td>Enter the contact email address of the customer. This is a mandatory field. The email address validations are:</td>
</tr>
<tr>
<td></td>
<td>• The address format of email address: &lt;username&gt;@&lt;domain&gt;.&lt;top-level-domain&gt;</td>
</tr>
<tr>
<td></td>
<td>• The address format can support hierarchical domain names; for example, <a href="mailto:abc@def.ghi.com">abc@def.ghi.com</a></td>
</tr>
<tr>
<td></td>
<td>• The username can start and end only with an alphanumeric character.</td>
</tr>
<tr>
<td></td>
<td>• The username can contain special characters like hyphen (-), dot (.), and underscore (_).</td>
</tr>
<tr>
<td></td>
<td>• The top level domain can vary from two to nine characters.</td>
</tr>
<tr>
<td>Company (Optional)</td>
<td>Enter the name of the company. You can enter up to 255 characters.</td>
</tr>
<tr>
<td>Contact Name (Optional)</td>
<td>Enter the contact name of the customer. You can enter up to 128 characters. The contact name can contain alphanumeric characters and some</td>
</tr>
<tr>
<td></td>
<td>special characters like dot (.), underscore (_) and hyphen (-).</td>
</tr>
<tr>
<td>Address (Optional)</td>
<td>Enter the address of the customer. You can enter up to 1024 characters.</td>
</tr>
<tr>
<td>Phone (Optional)</td>
<td>Enter the phone number of the customer.</td>
</tr>
<tr>
<td>Send Data to Cisco Technical Assistance Center (TAC)</td>
<td>Check this check box to communicate the Call Home messages securely to TAC. For communication, you can choose either Secure Web (HTTPS) or email option from the list.</td>
</tr>
</tbody>
</table>
**Limitations**

The following limitations apply when Unified CM server is down or unreachable:

- **Call Home Message Schedule**—Fails to capture the date and time of the last Call Home messages sent and the next message scheduled, until the server is reachable

- **Call Home Now**—Does not send the Call Home messages on demand, until the server is reachable

**Unified CM Administration Configuration Tips**

No configuration tips exist for this feature.

---

**Table 14  Unified CM Call Home Configuration Settings (continued)**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Send a copy to the following email addresses | Check this check box to send a copy of the Call Home messages to the specified email addresses. The email address validations are:  
• Multiple email addresses are separated by a comma but must not end with a comma.  
• The address format of email address: `<username>@<domain>.<top-level-domain>`  
• The address format can support hierarchical domain names; for example, `abc@def.ghi.com`  
• The username can start and end only with an alphanumeric character.  
• The username can contain special characters like hyphen (-), dot (.), and underscore (_).  
• The top level domain can vary from two to nine characters. To enable the Call Home feature, you must check either the Send Data to Cisco Technical Assistance Center (TAC) or Send a copy to the following email addresses check box.  

<table>
<thead>
<tr>
<th>Save</th>
<th>Saves your Call Home configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>After you save your Call Home Configuration, an End User License Agreement (EULA) message appears. If you are configuring for the first time, you must accept the license agreement.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>To deactivate the Call Home service that you activated, uncheck the Enable Call Home check box; then, click Save.</td>
</tr>
<tr>
<td>Reset</td>
<td>Resets to last saved configuration.</td>
</tr>
<tr>
<td>Save and Call Home Now</td>
<td>Saves and sends the Call Home messages instantly (on demand).</td>
</tr>
</tbody>
</table>
GUI Changes

A new Call Home Configuration window allows you to configure the Cisco Unified Call Home, and deliver the Call Home messages to the Smart Call Home back-end server. In Cisco Unified Serviceability, choose Call Home > Call Home Configuration.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations

You can configure the Unified CM Call Home by checking the Enable Call Home check box on the Call Home Configuration window in Cisco Unified Serviceability.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

Cisco Unified Real-Time Monitoring Tool

This section contains information about the following topics:

- Cisco TelePresence MCU Conference Bridge Device, page 93
- Single Sign On in RTMT, page 94
- Collecting SELinux Logs Using RTMT, page 95

Cisco TelePresence MCU Conference Bridge Device

The Cisco TelePresence MCU Conference Bridge Device provides information about registered MCU conference bridge devices. Table 15 contains information about the Cisco TelePresence MCU Conference Bridge Device counters, added in this release.
Single Sign On in RTMT

Single Sign On can be enabled in RTMT.

To enable the single sign on feature in RTMT, modify the Windows registry as follows:

```plaintext
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\nValue Name: allowtgtsessionkey
Value Type: REG_DWORD
Value: 0x01
```

Following is the procedure to launch RTMT, with or without enabling single sign on.

**Procedure**

**Step 1** After you install the plug-in, perform one of the following tasks:

- From your Windows desktop, double-click the **Cisco Unified Real-Time Monitoring Tool** icon.
- Choose **Start > Programs > Cisco > Unified-Communications-Manager Serviceability > Real-Time Monitoring Tool** > **Real-Time Monitoring Tool**.

The login window displays.

**Step 2** In the Host IP Address field, enter either the IP address or host name of the Unified CM server or (if applicable) the first Unified CM server in a cluster.

**Step 3** Enter the port that the application will use to listen to the server. The default setting equals 8443.
The Trace and Log Central tool in RTMT uses the port number that you specify to communicate with all the nodes in a cluster. If your system uses port mapping and all Cisco CallManager nodes do not map to the same port number, then some RTMT tools can not connect to those nodes. The tools that will fail to connect include Trace and Log Central, Job Status, SyslogViewer, Perfmon Log Viewer, and FTP/SFTP Configuration.

**Step 4** Check the **Secure Connection** check box.

**Step 5** Click **OK**.

If single sign on feature is enabled in the Unified CM server, RTMT does not prompt for the user name and password; proceed to Step 8.

If single sign on is not enabled, RTMT displays another window prompting for user name and password. Enter the details as given in the following steps.

**Step 6** In the **User Name** field, enter the Administrator username for the application.

**Step 7** In the **Password** field, enter the Administrator user password that you established for the username.

**Note** If the authentication fails or if the server is unreachable, the tool prompts you to reenter the server and authentication details, or you can click the Cancel button to exit the application. After the authentication succeeds, RTMT launches the monitoring module from local cache or from a remote server, when the local cache does not contain a monitoring module that matches the backend version.

**Step 8** When prompted, add the certificate store by clicking **Yes**.

Cisco Unified Real-Time Monitoring Tool starts.

**Note** If you have logged in using the single sign on feature, RTMT prompts for user name and password once, when you click on any one of the following menus:

- System > Performance > Performance log viewer
- System > Tools > Trace and Log Central
- System > Tools > Job status
- System > Tools > Syslog Viewer
- CallManager > CallProcess > Session Trace
- CallManager > CallProcess > Called Party Tracing
- CallManager > Report > Learned Pattern
- CallManager > Report > SAF forwarders
- Analysis Manager

### Collecting SELinux Logs Using RTMT

Collect logs for SELinux by using the Real-Time Monitoring Tool (RTMT). RTMT contains the following utilities to collect logs:
## Table 16  RTMT Utilities

<table>
<thead>
<tr>
<th>Utility</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Browse</td>
<td>The Remote Browse utility enables users to:</td>
</tr>
<tr>
<td></td>
<td>- Browse trace or log files for services, applications, and system logs.</td>
</tr>
<tr>
<td></td>
<td>- Download selected files from the Browse window</td>
</tr>
<tr>
<td></td>
<td>To enable the Remote Browse utility, click the Remote Browse option under Trace and Log Central. Scroll down the list to find SELinux logs, and select the servers from which to collect logs. Click Finish after all servers have been selected.</td>
</tr>
<tr>
<td></td>
<td>RTMT creates two separate log files: an SELinux Startup log file and a vos-audit log file. The SELinux Startup log file is located in the System &gt; SELinux logs &gt; platform folder. The vos-audit log is located in the System &gt; Cisco Audit Logs &gt; vos folder. These files can be downloaded to a local folder.</td>
</tr>
<tr>
<td>Collect Files</td>
<td>Enables users to collect log or trace files for services, applications, and system logs matching the given time range.</td>
</tr>
<tr>
<td>Query Wizard</td>
<td>Enables users to query log or trace files for services, applications, and system logs given a match string and time range.</td>
</tr>
<tr>
<td>Schedule Collection</td>
<td>Enables users to create scheduled collection tasks for log or trace files for services, applications, and system logs using a given time range and collection interval.</td>
</tr>
<tr>
<td>Real Time Trace</td>
<td>The Real Time Trace utility enables users to:</td>
</tr>
<tr>
<td></td>
<td>- See log or trace files for services, applications, and system logs in real time and give basic search functionality using the View Real Time Data option</td>
</tr>
<tr>
<td></td>
<td>- Monitor an event in log or trace files for services, applications, and system logs given a monitoring time range using the Monitor User Event option. When a match is found, several actions can be taken, such as:</td>
</tr>
<tr>
<td></td>
<td>- Raise an alert</td>
</tr>
<tr>
<td></td>
<td>- Local syslog</td>
</tr>
<tr>
<td></td>
<td>- Remote syslog</td>
</tr>
<tr>
<td></td>
<td>- Download file</td>
</tr>
<tr>
<td>Collect Crash Dump</td>
<td>Enables users to collect Core Dump Files for given services or applications and matched time ranges.</td>
</tr>
</tbody>
</table>
APIs

This section contains information about the following topics:

- Cisco CTI Scalability Increase, page 97
- Cisco Unified JTAPI Developers Guide, page 97
- Cisco Unified TAPI Developers Guide, page 102
- Cisco Unified Communications Manager XML Developers Guide, page 105
- Cisco Unified IP Phone Services Application Development Notes, page 106

Cisco CTI Scalability Increase

Cisco CTI now provides 100% support for all standard Users and Devices on a Unified Communications Manager cluster:

- Standard Users can be configured with up to 5 CTI applications and 5 lines on each device when the device Busy Hour Call Attempt (BHCA) rate is 6 calls per hour.
- To ensure cluster resources are sizing appropriately, use the Cisco Unified Communications Sizing Tool at http://tools.cisco.com/cucst.

Cisco Unified JTAPI Developers Guide

This section describes new and changed JTAPI information for Cisco Unified Communications Manager, release 8.6(1):

- EnergyWise Deep Sleep Mode, page 97
- Federal Information Processing Standard (FIPS) 140-2 Mode, page 98
- JTAPI Account lockout, page 99
- JTAPI Password expiry, page 100
- JTAPI 64-bit Client Support, page 101

EnergyWise Deep Sleep Mode

When a terminal unregisters from Unified CM, JTAPI exposes CiscoProvTerminalUnRegisteredEV event to application with a new reason “CiscoProvterminal UnRegisteredEVENERGYWISE POWER_SAVE_PLUS”.

JTAPI exposes CiscoTermOutOfServiceEv event to the application with the cause “CiscoOutOfServiceEv.CAUSE_ENERGYWISE_POWER_SAVE_PLUS” when a terminal goes out of service due to Deep Sleep mode configured.

JTAPI sends CiscoAddrOutOfServiceEv event to application with a new cause “CiscoOutOfServiceEv.CAUSE_ENERGYWISE_POWER_SAVE_PLUS” when an address goes out of service due to Deep Sleep mode configured.

Interface Changes

public interface CiscoProvTerminalUnRegisteredEv
When a terminal unregisters from the Unified CM because of Deep Sleep mode, JTAPI sends CiscoProvTerminalUnregisteredEv to the application with the reason “ENERGYWISE_POWER_SAVE_PLUS”.

### Reason Codes

**ENERGYWISE_POWER_SAVE_PLUS**

Sample Code:
```
public class MyTermObserver implements ProviderObserver {

    public void providerChangedEvent (ProvEv[] evlist) {
        for(int i=0; evlist != null && i < evlist.length; i++){
            ...
            If ( evlisth[i] instanceof  CiscoProvTerminalUnregisteredEv){
                CiscoProvTerminalUnregisteredEv ev = (CiscoProvTerminalUnregisteredEv)evlist[i];
                if(ev.getReason() ==
                    CiscoProvTerminalUnregisteredEv.ENERGYWISE_POWER_SAVE_MODE){
                    System.out.println("Terminal Unregistered from CUCM because of deep
                        with the reason as ENERGYWISE_POWER_SAVE_PLUS
                        ");
                }
            }
        }
    }

    public interface CiscoOutOfServiceEv

    When a terminal/address unregisters from Unified CM because of deep sleep mode, Jtapi will deliver CiscoTermOutOfServiceEv and CiscoAddrOutOfServiceEv to the application with this new cause “CAUSE_ENERGYWISE_POWER_SAVE_PLUS”.

```

### Cause Code

**CAUSE_ENERGYWISE_POWER_SAVE_PLUS**

### Federal Information Processing Standard (FIPS) 140-2 Mode

FIPS, or Federal Information Processing Standard, is a U.S. and Canadian government certification standard that defines requirements that cryptographic modules must follow.

Cisco Unified Communications Manager 8.6 is FIPS 140-2 compliant, in accordance with the U.S. National Institute of Standards (NIST), and can operate in FIPS mode, level 1 compliance.

When you enable FIPS 140-2 mode, Cisco Unified Communications Manager reboots, runs certification self-tests at startup, performs the cryptographic modules integrity check, and then regenerates the keying materials. At this point, Cisco Unified Communications Manager operates in FIPS 140-2 mode.

Cisco Unified Communications Manager 8.6 meets FIPS requirements, including the following: it performs startup self-tests and a restricts to a list of approved cryptographic functions.
Cisco Unified Communications Manager FIPS mode uses the following FIPS 140-2 level 1 validated cryptographic modules:

- OpenSSL 0.9.8l with FIPS Module 1.2
- RSA CryptoJ 4.1
- Red Hat Openssl
- Red Hat Openswan
- NSS

**Note**
By default, Cisco Unified Communications Manager is in non-FIPS mode. The administrator must enable FIPS mode.

**Unified CM Administration Configuration Tips**
No tips.

**GUI Changes**
No GUI changes.

**Service Parameter and Enterprise Parameter Changes**
No service or enterprise parameter changes exist for this feature.

**Installation/Upgrade (Migration) Considerations**
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can enable this feature via CLI.

**Serviceability Considerations**
No serviceability considerations exist for this feature.

**BAT Considerations**
No BAT considerations exist for this feature.

**CAR/CDR Considerations**
No CAR or CDR considerations exist for this feature.

**Security Considerations**
No security considerations exist for this feature.

**AXL and CTI Considerations**
No AXL or CTI considerations exist for this feature.

**User Tips**
No user tips exist for this feature.

**JTAPI Account lockout**

**Description**
Unified CM 8.6(1) supports JTAPI on Account lockout.
In case of account lockout, JTAPI delivers detailed exceptions without any warning messages. JTAPI does not allow applications to modify any of these values, it only reports the information.

**Unified CM Administration Configuration Tips**
No administration configuration tips exist for this feature.

**GUI Changes**
No GUI changes.

**Service Parameter and Enterprise Parameter Changes**
No service or enterprise parameter changes exist for this feature.

**Installation/Upgrade (Migration) Considerations**
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

**Serviceability Considerations**
No serviceability considerations exist for this feature.

**BAT Considerations**
No BAT considerations exist for this feature.

**CAR/CDR Considerations**
No CAR or CDR considerations exist for this feature.

**Security Considerations**
No security considerations exist for this feature.

**AXL and CTI Considerations**
No AXL or CTI considerations exist for this feature.

**User Tips**
No user tips exist for this feature.

For more information about JTAPI Account lockout feature documentation, see the *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager 8.6(1)*.

**JTAPI Password expiry**

**Description**
Unified CM 8.6(1) supports JTAPI on password expiry configuration.
The password expiry configuration allows the administrator to specify the following two parameters:
1. The time before the password expires (in days) and
2. The number of days before the end of the password expiry to alert the user to change the password
If a password is expired, JTAPI will deliver an exception to the application. In a scenario where a password is going to expire soon, JTAPI will deliver a new event to the application.
Unified CM Administration Configuration Tips
The administrator can use the Unified CM Admin Panel to configure options for login credentials.

GUI Changes
No GUI changes.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

For more information about JTAPI Password expiry feature documentation, see the Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager 8.6(1).

JTAPI 64-bit Client Support

Description
Unified CM 8.6(1) supports JTAPI on 64-bit platforms.

Unified CM Administration Configuration Tips
No administration configuration tips exist for this feature.

GUI Changes
No GUI changes.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.
Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

For more information about JTAPI 64-bit Client Support feature documentation, see the Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager 8.6(1).

Cisco Unified TAPI Developers Guide

This section describes new and changed JTAPI information for Cisco Unified Communications Manager, release 8.6(1):

- EnergyWise Deep Sleep Mode, page 102
- Federal Information Processing Standard (FIPS) 140-2 Mode, page 103
- TAPI Password Expiry Notification, page 104

EnergyWise Deep Sleep Mode

TAPI provides the PHONE_STATE message with dwparam1 = PHONESTATE_SUSPEND and EnergyWisePowerSavePlus reason in dwParam2 when the phone unregisters as it enters DeepSleep, and if the phone successfully negotiates with the appropriate extension version 0x000B0000 or higher.

TAPI provides the LINE_LINEDEVSTATE message with dwparam1 = LINEDEVSTATE_OUTOFSERVICE and EnergyWisePowerSavePlus reason in dwparam2 when the phone unregisters as it enters DeepSleep, and if the phone successfully negotiates with the appropriate extension version 0x000B0000 or higher.

As part of this feature TAPI exposes all out of service reason codes in the PHONESTATE_SUSPEND and LINEDEVSTATE_OUTOFSERVICE in dwParam2 when the phone unregisters, and if the phone successfully negotiates with the appropriate extension version 0x000B0000 or higher.

TAPI defines a new enum CiscoLineDevStateOutOfServiceReason in CiscoLineDevSpecificMsg.h
And enum CiscoPhoneStateOutOfServiceReason in CiscoPhoneDevSpecificMsg.h
Interface Changes

New Enum under CiscoLineDevSpecificMsg.h

```c
enum CiscoLineDevStateOutOfServiceReason {
    CiscoLineDevStateOutOfServiceReason_Unknown = 0x00000000,
    CiscoLineDevStateOutOfServiceReason_CallManagerFailure = 0x00000001,
    CiscoLineDevStateOutOfServiceReason_ReHomeToHigherPriorityCM = 0x00000002,
    CiscoLineDevStateOutOfServiceReason_NoCallManagerAvailable = 0x00000003,
    CiscoLineDevStateOutOfServiceReason_DeviceFailure = 0x00000004,
    CiscoLineDevStateOutOfServiceReason_DeviceUnregistered = 0x00000005,
    CiscoLineDevStateOutOfServiceReason_EnergyWisePowerSavePlus = 0x00000006,
    CiscoLineDevStateOutOfServiceReason_CtiLinkFailure = 0x00000101
};
```

New Enum under CiscoPhoneDevSpecificMsg.h

```c
enum CiscoPhoneStateOutOfServiceReason {
    CiscoPhoneStateOutOfServiceReason_Unknown = 0x00000000,
    CiscoPhoneStateOutOfServiceReason_CallManagerFailure = 0x00000001,
    CiscoPhoneStateOutOfServiceReason_ReHomeToHigherPriorityCM = 0x00000002,
    CiscoPhoneStateOutOfServiceReason_NoCallManagerAvailable = 0x00000003,
    CiscoPhoneStateOutOfServiceReason_DeviceFailure = 0x00000004,
    CiscoPhoneStateOutOfServiceReason_DeviceUnregistered = 0x00000005,
    CiscoPhoneStateOutOfServiceReason_EnergyWisePowerSavePlus = 0x00000006,
    CiscoPhoneStateOutOfServiceReason_CtiLinkFailure = 0x00000101
};
```

Federal Information Processing Standard (FIPS) 140-2 Mode

FIPS, or Federal Information Processing Standard, is a U.S. and Canadian government certification standard that defines requirements that cryptographic modules must follow.

Cisco Unified Communications Manager 8.6 is FIPS 140-2 compliant, in accordance with the U.S. National Institute of Standards (NIST), and can operate in FIPS mode, level 1 compliance.

When you enable FIPS 140-2 mode, Cisco Unified Communications Manager reboots, runs certification self-tests at startup, performs the cryptographic modules integrity check, and then regenerates the keying materials. At this point, Cisco Unified Communications Manager operates in FIPS 140-2 mode.

Cisco Unified Communications Manager 8.6 meets FIPS requirements, including the following: it performs startup self-tests and a restricts to a list of approved cryptographic functions.

Cisco Unified Communications Manager FIPS mode uses the following FIPS 140-2 level 1 validated cryptographic modules:

- OpenSSL 0.9.8l with FIPS Module 1.2
- RSA CryptoJ 4.1
- Red Hat OpenSSL
- Red Hat Openswan
- NSS

Note

By default, Cisco Unified Communications Manager is in non-FIPS mode. The administrator must enable FIPS mode.

Unified CM Administration Configuration Tips

No tips.
GUI Changes
No GUI changes.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can enable this feature via CLI.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

TAPI Password Expiry Notification

Description
Unified CM 8.6(1) supports TAPI on Password Expiry Notification.

The password expiry notification notifies the user about the password expiry date and provides the specific reason for the initialization failure if the password is already expired or the account is locked. The Cisco TSP initialization fails and a message is displayed if the password is expired.

A user account gets locked in any of the following conditions:

- Threshold number of incorrect logins is exceeded. This appears as Failed Logon in the user credential page.
- Administrator has locked the user account.
- Credential has not been used in a number of days as specified on the user credential page and the account is locked due to inactivity. This appears as Inactive Days Allowed on the user credential page.

Unified CM Administration Configuration Tips
No administration configuration tips exist for this feature.
GUI Changes
No GUI changes.

Service Parameter and Enterprise Parameter Changes
No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations
No special installation or upgrade considerations exist for this feature. After you install or upgrade to Unified CM 8.6(1), you can use this feature.

Serviceability Considerations
No serviceability considerations exist for this feature.

BAT Considerations
No BAT considerations exist for this feature.

CAR/CDR Considerations
No CAR or CDR considerations exist for this feature.

Security Considerations
No security considerations exist for this feature.

AXL and CTI Considerations
No AXL or CTI considerations exist for this feature.

User Tips
No user tips exist for this feature.

For more information about TAPI Password expiry notification feature documentation, see the Cisco Unified TAPI Developers Guide for Cisco Unified Communications Manager 8.6(1).

Cisco Unified Communications Manager XML Developers Guide

This sections provides information about the updates made in the following sections of the XML Developers guide for Cisco Unified Communications Manager, release 8.6(1):

- Administrative XML API, page 105
- Extension Mobility Service API, page 106
- Routing Rules API, page 106
- Serviceability XML API, page 106
- Web Dialer API, page 106

Administrative XML API

No changes in the Administrative XML APIs. The Administrative XML API only changes in the first major (x.0), and first minor (x.5) releases.
Extension Mobility Service API

No changes in the Extension Mobility Service APIs.

Routing Rules API

No changes in the Routing Rules APIs.

Serviceability XML API

No changes in the Serviceability XML APIs.

Web Dialer API

No Changes in the Web Dialer APIs.

Cisco Unified IP Phone Services Application Development Notes

No changes in the Cisco Unified IP Phone Services Application Development Notes.