Utils Commands

utils auditd

This command starts, stops, and provides the status of the system auditing service.

utils auditd enable | **disable** | **status**

Syntax Description

Parameters	Description
enable	Enables the collection of audit logs. When enabled, the system monitors and records user actions as well as Linux events such as the creation and removal of users, as well as the editing and deleting of files .
disable	Disables the collection of audit logs.
status	Displays the status of audit log collection. Cisco recommends that you retrieve the audit log by using the Real-Time Monitoring Tool, but you can also retrieve it by using the CLI.

Command Modes Administrator (admin:)

Usage Guidelines After the service has been enabled, it monitors and logs activity on the system. Be aware that the system auditing service logs a lot of information. Care must be taken not to overfill the disk.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils branding enable

Run this command to enable branding on this node.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Applies to: Cisco Unfiied Communications Manager, IM and Presence Service

utils branding disable

Run this command to disable branding on this node.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Applies to: Cisco Unfiied Communications Manager, IM and Presence Service

utils branding status

Run this command to see the status of whether branding is enabled or disabled on this node.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Applies to: Cisco Unfiied Communications Manager, IM and Presence Service

utils contactsearchauthentication disable

This command disables the secure contact search authentication mode. After this mode is disabled, you need to reset the phone for the changes to take effect.

utils contactsearchauthentication disable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils contactsearchauthentication enable

This command enables the secure contact search authentication mode. After this mode is enabled, reset the phone for the changes to take effect.

utils contactsearchauthentication enable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils contactsearchauthentication status

This command shows whether the system is operating in contact search authentication enable mode or contact search authentication disable mode.

utils contactsearchauthentication status

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils core analyze

This command generates a backtrace for a core file, a thread list, and the current value of all CPU registers.

utils core active | **inactive analyze** [*core_filename*]

Syntax Description

Parameters	Description
active	Specifies an active version
inactive	Specifies an inactive version
core_filename	Specifies the name of the core file from which to generate the stack trace.

Command Modes

Administrator (admin:)

Usage Guidelines

This command creates a file of the same name as the core file, with a .txt extension, in the same directory as the core file. After you execute this command on a core file created by cimserver, an unexpected message displays. This message is a known limitation of the command.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils core list

This command displays all active or inactive core files.

utils core active | **inactive list**

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils capf cert import

utils capf cert import

Use this command to upload signed phone certificates to your system.

Usage Guidelines

You can choose to import your signed certificates through either FTP or TFTP.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager

utils create report

This command creates reports about the server in the platform/log directory.

utils create report hardware | platform | security

Syntax Description

Parameters	Description
hardware	Creates a system report that contains disk array, remote console, diagnostic, and environmental data.
platform	Collects the platform configuration files into a TAR file.
security	Collects the diagnostic reports and creates a TAR file that you can download for troubleshooting purposes. You can retrieve this file with the **file get** command.

Command Modes

Administrator (admin:)

Usage Guidelines

You are prompted to continue after you enter the command.

After you create a report, use the command **file get activelog platform/log/***filename* command, to get the report. where *filename* specifies the report filename that displays after the command completes.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils create report database

This command collects all log the files that are needed for database troubleshooting.

utils create report hardware | platform | security

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils ctl

utils ctl set-cluster mixed-mode | set-cluster non-secure-mode | update CTLFile

This command changes the cluster security mode or updates the CTL file in each of the nodes.

Syntax Description

Parameters	Description
set-cluster mixed-mode	Updates the CTL file and sets the cluster to mixed mode (db secure mode is set to 1). If the cluster is already in mixed mode, this command shows that Unified Communications Manager is in mixed mode and Autoregistration is active. You need to confirm your action. **Note** To enable mixed-mode, ensure that the Communications Manager is registered with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite and the Registration Token received from the Smart account or Virtual account has Allow export-controlled functionality enabled while registering with this cluster.
set-cluster non-secure-mode	Updates the CTL file and set the cluster to non-secure mode. If the cluster is already in mixed mode, this command shows that Unified Communications Manager is in non-secure mode.
update CTLFile	Updates the CTL file in each of the nodes of the cluster. **Note** To update the CTLFile in mixed-mode, ensure that the Unified Communications Manager is registered with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite and the Registration Token received from the Smart account or Virtual account has Allow export-controlled functionality enabled while registering with this cluster.

Command Modes

Administrator (admin:)

Usage Guidelines

The CLI must be executed on the publisher. On all other nodes, this CLI command is disabled.

Note After you regenerate the CTL file, you must restart CallManager and TFTP services across the cluster.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager.

utils ctl reset localkey

This command is used to regenerate the CTL file and sign it with the secondary SAST role (CallManager). Use this command when the ITLRecovery certificate that was used to sign the original CTL file has changed and the endpoints are locked out.

utils ctl reset localkey

Syntax Description

localkey	Generates a new CTL file, updates the CTL file on the publisher. The command signs the CTLfile with CallManager key.

Command Modes

Administrator (admin:)

Usage Guidelines

Note

- You must run this command on the Unified Communications Manager publisher node.
- After the endpoints receive the new CTL file, which is signed by CallManager Key and contains the new ITLRecovery certificate, execute the CTL update command (utils ctl update CTLFile) again to sign it with the ITLRecovery certificate. The CTL file is regenerated but signed by the new ITLRecovery certificate, which is now trusted by the endpoint.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager

utils cuc activate CUSRSV

This command converts the standalone Cisco Unity Connection server to Cisco Unity Connection SRSV server.

utils cuc activate CUSRSV

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc cluster activate

This command activates this server in a Cisco Unity Connection cluster.

utils cuc cluster activate

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

utils cuc cluster deactivate

This command deactivates this server in a Cisco Unity Connection cluster.

utils cuc cluster deactivate

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

utils cuc cluster makeprimary

This command forces the specified server to take the primary server status in a Cisco Unity Connection cluster.

utils cuc cluster makeprimary

Syntax Description

Parameters	Description
server	Specifies the name of the server to take the primary server status in a Cisco Unity Connection cluster.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

utils cuc cluster overwritedb

This command overwrites the data on the server with the data on the other server in a Cisco Unity Connection cluster.

utils cuc cluster overwritedb

Command Modes

Administrator (admin:)

Usage Guidelines

This command overwrites the database on the server on which you run this command with the database from the other server in the Connection cluster. Replication restarts after the database is overwritten. This method is used when you restore one server from a backup and must copy the restored data to the other server.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

utils cuc cluster renegotiate

This command creates a cluster relationship with the publisher server in a Connection cluster after the server was replaced or the Connection was reinstalled on the publisher server. This command overwrites all data on the publisher server with data from the subscriber server and initializes replication between the servers.

utils cuc cluster renegotiate

Command Modes

Administrator (admin:)

Usage Guidelines

Run this command on the subscriber server in a Connection cluster to set up a trust with a publisher server that has been replaced or on which Connection has been reinstalled.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

utils cuc create report

This command collects data that is helpful to technical support staff for troubleshooting the system. Data collected includes version information, cluster status, service information, database information, trace files, log files, disk information, memory information, and restart information.

utils cuc create report

Command Modes

Administrator (admin:)

Usage Guidelines

After the command completes, detailed information gets saved in a .zip file, and the location of the zip file displays. Use the **file get** command to move the file to a computer on which you can uncompress the file and view the contents.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection only

Example

```
admin: utils cuc create report
Getting unity connection version. Please wait...Done
Getting cluster status. Please wait...Done
Getting service information. Please wait...Done
Getting installed locales. Please wait...Done
Getting database schema version. Please wait...Done
Getting database integrity. Please wait...Done
Getting database diagnostic log. Please wait...Done
Getting database message log. Please wait...Done
Getting trace files. Please wait...Done
Getting log files. Please wait...Done
Getting platform status. Please wait...Done
Compressing 75 files. Please wait...Done
Output is in file: cuc/cli/systeminfo_080318-140843.zip
To free disk space, delete the file after copying it to another computer
```

utils cuc dbreplication 01_tear_down

This command breaks the replication and connectivity between two Unity Connection servers in a cluster. Running this command on both the servers ensures ideal cleanup before establishing a good replication between the servers.

utils cuc dbreplication 01_tear_down

Command Modes

Administrator (admin:)

Usage Guidelines

In case of long Unity Connection database CDR queue buildup, this command cleans the buildup for providing clean ground to establish server connectivity and replication between the two servers in the cluster.

Note It is recommended to :

- Take the system backup before running the command.
- Collect the screen log information along with command line logs if the command fails and escalate it to Cisco TAC.
- Ensure that only Cisco TAC runs the command.
- Run the command on the server with obsolete data as the synchronization process deletes the data that clashes with the information on the other server.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc dbreplication 02_define_servers

This command establishes the network connectivity between the two Unity Connection servers in a cluster.

utils cuc dbreplication 02_define_servers

Command Modes

Administrator (admin:)

Usage Guidelines

You can use this command to track and report the CDR traffic from one server to another in a Unity Connection cluster. During SBR process, this command helps in defining the roles of the two server in a cluster.

Note It is recommended to :

- Take the system backup before running the command.
- Collect the screen log information along with command line logs if the command fails and escalate it to Cisco TAC.
- Ensure that only Cisco TAC runs the command.
- Run the command on the server with obsolete data as the synchronization process deletes the data that clashes with the information on the other server.

Note You should run this command on the server that has obsolete data in a Unity Connection cluster.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc dbreplication 03_define_db_template

This command creates the replication record of the set of tables in Unity Connection databases for replication synchronization. This command also negotiates the table templates of Unity Connection database on which the replication scheme needs to be established.

utils cuc dbreplication 03_define_db_template

Command Modes

Administrator (admin:)

Usage Guidelines

This command lists all the tables and defines templates on basis of which the data is negotiated and synchronized between the two servers in a Unity Connection cluster.

Note It is recommended to :

- Take the system backup before running the command.
- Collect the screen log information along with command line logs if the command fails and escalate it to Cisco TAC.
- Ensure that only Cisco TAC runs the command.
- Run the command on the server with obsolete data as the synchronization process deletes the data that clashes with the information on the other server.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc dbreplication 04_sync_database

This command synchronizes the database from the remote server to the server on which the command is executed.

utils cuc dbreplication 04_sync_database

Command Modes

Administrator (admin:)

Usage Guidelines

You should run this command on the server that has obsolete data in a Unity Connection cluster to copy the recent data from the remote server on the current server.

Note It is recommended to :

- Take the system backup before running the command.
- Collect the screen log information along with command line logs if the command fails and escalate it to Cisco TAC.
- Ensure that only Cisco TAC runs the command.
- Run the command on the server with obsolete data as the synchronization process deletes the data that clashes with the information on the other server.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc dbreplication reset_all

This command performs all the tasks, such as tear down and defining servers required to reset database replication between the two servers in a Unity Connection cluster.

utils cuc dbreplication reset_all

Command Modes

Administrator (admin:)

Usage Guidelines

This command executes the following commands sequentially to successfully reset database replication between the two servers in a Unity Connection cluster:

- utils cuc dbreplication01_tear_down

- utils cuc dbreplication 02_define_servers
- utils cuc dbreplication 03_define_db_template
- utils cuc dbreplication 04_sync_database

Note It is recommended to :

- Take the system backup before running the command.
- Collect the screen log information along with command line logs if the command fails and escalate it to Cisco TAC.
- Ensure that only Cisco TAC runs the command.
- Run the command on the server with obsolete data as the synchronization process deletes the data that clashes with the information on the other server.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc encryption

This command enables, disables and provides the status of the encryption on Cisco Unity Connection.

utils cuc encryption { enable | disable | status }

Syntex Description

Parameters	Description
enable	Enables the encryption on Unity Connection. When enabled, Unity connection allows you to use the security features.
disable	Disables the encryption on Unity Connection. When disabled, you can not use the security features in Unity Connection.
status	Displays the encryption status of the Unity Connection.

Usage Guidelines

When you enable the encryption on Unity Connection, make sure the following:

- The Cisco Unity Connection is registered with Cisco Smart Software Manager (CSSM) or Cisco Smart Software Manager satellite.
- Export Control Functionality is enabled for the product.

For more information on how to register and enable the Export Control Functionality for Cisco Unity Connection, see " Configuring Cisco Smart Software Licensing in Unity Connection" section of "Managing Licenses" chapter of *Install, Upgrade and Maintenance Guide for Cisco Unity Connection Release 12.x* available at "https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/install_upgrade/guide/b_12xcuciumg.html".

Note In case of cluster, the CLI is executed only on publisher server.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Cisco Unity Connection

Example

```
admin:utils cuc encryption enable
After successful execution, restart the following services on all nodes in the cluster

1.Connection Conversation Manager
2.Connection IMAP Server

Do you want to proceed (yes/no)? yes
Encryption enabled successfully
```

utils cuc jetty ssl disable

This command allows you to set the status of SSL (Disabled) on the Jetty Server for notifications.

utils cuc jetty ssl disable

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

```
admin: utils cuc jetty ssl disable

After successful execution of this command restart of Jetty server is required, which will
 result in loss of current event subscriptions. Are you sure?
Enter (yes/no)? yes

Command completed successfully.
Please restart Connection Jetty Service.
In case of cluster, run this command on the other node also.
```

utils cuc jetty ssl enable

This command allows you to enable the SSL on the Jetty Server for notifications.

utils cuc jetty ssl enable

Usage Guidelines

When you enable the SSL on the Jetty server, make sure the following:

- You are using the Restricted version of Cisco Unity Connection.
- The encryption is enabled on the Cisco Unity Connection.

Note In Evaluation Mode, you are not allowed to run the CLI command.

For more information, see "Cisco Unity Connection- Restricted and Unrestricted Version" chapter of Security Guide for Cisco Unity Connection Release 12.x available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/security/b_12xcucsecx.html.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

```
admin: utils cuc jetty ssl enable

After successful execution of this command restart of Jetty server is required, which will
 result in loss of current event subscriptions. Are you sure?
Enter (yes/no)? yes

Command completed successfully.
Please restart Connection Jetty Service.
In case of cluster, run this command on the other node also.
```

utils cuc networking clear_replication

This command stops all Digital Networking replication activities on the server.

utils cuc networking clear_replication

Command Modes

Administrator (admin:)

Usage Guidelines

This command stops the Connection Digital Networking Replication Agent and Connection SMTP service, deletes the drop, queue, and pickup replication folders, clears the status of in-progress directory pushes to or

pulls from this server, and restarts the Connection Digital Networking Replication Agent and Connection SMTP service. Depending on the size of the replication folders, this operation may take several minutes.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc networking dscp

This command causes Connection either to start or to stop including a DSCP value of 18 in packets sent between the Connection servers in a cluster, so a router configured to prioritize packets based on their DSCP value can prioritize Connection data and voice messages.

utils cuc networking dscp on | off

Syntax Description

Parameters	Description
on	Causes Connection to start including a DSCP value of 18 packets sent over the network.
off	Causes to stop including a DSCP value of 18 in packets sent over the network. 18 is the default value.

Command Modes

Administrator (admin:)

Usage Guidelines

This command makes the DSCP value available in the packets being passed between the Connection servers in a cluster. For the information to be used, you must configure the router. The command lets you control whether a DSCP value is included in outgoing packets, but you can not change the value.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection only

utils cuc reset password

This command resets the password for a specified user account. If Connection locked the account because of too many failed sign-in attempts, this command also unlocks the account.

utils cuc reset password

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection only

Example

```
admin: utils cuc reset password jdoe
Enter password:
Re-enter password:
jdoe
07/29/2008 12:41:14.704 : Update SUCCESSED
```

utilscucsetPinExpiry_PromptTime“AuthenticationRuleName”

This Command enables the Cisco Unity Connection telephone user interface (touchtone conversation) PIN feature and allows you to update the time interval during when the conditional expiry warning prompt will be played.

Requirements

If the value is set to:

- 0: disabled
- 1: enabled
    - Enter the time interval

For more information on utilscuc set PinExpiry_PromptTime "Authentication Rule Name" CLI command, see the Cisco Unity Connection telephone user interface (touchtone conversation) PIN section in Release Notes for Cisco Unity Connection 10.0(1).

utils dbreplication dropadmindb

This command drops the Informix syscdr database on any server in the cluster.

utils dbreplication dropadmindb

Command Modes

Administrator (admin:)

Usage Guidelines

You should run this command only if database replication reset or cluster reset fails and replication cannot be restarted.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication forcedatasyncsub

This command forces a subscriber server to have its data restored from data on the publisher server.

utils dbreplication forcedatasyncsub *nodename* [**offloadpub**] [*timeoutvalue*]

Syntax Description

Parameters	Description
nodename	Specifies a particular subscriber server to have its data restored from data on the publisher server. Enter **`all`** to restore data on all subscriber servers.
offloadpub	Minimizes the usage of the publisher server during the forcedatasyncsub process. **Note** Adding this option increases the time taken for forcedatasyncsub to finish
timeoutvalue	Specifies the recovery timeout value for each node in minutes (should be greater than the default timeout). Default: 40 minutes.

Command Modes

Administrator (admin:)

Usage Guidelines

Use this command only after you have run the **utils dbreplication repair** command several times, but the utils dbreplication status command still shows non-dynamic tables that are not in sync

Note Do not run this command if only dynamic tables are out of sync; dynamic tables can be out of sync during normal system operation.

You can only run this command from the publisher server. Enter **all** to force sync on all subscriber servers in the cluster. If only one subscriber server is out of sync, use the *nodename* parameter.

Note This command erases all existing data on the subscriber server and replaces it with the database from the publisher server. This erasure makes it impossible to determine the root cause for the subscriber server tables going out of sync.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication quickaudit

This command runs a quick database check on selected content on dynamic tables.

utils dbreplication quickaudit *nodename* | **all**

Syntax Description

Parameters	Description
nodename	Specifies the node on which the quick audit should be run.
all	Causes the audit to be run on all nodes

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication rebuild

This command is used to set up database replication across the cluster and runs the following commands on the specified nodes:

- **utils dbreplication stop**
- **utils dbreplication dropadmindb** or **dropadmindbforce**
- **utils dbreplication reset**

utils dbreplication rebuild [*nodename*] | **all**

Syntax Description

Parameters	Description
nodename	Specifies the node or nodes on which database replication will be rebuilt.
all	Specifies that database replication will be rebuilt on all nodes in the cluster.

Command Modes

Administrator (admin:)

Usage Guidelines

Caution This command can affect performance of other nodes in your cluster. We recommend that you run this command during a system maintenance window.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication repair

This command repairs database replication.

utils dbreplication repair *nodename* | **all**

Syntax Description

Parameters	Description
nodename	Specifies a particular subscriber server for data repair.
all	Causes data repair to take place on all subscriber servers.

Command Modes

Administrator (admin:)

Usage Guidelines

If the command **utils dbreplication status** shows that servers are connected but one or more tables have data that is out of sync, the **utils dbreplication repair** repairs the data on the subscriber servers so that the data is in sync with the data on the publisher server.

Specify **all** to repair all nodes in the cluster, or if only one subscriber server is out of sync, specify the *nodename* parameter.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication repairreplicate

This command repairs mismatched data between cluster nodes and changes the node data to match the publisher data.

utils dbreplication repairreplicate *replicatename* [*nodename* | **all**]

Syntax Description

Parameters	Description
replicatename	Specifies the replicate to repair.
nodename	Specifies the node on which to repair replication.

Parameters	Description
all	Specifies to fix replication on all nodes.

Command Modes

Administrator (admin:)

Usage Guidelines

The parameter *nodename* may not specify the publisher; any subscriber node name is acceptable.

Note This command can be executed on the publisher.

Note This command does not repair replication setup

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication repairtable

This command repairs mismatched data between cluster nodes and changes the node to match the publisher data.

utils dbreplication repairtable *tablename* [*nodename* | **all**]

Syntax Description

Parameters	Description
tablename	Specifies the table to repair
nodename	Specifies the node on which to repair replication.
all	Specifies to fix replication on all nodes.

Command Modes

Administrator (admin:)

Usage Guidelines

Note This command does not repair replication setup.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication reset

This command resets and restarts database replication. You can use this command to rebuild replication when the system has not set up replication properly.

utils dbreplication reset *nodename* | **all**

Syntax Description

Parameters	Description
nodename	Specifies a particular subscriber server to on which to have replication rebuilt.
all	Specifies that all subscriber servers in the cluster have replication rebuilt.

Command Modes

Administrator (admin:)

Usage Guidelines

This command is the best option to use when servers show an RTMT state of 4. If only one subscriber server shows an RTMT state of 4, you may reset that server by specifying the *hostname* parameter. To reset the entire cluster, use the **all** parameter.

Tip Before you run this command, first run the command **utils dbreplication stop** on all subscriber servers that are reset and then on the publisher server.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication runtimestate

This command monitors progress of the database replication process and provides replication state in the cluster.

utils dbreplication runtimestate *nodename*

Syntax Description

Parameters	Description
nodename	Specifies the node to monitor.

Command Modes

Administrator (admin:)

Usage Guidelines

If you provide a node name, the system provides the replication state from the context of the selected node.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication setprocess

This command improves replication performance of clusters that have nodes separated by WANs with delay (Clustering over WAN configuration).

utils dbreplication setprocess [*process*]

Syntax Description

Parameters	Description
process	The new database replication . Ensure that the value is between 1 and 40. Default value: 1

Command Modes

Administrator (admin:)

Usage Guidelines

Caution Setting the PROCESS option to near maximum consumes more system resources.

Changes made to this setting after an upgrade but before the switch-over to the new version will need to be manually re-applied.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils dbreplication setrepltimeout

This command sets the timeout for database replication on large clusters.

utils dbreplication setrepltimeout *timeout*

Syntax Description

Parameters	Description
timeout	The new database replication timeout, in seconds. Ensure that the value is between 300 and 3600. Default value: 300 (5 minutes)

Command Modes

Administrator (admin:)

Usage Guidelines

After the first subscriber server requests replication with the publisher server, the system sets this timer. After the timer expires, the first subscriber server, plus all other subscriber servers that requested replication within that time period, begin data replication with the publisher server in a batch. If you have several subscriber servers, batch replication is more efficient than individual server replication. For large clusters, you can use the command to increase the default timeout value, so that more subscriber servers are included in the batch.

Tip Cisco recommends that you restore this value back to the default of 300 (5 minutes) after you finish upgrading the entire cluster, and the subscriber servers have successfully set up replication.

Note After you upgrade the publisher server and restart it on the upgraded partition, you should set this timer value before you switch the first subscriber server to the new release. After the first subscriber server requests replication, the publisher server sets the replication timer based on the new value.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication status

This command shows the status of database replication and indicates whether the servers in the cluster are connected and the data is in sync.

utils dbreplication status all | node | replicate

Syntax Description

Parameters	Description
all	Specifies to show the status of all servers.
node	Specifies the node for which to show status.
replicate	Specifies the replicate for which to show status.

Command Modes

Administrator (admin:)

Usage Guidelines

Note You should run this command only on the first node (publisher server) of a cluster.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication stop

This command stops the automatic setup of database replication. Run this command on subscriber and publisher servers before executing the CLI command **utils dbreplication reset**. You can run this command on the subscriber servers simultaneously, before you run it on the publisher server.

utils dbreplication stop *nodename* | **all**

Syntax Description

Parameters	Description
nodename	Specifies the name of the node on which to stop the automatic setup of database replication.
all	Stops database replication on all nodes.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils imdb_replication replication status

This command validates that In Memory Database (IMDB) replication between the node pairs in each subcluster of the deployment has run correctly.

The command performs writes and reads on IMDB tables in each relevant Datastore using a utility from the calling IM and Presence Service node.

```
utils imdb_replication status
```

Command Modes

Administrator (admin:)

Usage Guidelines

For the utility to run successfully, ports 6603, 6604, and 6605 must be opened on any firewalls that are configured between the nodes on the IM and Presence Service clusters.

This is not required for the normal operation of the IMDB.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: IM and Presence Service

utils diagnose

This command enables you to diagnose and attempt to automatically fix system problems.

utils diagnose **fix** | **list** | **test** | **version** *[module_name]*

Syntax Description

Parameters	Description
fix	Runs all diagnostic commands and attempts to fix problems.
hcs	Lists all the diagnostic commands available for HCS services.
list	Lists all available diagnostic commands.
module	Runs a single diagnostic command or group of commands and attempts to fix problems.
test	Runs all diagnostic commands but does not attempt to fix problems.
version	Displays the diagnostic framework version.
module_name	Specifies the name of a diagnostics module.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0 for **version** and 1 for all other parameters

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery backup network

Displays information about the backup files that are stored on a remote server.

utils disaster_recovery backup network [*featurelist*][*path*][*servername*][*username*]

Syntax Description

Parameters	Description
[*featurelist*]	Specifies a list of features to back up, separated by commas.
[*path*]	Represents the location of the backup files on the remote server.
[*servername*]	Represents the IP address or hostname of the server where you stored the backup files.
[*username*]	Represents the username that is needed to log in to the remote server.

Command Modes

Administrator (admin:)

Usage Guidelines

The system prompts you to enter the password for the account on the remote server.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery cancel_backup

This command cancels the ongoing backup.

utils disaster_recovery cancel_backup [*confirm*]

Command Modes

Administrator (admin:)

Usage Guidelines

After you enter the command, you must confirm that you want to cancel the backup. Enter **Y** to cancel the backup or any other key to continue the backup.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

Example

```
admin: utils disaster_recovery cancel_backup yes
Cancelling backup...
Backup cancelled successfully.
```

utils disaster_recovery device add network

This command adds the backup network device.

utils disaster_recovery device add network *devicename* *path* *server_namei/ip_address* *username* [*Number_of_backups*]

Syntax Description

Parameters	Description
devicename	Specifies the name of the backup device to be added (mandatory).
path	Specifies the path to retrieve the backup device (mandatory).
server_name/ip_address	Specifies the hostname or IP address of the server where the backup file is stored (mandatory).
username	Specifies the userid required to connect to the remote machine (mandatory).
[*Number_of_backups*]	Specifies the number of backups to store on the Network Directory (default 2). This parameter is optional.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

Example

```
admin: utils disaster_recovery device add network networkDevice /root 10.77.31.116 root 3
```

utils disaster_recovery device delete

This command deletes the specified device.

utils disaster_recovery device delete
*device_name**

Syntax Description

Parameters	Description
device_name	Name of the device to be deleted.
*	Deletes all existing devices except for the ones associated to a schedule.

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery device list

Displays the device name, device type, and device path for all the backup devices.

utils disaster_recovery device list

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery estimate_tar_size

This command provides the estimated size of last successful backup from SFTP or local device.

utils disaster_recovery estimate_tar_size utils disaster_recovery device list

Syntax Description

Parameters	Description
featurelist	Specifies a list of features to back up, separated by commas.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery history

This command displays the history of previous backups and restores.

utils disaster_recovery history [*operation*]

Syntax Description

Parameters	Description
operation	Specifies backup or restore.

Command Modes

Administrator (admin:)

Requirements

Command privilege level:

Allowed during upgrade:

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

Example

```
admin: utils disaster_recovery history backup
Tar Filename: Backup Device: Completed On: Result: Backup Type: Features Backed Up:
2009-10-30-14-53-32.tar TAPE Fri Oct 30 14:55:31 CDT 2009 ERROR MANUAL
2009-12-10-10-30-17.tar TAPE Thu Dec 10 10:35:22 CST 2009 SUCCESS MANUAL CDR_CAR,CCM
```

utils disaster_recovery jschLogs operation

This command enables and disables the detailed JSch logging.

utils disaster_recovery jschLogs operation [*operation*]

Syntax Description

Parameters	Description
operation	Specifies the name of operation—enable or disable.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery prepare restore pub_from_sub

This command handles the tasks to prepare for restore of a publisher node from a subscriber node.

Note This command is applicable only when a publisher node is rebuilt and restored from the subscriber node database. A specific procedure is used for restore instead of restoring the data from the remote backup source. After a publisher node is rebuilt, you must use this command prior to the insertion of process node information.

utils disaster_recovery prepare restore pub_from_sub

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery restore network

This command restores a remote server. You must restore the Unified Communications Manager publisher node before you restore subscriber nodes in the same cluster. If you are restoring IM and Presence Service nodes, you must restore the database publisher node before you restore subscriber nodes in the same cluster.

utils disaster_recovery restore network *restore_server* *tarfilename* *devicename*

Syntax Description

Parameters	Description
restore_server	Specifies the hostname of the remote server that you want to restore.
tarfilename	Specifies the name of the file to restore.
devicename	Specifies the name of the device on which to restore files.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery schedule add

This command adds the configured schedules.

utils disaster_recovery schedule add *schedulename* *devicename* *featurelist* *datetime* *frequency*

Syntax Description

Parameters	Description
schedulename	Represents the name of the scheduler (mandatory).
devicename	Represents the name of the device for which scheduling is done (mandatory).
featurelist	Represents the comma-separated feature list to back up (mandatory).
datetime	Represents the date when the scheduler is set (mandatory). Format specified (yyyy/mm/dd-hh:mm) 24-hr clock.
frequency	Represents the frequency at which the schedule is set to take a backup. Examples: once, daily, weekly and monthly.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery schedule

This command enables or disables the specified schedule.

utils disaster_recovery schedule **enable** | **disable** [*schedulename*]

Syntax Description

Parameters	Description
enable	Enables the specified schedule.
disable	Disables the specified schedule.

Parameters	Description
schedulename	Represents the name of the scheduler.

Command Modes

Administrator (admin:)

Requirements

Command privilege level:1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

Example

```
admin: utils disaster_recovery schedule enable schedule1
Schedule enabled successfully.
```

utils disaster_recovery schedule delete

This command deletes the configured schedules.

utils disaster_recovery schedule delete *schedulename*

Syntax Description

Parameters	Description
schedulename	Represents the name of the schedule that is to be deleted.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery schedule disable

This command disables the configured schedules.

utils disaster_recovery schedule disable *schedulename*

Syntax Description

Parameters	Description
schedulename	Represents the name of the schedule that is to be disabled.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery schedule list

Displays the schedules that are configured.

utils disaster_recovery schedule list

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

Example

```
admin: utils disaster_recovery schedule list
schedule name device name Schedule Status
----------------------------------------
schedule1      device 1     enabled
schedule2      device 2     disabled
```

utils disaster_recovery show_backupfiles

This command retrieves the information of backup files, which are available at storage location.

utils disaster_recovery show_backupfiles *devicename*

Syntax Description

Parameters	Description
devicename	Represents the name of the device to show backup files at the storage location.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery show_registration

This command displays the registered features and components on the specified server.

utils disaster_recovery show_registration *hostname*

Syntax Description

Parameters	Description
hostname	Specifies the server for which you want to display registration information.

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery status

This command displays the status of the current backup or restore job.

utils disaster_recovery status *operation*

Syntax Description

Parameters	Description
operation	Specifies the name of the ongoing operation: backup or restore.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils EnhancedSecurityMode disable

The command disables the EnhancedSecurityMode mode on the system. The system reboots after this mode is disabled.

utils EnhancedSecurityMode disable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils EnhancedSecurityMode enable

The command enables the EnhancedSecurityMode mode on the system. The system reboots after this mode is enabled.

utils EnhancedSecurityMode enable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils EnhancedSecurityMode status

The command displays whether the system is operating in EnhancedSecurityMode or non-EnhancedSecurityMode mode.

utils EnhancedSecurityMode status

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils filebeat config

The command configures the Logstash server details for downloading the information.

utils filebeat configIP addressport numberlog type

Syntax Description

Parameters	Description
IP address	Enter the IP address of the Logstash server.
port number	Enter the port number of Logstash server.
log type	Enter the log type that you have to uploaded to the Logstash server.

You can also secure the FileBeat sevice by enabling TLS. The following prompt is displayed after setting the parameters.

```
Do you wish to secure the filebeat service by enabling TLS?

Enter (yes/no) ?
```

Enter **Yes** to enable TLS.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils filebeat disable

The command disables the filebeat configuration on the system.

utils filebeat disable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils filebeat enable

The command enables the filebeat configuration on the system.

utils filebeat disable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils filebeat status

The command shows whether the filebeat is running or not and its configuration values.

utils filebeat status

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils filebeat tls

This command configures Transport Layer Security (TLS) 1.2 as the protocol for communication between the FileBeat client and the logstash server. This enables a secure connection between the FileBeat client and the logstash server, which is a requirement for compliance to Common Criteria guidelines.

In Common Criteria Mode, strict host name verification is implemented. Hence, it is required to configure the server with a fully qualified domain name (FQDN) which matches the certificate.

utils filebeat tls enable | **disable** | **status**

Syntax Description

Parameters	Description
enable	Enables a secure connection between the FileBeat client and the logstash server.
disable	Disables the TLS for FileBeat client.
status	Displays the status for TLS.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

A security certificate has to be uploaded from logstash server to the tomcat trust store on Unified Communications Manager and IM and Presence service.

utils fior

This command allows you to monitor the I/O on the server. The File I/O Reporting service provides a kernel-base daemon for collecting file I/O per process.

utils fior

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior disable

This command disables I/O statistics monitoring and deletes all the monitoring data collected on the system. Use this command to disable monitoring and free up disk space that is used by the monitoring data.

utils fior disable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior enable

This command enables I/O statistics monitoring.

Note Use this command before monitoring begins.

utils fior enable

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior list

This command displays a list of the I/O events for all processes.

utils fior list

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior start

This command starts the I/O statistics utility monitoring and data collection. After the monitoring starts, the I/O statistics data is collected in the platform logs. This data can range up to 25 MB per day. Data is rotated after 7 days of data collection. This data is deleted after you disable the I/O statistics utility monitoring.

Note Enable the I/O statistics utility monitoring begins before the monitoring begins.

utils fior start

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior status

This command provides the status of the I/O statistics monitoring utility.

utils fior status

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior stop

This command stops the I/O statistics monitoring and data collection. However, this command does not delete the collected data.

Note If I/O statistics are no longer needed, disable the cleanup of the monitoring data from the platform logs.

utils fior stop

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior top

This command displays a list of I/O statistics for I/O bound processes at the time that you run this command.

utils fior top

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fips

Caution FIPS mode is only supported on releases that have been through FIPS compliance. Be warned that FIPS mode should be disabled before you upgrade to a non-FIPS compliance version of Unified Communications Manager.

For information about which releases are FIPS compliant and to view their certifications, see the *FIPS 140* document at https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html.

This command enables, disables, or displays the status of FIPS 140-2 mode. FIPS 140-2 mode is disabled by default; only an administrator can enable FIPS.

utils fips enable | disable | status

Syntax Description

Parameters	Description
enable	Activates FIPS 140-2 mode.
disable	Deactivates FIPS 140-2 mode.
status	Displays the status of FIPS 140-2 mode.

Command Modes

Administrator (admin:)

Usage Guidelines

Before enabling FIPS mode, we 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.

Consider the following information before you enable FIPS 140-2 mode:

- When you switch from non-FIPS to FIPS mode, the MD5 and DES protocols will not be functional.
- 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.
- In FIPS mode, the IM and Presence service uses Red Hat 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 asks you to redefine the security policies with FIPS approved functions and abort.

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

Consider the following information before you disable FIPS 140-2 mode: In multiple server clusters, each server must be disabled separately; FIPS mode is not disabled cluster-wide but on a per server basis.

Consider the following information after you enable FIPS 140-2 mode: If you have a single server cluster and chose to apply "Prepare Cluster for Rolback to pre 8.0" enterprise parameter before enabling FIPS mode, disable this parameter after making sure that all the phones registered successfully with the server.

Consider the following information before you enable or disable FIPS 140-2 mode for IM and Presence Service: After you enable or disable FIPS 140-2 mode for IM and Presence Service, the Tomcat certificate is regenerated and the node reboots. The Intercluster Sync Agent syncs the new Tomcat certificate across the cluster; this can take up to 30 minutes. Until the new Tomcat certificate is synced across the cluster, an IM and Presence Servicee subscriber node cannot access information from the IM and Presence Service database publisher node. For example, a user who is logged into the Cisco Unified Serviceability GUI on a subscriber node will not be able to view services on theIM and Presence Service database publisher node. Users will see the following error message until the sync is complete: `Connection to server cannot be established (certificate exception)`

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

utils fips_common_criteria

This command configures the Common Criteria mode in the system.

utils fips_common_criteria enable | disable | status

Syntax Description

Parameters	Description
enable	Enables the Common Criteria mode in the system
disable	Disables the Common Criteria mode in the system When Common Criteria mode is disabled, a prompt is displayed to set the minimum TLS version.

Parameters	Description
status	Displays the status of Common Criteria mode in the system

Command Modes

Administrator (admin:)

Usage Guidelines

Secure connections using TLS version 1.0 are not permitted after enabling the Common Criteria mode. FIPS mode will be enabled while enabling Common Criteria mode. Enabling or disabling Common Criteria mode does not require certificates to be regenerated. However, enabling or disabling FIPS does require rebooting of the system along with regeneration of certificates.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and IM and Presence Service

Note This CLI command is not applicable to Cisco Unity Connection.

utils firewall ipv4 debug

This command turns IPv4 firewall debugging on or off. If you do not enter a time parameter, this command turns on debugging for 5 minutes.

utils firewall ipv4 debug off[*time*]

Syntax Description

Parameters	Description
off	Turns off the IPv4 firewall debugging. If you do not enter the time parameter, this command disables the firewall for 5 minutes.
time	(Optional) Sets the duration for which the firewall debugging is to be enabled in the following formats: • Minutes: 0–1440m • Hours: 0–23h • Hours and minutes: 0–23h 0–60m

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils firewall ipv4

This commands enables and disables IPv4 firewall.

utils firewall ipv4 enable | **disable***[time]*

Syntax Description

Parameters	Description
enable	Turns on the IPv4 firewall.
disable	Turns off the IPv4 firewall. If you do not enter the time parameter, this command disables the firewall for 5 minutes.
time	(Optional) Sets the duration for which the firewall is to be disabled in the following formats: • Minutes: 0–1440m • Hours: 0–23h • Hours and minutes: 0–23h 0–60m

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils firewall ipv4 list

This commands displays the current configuration of the IPv4 firewall.

utils firewall ipv4 list

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils firewall ipv4 status

This command displays the current status of the IPv4 firewall.

utils firewall ipv4 status

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils firewall ipv6 debug

This command turns IPv6 firewall debugging on for the configured time period. The default value of time period is 5 minutes.

utils ipv6 firewall debug off[*time*]

Syntax Description

Parameters	Description
off	(Optional) Turns off the IPv6 firewall debugging. If you do not enter the time parameter, this command disables the firewall as per the default time period value.
time	(Optional) Sets the duration for which the firewall debugging is to be enabled in the following formats: • Minutes: 0–1440m • Hours: 0–23h • Hours and minutes: 0–23h 0–60m

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, and Cisco Unity Connection.

utils firewall ipv6

This commands enables and disables IPv6 firewall.

utils firewall ipv6 enable | **disable***[time]*

Syntax Description

Parameters	Description
enable	Turns on the IPv6 firewall.
disable	Turns off the IPv6 firewall. If you do not enter the time parameter, this command disables the firewall for 5 minutes.
time	(Optional) Sets the duration for which the firewall is to be disabled in the following formats: • Minutes: 0–1440m • Hours: 0–23h • Hours and minutes: 0–23h 0–60m

Command Modes

Administrator (admin:)

Usage Guidelines

You can use this command to enable or disable firewall tables. If you are testing the Unified Communications Manager for compliance with the USGv6 Profile, you must disable the IPv6 firewall tables for a duration of 23 hours before you begin the test.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection.

utils firewall ipv6 list

This commands displays the current configuration of the IPv6 firewall.

utils firewall ipv6 list

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection.

utils firewall ipv6 status

This command displays the current status of the IPv6 firewall.

utils firewall ipv6 status

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection.

utils ha failover

This command initiates a manual failover for a specified node, where the Cisco Server Recovery Manager stops the critical services on the failed node and moves all users to the backup node.

For IM and Presence nodes, the backup node must be another IM and Presence server. Two servers must be assigned to the same presence redundancy group before you specify the backup server. The back-up server you specify is the other server that is assigned to the presence redundancy group.

utils ha failover node name

Syntax Description

Parameters	Description
node name	Specifies the node on which to perform the manual failover.

Command Modes

Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

Failover Example

```
admin: ha failover shorty-cups
Initiate Manual Failover for Node > shorty-cups
Request SUCCESSFUL.
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Taking Over Reason: On Admin Request
Node 2 Name : shorty-cups State: Failover Reason: On Admin Request
```

utils ha fallback

This command initiates a manual fallback for a specified node, where the Cisco Server Recovery Manager restarts the critical services on the active node and moves users back to the active node.

utils ha fallback *node name*

Syntax Description

Parameters	Description
node name	Specifies the node on which to perform a manual fallback.

Command Modes

Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

Fallback Example

```
admin: ha fallback shorty-cups
Initiate Manual fallback for Node >shorty-cups<
Request SUCCESSFUL.
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Falling Back Reason: On Admin Request
Node 2 Name : shorty-cups State: Taking Back Reason: On Admin Request
```

utils ha recover

This command initiates a manual recovery of the presence redundancy group (when nodes are in a Failed state), where IM and Presence restarts the Cisco Server Recovery Manager service in that presence redundancy group.

utils ha recover *presence redundancy group name*

Syntax Description

Parameters	Description
presence redundancy group name	Specifies the presence redundancy group on which to monitor HA status. If no presence redundancy group name is provided, all cluster information is provided.

Command Modes

Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

Recover Example

```
admin: ha recover Defaultcluster
Stopping services... Stopped
Starting services... Started
admin:
```

utils ha status

This command displays the HA status for a specified presence redundancy group.

utils ha status *presence redundancy group name*

Syntax Description

Parameters	Description
presence redundancy group name	Specifies the presence redundancy group for which to monitor HA status. If no presence redundancy group name is provided, all cluster information is displayed.

Command Modes

Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

Status Example with HA Not Enabled

```
admin: ha status
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Unknown Reason: High Availability Not Enabled
Node 2 Name : shorty-cups State: Unknown Reason: High Availability Not Enabled
```

Status Example with HA Enabled

```
admin: ha status
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Normal
Node 2 Name : shorty-cups State: Normal
```

Status Example with a Critical Service Down

```
admin: ha status
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Failed Over with Critical Services not Running Reason:
Critical Service Down
Node 2 Name : shorty-cups State: Running in Backup Mode Reason: Critical Service Down
```

Status Example Failed

```
admin: ha status
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Failed Reason: Critical Service Down
Node 2 Name : shorty-cups State: Failed Reason: Critical Service Down
```

utils ils showpeerinfo

This command returns the peer info vector for either a single cluster in an ILS network, or for all the clusters in an ILS network.

utils ils showpeerinfo *clustername*

Syntax Description

Parameters	Description
clustername	Specifies the fully qualified domain name of the publisher node for a Unified Communications Manager cluster in an ILS network.

Command Modes

Administrator (admin:)

Usage Guidelines

The peer info vector contains information about a cluster in an ILS network. The available information includes clustername, cluster ID and IP addresses for the cluster nodes. If you want information about a specific cluster in an ILS network, enter the *clustername* parameter. If you want information on all the clusters in the network, leave the *clustername* parameter empty

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager

utils import config

This command takes data from the platformConfig.xml file on the virtual floppy drive and modifies the system to match the configuration file. The system reboots after the command successfully completes.

utils import config

Command Modes

Administrator (admin:)

Usage Guidelines

This command can be executed on any VMware deployment.

1. Power on the VMware.
2. Use the Answer File Generator (AFG) tool (http://www.cisco.com/web/cuc_afg/index.html) to create a platformConfig.xml file.

3. Insert the Config.xml file into a virtual floppy instance (see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1739for directions).
4. Mount the .flp file in the floppy drive of the new VMware.
5. Sign in to the CLI of the VM (with console or SSH) and execute the **utils import config** command.

   The command cycles through all of the data found in the xml file and if data is found that is different than what is currently set on the VM, it modifies the VM to match the new data.
6. The system reboots with the new identity.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Execute utils import config in Vmware Deployment

Procedure

utils iostat

This command displays the iostat output for the given number of iterations and intervals.

utils iostat interval | **iterations** | **filename**

Syntax Description

Parameters	Description
interval	Sets the seconds between two iostat readings. You must set this value if you are using the iteration parameter
iterations	Sets the number of iostat iterations. You must set this value if you are using the interval parameter.
filename	Redirects the output to a file.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils iothrottle

This command allows you to manage and monitor IO throttling on the server.

utils iothrottle enable | disable | status

Syntax Description

Parameters	Description
Enable	Enables I/0 throttling enhancements which lowers the impact of upgrades on an active system.
Disable	Disables I/0 throttling enhancements.
Status	Displays the status of I/0 throttling enhancements.

Command Modes

Administrator (admin:)

Usage Guidelines

Disabling I/0 throttling enhancements can adversely affect the system during upgrades.

Requirements

Command privilege level: 1 for **Enable** and **Disable**, 0 for **Status**

utils itl reset

This command is used when endpoints are unable to validate their configuration files.

utils itl reset localkey | remotekey

Syntax Description

localkey	Generates a new ITL file by taking the existing ITL file on the publisher. The command replaces the signature of that ITL file and signs the new ITL file with the ITL recovery key.
remotekey	Generates a new ITL file after importing the PKCS 12 bag that contains the recovery certificate key pair from the remote location. It then signs the newly generated ITL file with the recovery private key. **remotekey** has the following parameters: • IP address or hostname • User ID • ITLRecovery.p12

Command Modes

Administrator (admin:)

Usage Guidelines

Note You must run this command on the Unified Communications Manager publisher node.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager

Example

```
admin:utils itl reset

Name is None


Generating the reset ITL file.....

The reset ITL file was generated successfully

Locating active Tftp servers in the cluster.....

Following is the list of Active tftp servers in the cluster

====================

se032c-94-42

=====================

Number of Active TFTP servers in the cluster : 1

Transferring new reset ITL file to the TFTP server nodes in the cluster.........

Successfully transferred reset ITL to node se032c-94-42
```

utils ldap config

This command configures the system LDAP authentication.

utils ldap config *fqdnipaddr*

Syntax Description

Parameters	Description
fqdn	Configures the system to use an FQDN for LDAP authentication.
ipaddr	Configures the system to use an IP address for LDAP authentication

Command Modes

Administrator (admin:)

Usage Guidelines

- **utils ldap config fqdn**—This command is preferred for LDAP authentication, however, you can only use this command if DNS is configured on the system; if the system is not configured to use DNS, use **utils ldap config ipaddr**.
- **utils ldap config ipaddr**—This command is not preferred and should only be used if the system is not, or can not be, configured to use DNS; if the system is configured to use DNS, use **utils ldap config fqdn**.

Requirements

Command privilege level: 1

Applies to: Unified Communications Manager and Cisco Unity Connection

utils ldap config status

This command displays the utils ldap configuration status.

utils ldap config status

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils managementAgent alarms minpushLevel

If Push Notifications is enabled, run this command to configure the minimum alarm severity for which Unified Communications Manager sends push notifications alarms to the Cisco cloud.

utils managementAgent alarms minpushLevel*severity*

Syntax Description

Parameters	Description
severity	This value represents the minimum alarm severity for which Unified Communications Manager sends Push Notifications alarms to the Cisco cloud. The possible options are: • Critical • Error (this is the default) • Warning • Notice • Information

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager and IM and Presence Service

utils managementAgent alarms pushfrequency

If Push Notifications is enabled, run this command to configure the interval following which Unified Communications Manager sends push notifications alarms to the Cisco cloud.

utils managementAgent alarms pushfrequency*minutes*

Syntax Description

Parameters	Description
minutes	The upload frequency in minutes. This value must be an integer between 5 and 90 with a default of 30 minutes.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager and IM and Presence Service

utils managementAgent alarms pushnow

If Push Notifications is enabled, run this command to send push notifications alarms to the Cisco cloud immediately, without having to wait for the next scheduled upload.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager and IM and Presence Service

utils network arp delete

This command deletes an entry in the Address Resolution Protocol table.

utils network arp delete *host*

Syntax Description

Parameters	Description
host	(Optional) Represents the host name or IP address of the host to delete from the table.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Delete Example

```
admin:utils network arp delete myhost
```

utils network arp set

This command sets an entry in the Address Resolution Protocol table.

utils network arp set *host* *addr*

Syntax Description

Parameters	Description
host	Represents the host name or IP address of the host to add to the table.
addr	Represents the hardware address (MAC) of the host to be added in the format: XX:XX:XX:XX:XX:XX

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Set Example

```
admin:utils network arp set myhost 11:22:33:44:55:66
```

utils network arp list

This command lists the contents of the Address Resolution Protocol table.

utils network arp list host *hostname* [*options*]

Syntax Description

Parameters	Description
host	
hostname	
options	(Optional) page, numeric • Page: Pauses to display the output one page at a time. • Numeric: Shows hosts as dotted IP addresses.

Command Modes

Administrator (admin:)

Usage Guidelines

In the Flags column, C=cached, M=permanent, P=published.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

List example

```
admin:admin: utils network arp listAddress HWtype HWaddress
Flags Mask Iface
sjc21-3f-hsrp.cisco.com ether 00:00:0C:07:AC:71 C
eth0
philly.cisco.com ether 00:D0:B7:85:98:8E C
eth0
Entries: 2 Skipped: 0 Found: 2
```

utils network capture

This command captures IP packets on the specified Ethernet interface.

utils network capture eth0 [*page*] [*numeric*] [**file***fname*] [**count***num*] [**size***bytes*] [**src***addr*] [**dest***addr*] [**port***num*]

Syntax Description

Parameters	Description
eth0	Specifies Ethernet interface 0.
page	(Optional) Displays the output one page at a time. When you use the page or file options, the complete capture of all requested packets must occur before the command completes.
numeric	(Optional) Displays hosts as dotted IP addresses.
file *fname*	(Optional) Outputs the information to a file. The file option saves the information to `platform/cli/fname.cap`. The filename cannot contain the "." character.
count*num*	(Optional) Sets a count of the number of packets to capture. For screen output, the maximum count equals 1000, and, for file output, the maximum count equals 10,000.
size*bytes*	(Optional) Sets the number of bytes of the packet to capture. For screen output, the maximum number of bytes equals 128, for file output, the maximum of bytes can be any number or ALL.
src *addr*	(Optional) Specifies the source address of the packet as a host name or IPV4 address.
dest*addr*	(Optional) Specifies the destination address of the packet as a host name or IPV4 address.
port*num*	(Optional) Specifies the port number of the packet, either source or destination.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils network capture-rotate

This command captures IP packets beyond the 100,000 packet limit of **utils network capture**.

utils network capture-rotate **file***fname* [**size***bytes*] [**sizePerFile***megabytes*] **maxFiles** *num*[**src***addr*] [**dest***addr*] [**port***num*][**host protocol***addr*]

Syntax Description

Parameters	Description
file *fname*	Outputs the information to a file. **Note** The file will be saved in platform/cli/fname. fname should not contain the "." character.
size*bytes*	The number of bytes of the packet to capture. Valid values include any number up to 65535 or ALL. The default is ALL.
sizePerFile *megabytes*	The sizePerFile sets the value for the size of the log files. (Unit is millions of bytes.) The default value of sizePerFile is 25 MB.
maxFiles *num*	the maxFiles indicates the maximum number of log files to be created. The default value of maxFiles is 10.
src *addr*	(Optional) Specifies the source address of the packet as a hostname or IPV4 address.
dest *addr*	(Optional) Specifies the destination address of the packet as a host name or IPV4 address.
port *num*	(Optional) Specifies the port number of the packet, either source or destination.
host *protocol addr*	(Optional) Limits capture to traffic to and from a specific host. Options for *protocol* are IP, arp, rarp, all, and *addr* must be in IPv4 or hostname format. If **host** is used, do not provide **src** or **dest**.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils network connectivity

This command verifies the node network connection to the first node in the cluster (this connection is only valid on a subsequent node) and to a remote node.

utils network connectivity [**reset**] [*hostname/ip address*]

```
utils network connectivity  [hostname/ip address] [port-number] [timeout]
```

Syntax Description

Parameters	Description
connectivity	This command verifies the node network connection to the first node in the cluster. It is also used to check connectivity to a remote node, where there are two mandatory parameters, **hostname/ip address** and **port-number**.
reset	(Optional) Clears previous return codes.
hostname/ip address	• (Optional) Hostname or IP address of cluster node to check network connectivity with the publisher or the first node. • (Mandatory) Hostname or IP address of the host that has to be tested for the TCP connection, to check network connectivity on the remote server.
port-number	(Mandatory) Port number of the host that requires connection test.
timeout	(Optional) Specifies the time in seconds after which port connectivity message is displayed.

Command Modes

Administrator (admin:)

Usage Guidelines

- The **utils network connectivity** ［**reset**］ *[hostname/ip address]* command is used to check the network connectivity to the publisher or the first node.
- The **utils network connectivity** ［**hostname/ip address**］ ［**port-number**］ *[timeout]* command is used to check the network connectivity to a remote server.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils network host

This command resolves a host name to an address or an address to a host name.

utils network host *name* [**server***serv*] [**page**] [**detail**] [**srv**]

Syntax Description

Parameters	Description
name	Represents the host name or IP address that you want to resolve.
serv	(Optional) Specifies an alternate domain name server.
[**page**]	(Optional) Displays the output one screen at a time.
[**detail**]	(Optional) Displays a detailed listing.
[**srv**]	(Optional) Displays DNS SRV records.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils network ipv6 host

This command does an IPv6 host lookup (or IPv6 address lookup) for the specified host name or IPv6 address.

utils network ipv6 host *host_nameipv6_address*

Syntax Description

Parameters	Description
host_name	Specifies the name of the server.
ipv6_address	Specifies the IPv6 address of the server.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection.

utils network ipv6 traceroute

This command to traces an IPv6 address or hostname.

utils network ipv6 traceroute [*ipv6-addresshostname*]

Syntax Description

Parameters	Description
ipv6-address	Specifies IPv6 address that you want to trace.
hostname	Specifies the host name that you want to trace.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection.

utils network ipv6 ping

This command allows you to ping an IPv6 address or hostname.

utils network ipv6 ping *destination* [*count*]

Syntax Description

Parameters	Description
destination	Specifies a valid IPv6 address or host name that you want to ping.
[*count*]	Specifies the number of times to ping the external server. The default count equals 4.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection.

utils network ping

This command allows you to ping another server.

utils network ping *destination* [*count*] [*size*]

Syntax Description

Parameters	Description
destination	Represents the ip address or host name of the server that you want to ping.
[*count*]	Specifies the number of times to ping the external server. The default count is 4.
[*size*]	Specifies the size of ping packets in bytes. The default value is 56.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils network traceroute

This command traces IP packets that are sent to a remote destination.

utils network traceroute [*destination*]

Syntax Description

Parameters	Description
destination	Represents the hostname or IP address of the server to which you want to send a trace.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils network name-service {hosts|services} cache invalidate

This command clears the name service cache.

utils network name-service *{hosts \ services}* [*cache invalidate*]

Syntax Description

Parameters	Description
Hosts	Host services cache
Services	Services service cache

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Consider the following example for flushing/clearing the cache:

```
admin:utils network name-service hosts cache invalidate
admin:
Successful
```

utils ntp auth symmetric-key

utils ntp auth symmetric-key enable | disable | status

This command helps you enable or disable authentication of the selected NTP server. The authentication is based on symmetric keyID and key. The symmetric key is stored in the encrypted format in Unified Communications Manager.

Note Before you run this command, ensure that you know the NTP server keyID and its corresponding key.

Syntax Description

Parameters	Description
enable	Choose one of the NTP servers from the list of available servers and enable it for authentication.
disable	Choose one of the NTP servers from the list of available servers and disable it for authentication.
status	Shows the authentication status of all the listed NTP servers.

Usage Guidelines

The system prompts you to enter the KeyID or Symmetric key for authentication of an NTP server.

Note

- Unified Communications Manager sends Syslog alert messages when the authentication status of an NTP server changes. You can secure the connections to the syslog server with TLS.
- You can configure the NTP server authentication after you install Unified Communications Manager.

Requirements

Command privilege level: Level 1 can execute all commands, Level 0 can execute only status command

Allowed during upgrade: No

Applies to: Unified Communications Manager

Example: utils ntp auth symmetric-key status - View status when NTP authentication is not enabled

```
admin:utils ntp auth symmetric-key status
10.77.32.92 : NTP Authentication is disabled.
10.77.46.203 : NTP Authentication is disabled.

ind assid status conf reach auth condition last_event cnt
=========================================================
 1  8468   963a   yes  yes  none  sys.peer   sys_peer  3
 2  8469   9024   yes  yes  none    reject  reachable  2
```

Example: utils ntp auth symmetric-key enable - Enable NTP authentication

```
admin:utils ntp auth symmetric-key enable
The List of NTP servers Configured:
1. 10.77.32.92
2. 10.77.46.203
q. press q to exit
Enter the selection for which to configure NTP authentication: 1
Please enter the Key ID [1-65534]:
2
Please enter the Symmetric Key of the NTP Server (SHA1):
Restarting NTP
please run the utils ntp auth symmetric-key status to check the status of NTP Authentication
```

Example: utils ntp auth symmetric-key status - View status after NTP authentication is enabled

```
admin:utils ntp auth symmetric-key status
10.77.46.203 : NTP Authentication is disabled.
10.77.32.92 : NTP Authentication is enabled.

ind assid status conf reach auth condition last_event cnt
=========================================================
 1  57733  9044  yes  yes   none   reject   reachable  4
 2  57734  f014  yes  yes   ok     reject   reachable  1
```

Example: utils ntp auth symmetric-key disable - Disable NTP authentication

```
admin:utils ntp auth symmetric-key disable
The List of NTP servers Configured:
0. All
1. 10.77.46.203
2. 10.77.32.92
q. press q to exit
Enter the selection for which to disable NTP authentication: 2
NTP authentication has been disabled on the particular server.
Restarting NTP
```

Example: utils ntp auth symmetric-key status - View status after NTP authentication is disabled

```
10.77.46.203 : NTP Authentication is disabled.
10.77.32.92 : NTP Authentication is disabled.

ind assid status conf reach auth  condition  last_event cnt
```

```
============================================================
 1  42767  9144   yes  yes  none  falsetick  reachable   4
 2  42768  912a   yes  yes  none  falsetick  sys_peer    2
```

Example: utils ntp auth symmetric-key status - View status of NTP authentication

```
admin:utils ntp auth symmetric-key status
10.77.32.92  :  NTP authentication is failed. Please check the NTP authentication Key ID
and Symmetric Key entered is correct. To update, disable and reenable authentication for
this NTP server.
10.77.32.78  :  NTP Authentication is disabled.

ind assid status  conf reach auth condition  last_event cnt
============================================================
  1 31609  c02c   yes    no   bad    reject              2
  2 31610  803a   yes    no  none    reject    sys_peer  3
```

utils ntp server add

The command adds a maximum of five specified NTP servers.

utils ntp server add *s1* [*s1s2s3s4s5*] [**norestart**]

Syntax Description

Parameters	Description
s1...	Specifies the NTP servers.
norestart	Causes the NTP service to not restart after you add the servers.

Command Modes

Administrator (admin:)

Usage Guidelines

If you use **norestart**, an explicit restart of the NTP service is required for the changes to take effect.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager

Example: Attempting to Add Servers with Incorrect Command Line Parameters

```
admin: admin:utils ntp server add s1 s2 s3 s4 s5 s6 s7 s8
Incorrect number of parameters entered for add
usage: utils ntp server add s1 [s2 s3 s4 s5] [norestart]
```

Example: Attempting to Add a Server Using norestart Without Specifying a Server

```
admin: utils ntp server add s1 s2 s3 s4 s5 s6 s7 s8
Incorrect number of parameters entered for add
usage: utils ntp server add s1 [s2 s3 s4 s5] [norestart]
```

Example: Adding servers without norestart

```
admin: utils ntp server add clock1.cisco.com clock2.cisco.com
clock1.cisco.com :  added successfully.
clock2.cisco.com :  added successfully.
Restarting NTP on the server.
```

Example: Adding Servers That Are Already Added, Without norestart

```
admin: utils ntp server add clock1.cisco.com clock2.cisco.com
clock1.cisco.com : [The host has already been added as an NTP server.]
clock2.cisco.com : [The host has already been added as an NTP server.]
```

Example: Adding Server to Self Without norestart

```
admin: utils ntp server add bglr-ccm26
bglr-ccm26 : [This server cannot be added as an NTP server.]
```

Example: Adding Inaccessible Server Without norestart

```
admin: utils ntp server add clock3.cisco.com
clock3.cisco.com : [ Inaccessible NTP server. Not added. ]
```

Example: Adding Servers with norestart

```
admin: utils ntp server add ntp01-syd.cisco.com ntp02-syd.cisco.com clock.cisco.com norestart
ntp01-syd.cisco.com :  added successfully.
ntp02-syd.cisco.com :  added successfully.
clock.cisco.com :  added successfully.
The NTP service will need to be restarted for the changes to take effect.
```

Example: Adding Servers When Five Are Already Configured

```
admin:utils ntp server add clock3.cisco.com
The maximum permissible limit of 5 NTP servers is already configured.
```

utils ntp server delete

This command deletes NTP servers that are configured.

utils ntp server delete

Command Modes

Administrator (admin:)

Usage Guidelines

This command allows you to delete a configured Network Time Protocol (NTP) server or multiple NTP servers. When you choose the server to delete, you are prompted to indicate if you want to restart the NTP service. If you choose no, the NTP service does not get restarted after the server is deleted.

Note It is required to have at least 1 NTP server configured. Therefore, you cannot delete an NTP server if only one is configured. If you select the option to delete all the NTP servers, the NTP servers are deleted in top down order and the last NTP server on the list does not get deleted. The process is similar to the top down order followed during `utils ntp config` or `utils ntp status`

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager

Example: Deleting Servers with Incorrect Command Line Parameters

```
admin: utils ntp server delete clock1.cisco.com clock2.cisco.com
Incorrect number of optional parameters entered for delete
usage: utils ntp server delete
```

Example: Deleting Single Server with NTP Restart

```
admin: utils ntp server delete
1: clock1.cisco.com
2: clock2.cisco.com
3: ntp01-syd.cisco.com
4: ntp02-syd.cisco.com
5: clock.cisco.com
a: all
q: quit

Choice: 1

Restart NTP (y/n): y

clock1.cisco.com will be deleted from the list of configured NTP servers.
Continue (y/n)?y

clock1.cisco.com :  deleted successfully.
Restarting NTP on the server.
```

Example: Deleting All Servers Without NTP Restart

```
admin: utils ntp server delete
1: clock1.cisco.com
2: clock2.cisco.com
3: ntp01-syd.cisco.com
4: ntp02-syd.cisco.com
5: clock.cisco.com
a: all
q: quit

Choice: a

Restart NTP (y/n): n

This will result in all the configured NTP servers being deleted.
Continue (y/n)?y

clock1.cisco.com :  deleted successfully.
clock2.cisco.com :  deleted successfully.
ntp01-syd.cisco.com :  deleted successfully.
ntp02-syd.cisco.com :  deleted successfully.
clock.cisco.com :  [The NTP server was not deleted.  At least one NTP server is required.]
The NTP service will need to be restarted for the changes to take effect.
```

Example: Deleting All Servers When No Servers Are Configured

```
admin: utils ntp server delete
There are no NTP servers configured to delete.
```

utils ntp config

This command displays the current configuration of the NTP client and server.

Note To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node should be NTP v4 (version 4).

utils ntp config

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence server on Unified Communications Manager, Cisco Unity Connection

utils ntp restart

This command restarts the NTP service.

utils ntp restart

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils ntp server list

This command lists all NTP servers.

utils ntp server list

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: IM and Presence server on Unified Communications Manager

utils ntp start

This command starts the NTP service if it is not already running.

Note You can not stop the NTP service from the command line interface. Use this command when the utils ntp status command returns stopped.

utils ntp start

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence server on Unified Communications Manager, and Cisco Unity Connection

utils ntp status

This command displays the current status of NTP.

utils ntp status

Command Modes

Administrator (admin:)

Requirements

Command privilege level:

Allowed during upgrade:

Applies to: IM and Presence service on Unified Communications Manager.

utils os kerneldump

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

utils os kerneldump enable | disable

Command Modes

Administrator (admin:)

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 the **kexec** command to boot into a capture kernel whenever the kernel crashes.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

Example

```
admin: utils os kerneldump enable
***************WARNING******************
Enabling kerneldump requires system reboot
Would you like to boot the machine (y/n):y
kerneldump enable operation succeeded
System going for a reboot
```

utils os kerneldump ssh

This command enables, disables, or displays the status of an external SSH server.

utils os kerneldump ssh enable | disable | status

Syntax Description

Parameters	Description
enable	Configures an external SSH server as a kerneldump server to kernel dumps.
disable	Removes support of the external SSH server that is configured to collect kernel dumps.
status	Indicates whether an external SSH server is configured or not, to collect kernel dumps.

Command Modes

Administrator (admin:)

Usage Guidelines

If external SSH server has the kerneldump service enabled and a kernel crash occurs, the capture kernel dumps the core on the external server that is configured to collect the dump.
Enabling and disabling kerneldump require a system reboot for the changes to come into effect.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

Example

```
admin: utils os kerneldump ssh disable 10.77.31.60
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 provides the status of the kdump service.

utils os kerneldump status

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils os secure

This command is used to specify the level of security provided by selinux.

utils os secure enforce | permissive | status

Syntax Description

Parameters	Description
enforce	
permissive	
status	

Command Modes

Administrator (admin:)

Usage Guidelines

Note that selinux does not handle rate limiting. Rate limiting is handled by ipprefs and ip tables.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: IM and Presence service on Unified Communications Manager

utils os secure dynamic-policies compile

This command generates the selinux policy module and type enforcement that resolves the recorded denials under the dynamic policy.

utils os secure dynamic-policies compile *policy name*

Syntax Description

Parameters	Description
policy name	Type the dynamic policy name under which the compilation of the selinux policy module and type enforcement is done.

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager

utils os secure dynamic-policies list

This command lists all the operating system dynamic policies with their statuses.

utils os secure dynamic-policies list

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager

utils os secure dynamic-policies load

This command loads the selinux policy module for the dynamic policy into selinux. This command applies new rules into selinux that prevent the denials that are recorded under the dynamic policy from reoccurring.

utils os secure dynamic-policies load *policy name*

Syntax Description

Parameters	Description
policy name	Type the dynamic policy name that has a generated selinux policy module, which is not loaded into selinux..

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager

utils os secure dynamic-policies remove

This command deletes all the data for the dynamic policy from the operating system. The data includes unloading the policy module from selinux and deleting the generated policy module, type enforcements, recorded denials, and delta logs.

utils os secure dynamic-policies remove *policy name*

Syntax Description

Parameters	Description
policy name	Type the dynamic policy name that is unnecessary or no longer required.

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager

utils os secure dynamic-policies show

This command displays the rules to be introduced by loading the generated selinux policy module of the dynamic policy. Run this command after the successful compilation to verify that the rules to be loaded are secure.

utils os secure dynamic-policies show *policy name*

Syntax Description

Parameters	Description
policy name	Type the dynamic policy name for which you want to view the rules.

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager

utils os secure dynamic-policies start-recording

This command starts recording the selinux denials and organizes them under the new dynamic policy.

Note

- This command sets the system into the permissive mode.
- The dynamic-policies are generated on a per-node basis. As a restriction, these policies cannot be exported or imported. This restriction has the following advantages:
  - Prevent loading external and unsigned policy modules into selinux that may create security vulnerabilities.
  - Prevent the transfer of policy modules between Unified Communications Manager clusters with different configurations.

utils os secure dynamic-policies start-recording *policy name*

Syntax Description

Parameters	Description
policy name	Type the dynamic policy name where the selinux denials and future policy data is to be organized.

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager

utils os secure dynamic-policies stop-recording

This command stops recording the selinux denials for the dynamic policy. This command switches the system back to the original enforcement mode—either permissive mode or enforcing mode. This log generates a delta log for all selinux denials that occurred between the start of the recording till it ends.

Note This command fails if the delta log has no new denials. Then, the dynamic policy is purged and you will have to use this command again.

utils os secure dynamic-policies stop-recording *policy name*

Syntax Description

Parameters	Description
policy name	Type the dynamic policy name the recording of which you want to stop.

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager

utils PlatformWebAccess disable

Use this command to restrict the user sign-in to Cisco OS Administration and Disaster Recovery System applications when SSO is enabled.

utils PlatformWebAccess disable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils PlatformWebAccess enable

Use this command to enable the user sign-in to Cisco OS Administration and Disaster Recovery System applications.

utils PlatformWebAccess enable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils PlatformWebAccess status

Use this command to display the status of the web access of the system—whether the platform web access is enabled or disabled for Cisco OS Administration and Disaster Recovery System applications.

utils PlatformWebAccess status

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils processCoreDumps disable

This command disables the process core dumps.

utils processCoreDumps disable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils processCoreDumps enable

This command enables the process core dumps.

utils processCoreDumps enable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils processCoreDumps status

This command provides the status of the kdump service.

utils processCoreDumps status

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils remote_account create

This command creates a remote account.

utils remote_account create

Command Modes

Administrator (admin:)

Usage Guidelines

A remote account generates a pass phrase that allows Cisco Systems support personnel to get access to the system for the specified life of the account.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils remote_account disable

This command allows you to disable a remote account.

utils remote_account disable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils remote_account enable

This command allows you to enable a remote account.

utils remote_account enable

Command Modes

Administrator (admin:)

Usage Guidelines

You can have only one remote account that is enabled at a time.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils remote_account status

This command allows you to check the status of a remote account.

utils remote_account status

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils remotesyslog set protocol tcp

This command configures the protocol for communication with remote syslog server as TCP on the system. Restart the node for changes to take effect.

utils remotesyslog set protocol tcp

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils remotesyslog set protocol udp

This command configures the protocol for communication with remote syslog server as UDP on the system. Restart the node for changes to take effect.

utils remotesyslog set protocol udp

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils remotesyslog set protocol tls

This command configures the protocol for communication with remote syslog server as Transport Layer Security (TLS) 1.2 on the system. TLS 1.2 enables Unified Communications Manager and IM and Presence Service to establish a secure connection with syslog servers. This enables Unified Communications Manager and IM and Presence Service to comply with Common Criteria guidelines.

Note

- Ensure that the syslog server supports TLS 1.2 protocol as a secure connection will be established only if the syslog server supports TLS 1.2 protocol.
- In Common Criteria Mode, strict host name verification is implemented. Hence, it is required to configure the server with a fully qualified domain name (FQDN) which matches the certificate.

Restart the node for changes to take effect.

utils remotesyslog set protocol tls

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

A security certificate has to be uploaded from the syslog server to the tomcat trust store on Unified Communications Manager and IM and Presence service.

utils remotesyslog show protocol

This command shows whether the protocol for communication with remote syslog server is TCP or UDP on the system.

utils remotesyslog show protocol

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils reset_application_ui_administrator_name

This command resets the application user interface administrator name.

utils reset_application_ui_administrator_name

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

utils reset_application_ui_administrator_password

This command resets the application user interface administrator password.

Note For password changes on IM and Presence nodes, stop the Cisco Presence Engine service in all IM and Presence nodes before resetting the administrator password. After the password reset, restart Cisco Presence Engine service in all the nodes. Make sure that you perform this task during maintenance because you may face presence issues when the PE is stopped. If you change the password from IM and Presence nodes, make sure the new password is same as the current administrator password in Unified Communication Manager.

utils reset_application_ui_administrator_password

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

utils restore_application_ui_administrator_account

This command restores the application user interface administrator account.

utils restore_application_ui_administrator_account

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils rosters list limited

Run this command on the database publisher node to obtain a count of invalid watchers and invalid contacts. The total counts display in the CLI.

Command Modes

Administrator (admin:)

Usage Guidelines

We recommend that you run this command only during a maintenance window. This command will list only the count and no details of the invalid records. For details on the invalid records, try **utils rosters list [watchers | contacts | full**.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence Service

utils rosters list full

Run this command on the database publisher node to write the details of all invalid watchers and invalid contacts to a file. The command also displays the total counts in the CLI.

Command Modes

Administrator (admin:)

Usage Guidelines

We recommend that you run this command only during a maintenance window.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence Service

utils rosters list watchers

Run this command on the database publisher node to write the details of all invalid watchers in the cluster to a file. The total count of invalid contacts also displays in the CLI.

Command Modes

Administrator (admin:)

Usage Guidelines

We recommend that you run this command only during a maintenance windows. While executing, progress is displayed in the CLI as well as in a log file.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence Service

utils rosters list contacts

Run this command on the database publisher node to write the details of all invalid contacts in the cluster to a file. The total count of invalid contacts also displays in CLI.

Command Modes

Administrator (admin:)

Usage Guidelines

We recommend that you run this command only during a maintenance window.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence Service

utils rosters delete

Run this command on the database publisher node to delete all invalid watchers and invalid contacts in the IM and Presence cluster.

Command Modes

Administrator (admin:)

Usage Guidelines

We recommend that you run this command only during a maintenance windows. While executing, progress is displayed in the CLI as well as in a log file.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence Service

utils scheduled-task disable

This command disables the scheduled-task.

utils scheduled-task disable scheduled-task

Syntax Description

Parameters	Description
scheduled-task	Enter the name of the task that you need to disable.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils scheduled-task enable

This command enables the scheduled-task.

utils scheduled-task enable scheduled-task

Syntax Description

Parameters	Description
scheduled-task	Enter the name of the task that you need to enable.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils scheduled-task list

This command lists all the scheduled tasks.

utils scheduled-task list

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils set urlpattern disable

This command disables the URL pattern and modifies the `zzz20_product_profile.sh` file. After the URL pattern is disabled, this command appends the following line:

```
export TOMCAT_EXCLUDE_URLPATTERNS="/ucmuser"
```

utils set urlpattern disable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils set urlpattern enable

This command enables the URL pattern and modifies the `zzz20_product_profile.sh` file. After the URL pattern is enabled, this command appends the following line:

```
export TOMCAT_EXCLUDE_URLPATTERNS=""
```

utils set urlpattern enable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils service

This command activates, deactivates, starts, stops, or restarts a service.

utils service **activate** | **deactivate** | **start** | **stop** | **restart** *service_name*

Syntax Description

Parameters	Description
service_name	Represents the name of the service you want to affect, for example: • System NTP • System SSH • Service Manager • A Cisco DB • Cisco Database Layer Monitor • Cisco Unified Serviceability This list is not exhaustive. For a full list of services for the node enter the command: **utils service list** **Note** If you want to restart the Cisco Tomcat service for standalone Cisco Prime License Manager, execute the following command or reboot the server: **utils service restart Cisco Prime LM Server**.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

utils service list

This command retrieves a list of all services.

utils service list [**page**]

Syntax Description

Parameters	Description
[**page**]	Displays the output one page at a time.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: IM and Presence service on Unified Communications Manager

utils service auto-restart

This command starts or stops a specified service.

utils service auto-restart **enable** | **disable** | **show** *service-name*

Syntax Description

Parameters	Description
enable	Starts auto-restart.
disable	Stops auto-restart.
show	Shows the status of a service.
service-name	Represents the name of the service that you want to start, stop, or show: • System NTP • System SSH • Service Manager • A Cisco DB • Cisco Tomcat • Cisco Database Layer Monitor • Cisco Unified Serviceability

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils service start

This command starts a service.

utils *service* **start**

Syntax Description

Parameters	Description
service	Enter the name of a service, which can consist of multiple words.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service onUnified Communications Manager, and Cisco Unity Connection

utils service stop

This command stops a service.

utils *service* **stop**

Syntax Description

Parameters	Description
service	Enter the name of a service, which can consist of multiple words.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service onUnified Communications Manager, and Cisco Unity Connection

utils snmp config 1/2c community-string

This interactive command adds, deletes, lists or updates a community string.

utils snmp config 1/2c community-string add | **delete** | **list** | **update**

Syntax Description

Parameters	Description
add	Adds a new community string.
delete	Deletes a community string.
list	Lists all community strings.
update	Updates a community string.

Command Modes

Administrator (admin:)

Usage Guidelines

The system prompts you for the parameters.

The SNMP Master Agent service is restarted for configuration changes to take effect. Do not abort command after execution until restart is complete. If the command is aborted during service restart, verify service status of "SNMP Master Agent" by using `utils service list`. If service is down, start it by using `utils service start SNMP Master Agent`

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp config 1/2c inform

This interactive command adds, deletes, lists or updates inform notification destinations.

utils snmp config 1/2c inform add | delete | list | update

Syntax Description

Parameters	Description
add	Adds a notification destination.
delete	Deletes a notification destination.
list	Lists all notification destinations.
update	Updates a notification destination.

Command Modes

Administrator (admin:)

Requirements

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp config 1/2c trap

This interactive command affects trap notifications.

utils snmp config 1/2c trap add | delete | list | update

Syntax Description

Parameters	Description
add	Adds a new v1/2c trap notification destination associated with a configured v1/2c community string.

Parameters	Description
delete	Deletes the configuration information for an existing v1/2c trap notification destination.
list	Lists the v1/2c trap notifications currently configured.
update	Updates configuration information for an existing v1/2c trap notification destination.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

utils snmp config 3 inform

This interactive command affects the v3 inform notification.

utils snmp config 3 inform add | delete | list | update

Syntax Description

Parameters	Description
add	Adds a new v3 inform notification destination associated with a configured v3 username.
delete	Deletes the configuration information for an existing v3 inform notification destination.
list	Lists the v3 inform notifications currently configured.
update	Updates configuration information for an existing v3 inform notification destination.

Command Modes

Administrator (admin:)

Usage Guidelines

The system prompts you for the parameters.

The SNMP Master Agent service is restarted for configuration changes to take effect. Do not abort command after execution until restart is complete. If the command is aborted during service restart, verify service status of "SNMP Master Agent" by using `utils service list`. If service is down, start it by using `utils service start SNMP Master Agent`

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp config mib2

This interactive command affects the Mib2 configuration information.

utils snmp config mib2 add | delete | list | update

Syntax Description

Parameters	Description
add	Adds the Mib2 configuration information.
delete	Deletes the Mib2 configuration information.
list	Lists the Mib2 configuration information.
update	Updates the Mib2 configuration information.

Command Modes

Administrator (admin:)

Usage Guidelines

The system prompts you for the parameters.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp config 3 trap

This interactive command affects trap notifications.

utils snmp config 3 trap add | delete | list | update

Syntax Description

Parameters	Description
add	Adds a new v3 trap notification destination associated with a configured v3 username.
delete	Deletes the configuration information for an existing v 3 trap notification destination.
list	Lists the v3 trap notifications currently configured.
update	Updates configuration information for an existing v3 trap notification destination.

Command Modes

Administrator (admin:)

Usage Guidelines

The system prompts you for the parameters.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp config 3 user

This interactive command affects v3 user configuration.

utils snmp config 3 user add | **delete** | **list** | **update**

Syntax Description

Parameters	Description
add	Adds a new v3 user with the v3 authentication and privacy passwords.
delete	Deletes the configuration information for an existing v3 user.
list	Lists the v3 users currently configured.
update	Updates configuration information for an existing v3 user.

Command Modes

Administrator (admin:)

Usage Guidelines

The system prompts you for the parameters.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp get

This interactive command gets the SNMP data using the specified version for the specified MIB OID.

utils snmp get *version*

Syntax Description

Parameters	Description
version	Specifies the SNMP version. Possible values include 1, 2c or 3.
community	Specifies the SNMP community string.

Parameters	Description
ip-address	Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node.
object	Specifies the SNMP Object ID (OID) to get.
file	Specifies a file in which to save the command output.

Command Modes

Administrator (admin:)

Usage Guidelines

If you run the command on a specific OID (leaf) in the MIB, you get the value of the MIB. For example to get the system uptime: `iso.3.6.1.2.1.25.1.1.0 = Timeticks: (19836825) 2 days, 7:06:08.25`

If you provide the IPv4/IPv6 address of a remote host, the command gets executed on the remote host.

The IPv4/IPv6 address is required. You cannot use a domain name.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils snmp get 1

This command gets the SNMP data using version 1 for the specified MIB OID.

utils snmp get 1 *version*

Syntax Description

Parameters	Description
version	Specifies the SNMP version. Possible values include 1, 2c or 3.
community	Specifies the SNMP community string.
ip-address	Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node.
object	Specifies the SNMP Object ID (OID) to get.
file	Specifies a file in which to save the command output.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils snmp get 2c

This command gets the SNMP data using version 2c for the specified MIB OID.

utils snmp get 2c *version*

Syntax Description

Parameters	Description
version	Specifies the SNMP version. Possible values include 1, 2c or 3.
community	Specifies the SNMP community string.
ip-address	Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node.
object	Specifies the SNMP Object ID (OID) to get.
file	Specifies a file in which to save the command output.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils snmp get 3

This command gets the SNMP data for the specified MIB OID.

utils snmp get 3 *version*

Syntax Description

Parameters	Description
version	Specifies the SNMP version. Possible values include 1, 2c or 3.
community	Specifies the SNMP community string.

Parameters	Description
ip-address	Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node.
object	Specifies the SNMP Object ID (OID) to get.
file	Specifies a file in which to save the command output.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils snmp hardware-agents

This command affects the SNMP agents on the server.

utils snmp hardware-agents status | start | stop | restart

Syntax Description

Parameters	Description
status	Displays the status of the SNMP agents provided by the vendor of the hardware. **Note** Only agents that provide status get displayed by this command. Not all hardware agents provide status.
stop	Stops all SNMP agents provided by the hardware vendor.
restart	Restarts all of the SNMP agents provided by the vendor of the hardware.
start	Starts all of the SNMP agents provided by the vendor of the hardware.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp test

This command sends sample alarms to local syslog and remote syslog.

utils snmp test

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

```
admin: admin:utils snmp test
Service Manager is running
Test SNMP Trap starts with Local Host Name, Specify a Remote Sever Name to test Remote
Syslog
TestAlarmInformational sent [Returncode=0]
TestAlarmEmergency sent [Returncode=0]
TestAlarmAlert sent [returncode=0]
TestAlarmCritical sent [Returncode=0]
TestAlarmDebug sent [Returncode=0]
TestAlarmNotice sent [Returncode=0]
TestAlarmWarning sent [Returncode=0]
TestAlarmError sent [Returncode=0]
TestAlarmWindows sent [Returncode=0]
Message from syslogd@ipcbu-plat44 at Sat Jul 17 03:56:11 2010 ...
ipcbu-plat44 local7 0 : 1: ipcbu-plat44.blr.eng: Jul 16 2010 22:26:11.53 UTC :
%UC_-0-TestAlarmEmergency: %[AppID=Cisco CallManager][ClusterID=][NodeID=ipcbu-plat44]:
Testing EMERGENCY_ALARM
```

utils snmp walk

This interactive command command walks through the SNMP MIB using the specified version, starting with the specified OID.

utils snmp walk *version*

Syntax Description

Parameters	Description
version	Specifies the SNMP version. Possible values include 1, 2c or 3.
community	Specifies the SNMP community string.
ip-address	Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node.
object	Specifies the SNMP Object ID (OID) to walk
file	Specifies a file in which to save the command output.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

Example

For the below example, community string is created using the `utils snmp config 1/2c community-string` command.

```
admin:utils snmp walk 1

ctrl-c: To quit the input.


Enter the community string:: public
Enter the ip address of the Server, use 127.0.0.1 for localhost.
Note that you need to provide the IP address, not the hostname.:: <enter the IP address of
 your server>
The Object ID (OID):: iso.3.6.1.2.1.1.1.0
Enter parameter as "file" to log the output to a file. [nofile]::
This command may temporarily impact CPU performance.
Continue (y/n)?y
SNMPv2-MIB::sysDescr.0 = STRING: Linux release:3.10.0-1062.18.1.el7.x86_64 machine:x86_64
##########################################################################################
utils snmp walk 2c -> same as utils snmp walk 1
##########################################################################################
For the below example, user is created using
utils snmp config 3 user add

utils snmp walk 3
admin:utils snmp walk 3

ctrl-c: To quit the input.


Enter the user name:: test
Enter the authentication protocol [SHA]:: SHA
Enter the authentication protocol pass phrase:: ********
Enter the privacy protocol [AES128]:: AES128
```

```
Enter the privacy protocol pass phrase:: ********
Enter the ip address of the Server, use 127.0.0.1 for localhost.
Note that you need to provide the IP address, not the hostname.:: <enter the IP address of
 your server>
The Object ID (OID):: iso.3.6.1.2.1.1.1.0
Enter parameter as "file" to log the output to a file. [nofile]::
This command may temporarily impact CPU performance.
Continue (y/n)?y
SNMPv2-MIB::sysDescr.0 = STRING: Linux release:3.10.0-1062.18.1.el7.x86_64 machine:x86_64
```

utils snmp walk 1

This interactive command walks through the SNMP MIB using SNMP version 1 starting with the specified OID

utils snmp walk 1 *version*

Syntax Description

Parameters	Description
version	Specifies the SNMP version. Possible values include 1, 2c or 3.
community	Specifies the SNMP community string.
ip-address	Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node.
object	Specifies the SNMP Object ID (OID) to walk
file	Specifies a file in which to save the command output.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils snmp walk 2c

This interactive command walks through the SNMP MIB using SNMP version 2c starting with the specified OID.

utils snmp walk 2c *version*

Syntax Description

Parameters	Description
version	Specifies the SNMP version. Possible values include 1, 2c or 3.

Parameters	Description
community	Specifies the SNMP community string.
ip-address	Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node.
object	Specifies the SNMP Object ID (OID) to walk
file	Specifies a file in which to save the command output.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils snmp walk 3

This interactive command walks through the SNMP MIB starting with the specified OID.

utils snmp walk 3 *version*

Syntax Description

Parameters	Description
version	Specifies the SNMP version. Possible values include 1, 2c or 3.
community	Specifies the SNMP community string.
object	Specifies the SNMP Object ID (OID) to walk
ip-address	Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node.
file	Specifies a file in which to save the command output.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils soap realtimeservice test

This command executes a number of test cases on the remote server.

utils soap realtimeservice test [*remote-ip*]*remote-httpsremote https-password*

Syntax Description

Parameters	Description
remote-ip	Specifies the IP address of the server under test.
remote-https-user	Specifies a username with access to the SOAP API.
remote-https-password	Specifies the password for the account with SOAP API access.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on IM and Presence, Cisco Unity Connection

utils sso

This command provides information about SAML SSO authentication.

utils sso enable | **disable** | **status**

Syntax Description

Parameters	Description
enable	Provides the location in Cisco Unified CM Administration where you can enable SAML SSO.
disable	Disables SAML SSO based authentication.
status	Provides the status of SAML SSO.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

Example

```
Admin: utils sso enable
*** W A R N I N G ***
SSO cannot be enabled using CLI command
=======================================================
To enable Cluster wide SAML SSO please access
Cisco Unified CM Administration Page->System->SAML Single Sign On

=======================================================
```

utils sso recovery-url

This command enables or disables recovery URL for SAML SSO based authentication.

utils sso recovery-url enable | disable

Syntax Description

Parameters	Description
enable	Enables recovery URL for SAML SSO based authentication.
disable	Disables recovery URL for SAML SSO based authentication.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils system restart

This command allows you to restart the system on the same partition.

utils system restart

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils system shutdown

This command allows you to shut down the system.

utils system shutdown

Command Modes

Administrator (admin:)

Usage Guidelines

This command has a five-minute timeout. If the system does not shut down within five minutes, the command gives you the option of doing a forced shutdown.

Caution If the server is forced to shutdown and restart from your virtual machine, the file system may become corrupted.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils system switch-version

This command allows you to restart the system on the inactive partition.

utils system switch-version

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils system boot

This command redirects where the system boot output gets sent.

utils system boot console | serial

Syntax Description

Parameters	Description
console	Redirects the system boot output to the console.
serial	Redirects the system boot output to the COM1 (serial port 1).

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

utils system upgrade

This command allows you to install upgrades and Cisco Option (COP) files from both local and remote directories.

utils system upgrade initiate | **cancel** | **status**

Syntax Description

Parameters	Description
cancel	Cancels the active upgrade.
initiate	Starts a new upgrade wizard or assumes control of an existing upgrade wizard. The wizard prompts you for the location of the upgrade file from the source. The source displays the following options: • Remote Filesystem via SFTP • Remote Filesystem via FTP • Local DVD/CD • quit
status	Displays the status of an upgrade.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection.

utils system enableAdministration

Configuration changes are not permitted during an upgrade; however, you can use this command to enable emergency provisioning during an upgrade.

Caution Once you begin the upgrade process, configuration changes are not permitted until the upgrade is complete and you have performed all of the post-upgrade tasks. Configuration changes include:

- changes made through any of the Unified Communications Manager or IM and Presence Service graphical user interfaces (GUI), the command line interface (CLI), or the AXL API
- LDAP synchronizations, including incremental synchronizations that are pushed to Unified Communications Manager from an Oracle LDAP
- automated jobs
- devices attempting to autoregister

Any configuration changes that you make during an upgrade may be lost, and some configuration changes can cause the upgrade to fail.

utils system enableAdministration

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1 and 4

utils update dst

This command updates the daylight saving time (DST) rules for the current year.

utils update dst

Command Modes Administrator (admin:)

Usage Guidelines This command takes a backup of the existing DST rules file and creates a new DST rules file for the current year.

Caution Restart the phones after you execute the command. Not restarting the phones results in wrong DST start and stop dates.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to Unified Communications Manager and IM and Presence service.

utils users validate

This command checks user records across all nodes and clusters in the deployment to identify duplicate or invalid userid or directory URI values.

utils users validate all | userid | uri

Syntax Description

Parameters	Description
all	Validate the userid and directory URI values for all users in the nodes and clusters.
userid	Validate the userid value for all users in the nodes and clusters.
uri	Validate the directory URI value for all users in the nodes and clusters.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: IM and Presence Service on Unified Communications Manager

utils vmtools refresh

This command refreshes the currently installed VMware Tools to the latest version that is prescribed by the ESXi host for that VM.

Note After the initial reboot, VMware Tools are in the `running` state. When you upgrade to a newer version of VMware Tools, selinux may initially block the installation. In this case, the system still allows VMware Tools to install, but a new dynamic policy is generated to suppress any additional selinux blockage. You can view the new dynamic policy with the **utils os secure dynamic-policies list** command. For more information, see the **utils os secure dynamic-policies** CLI command.

Note This is applicable for native vmtools.

utils vmtools refresh

Command Modes

Administrator (admin:)

Usage Guidelines

To update the current version of the VMware Tools, select **Guest** > **Install/Upgrade VMWare Tools** > **Interactive Tools Upgrade**.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:utils vmtools refresh
VMware Tools match host. Upgrade allowed, though not required.

***   W A R N I N G   ***
Running this command will update your current version of VMware Tools
to the latest version prescribed by the ESXi host on which this VM is
running. The tools install will cause your system to reboot twice.
```

utils vmtools status

This command displays the type and the version of currently installed VMware Tools.

utils vmtools status

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils vmtools switch open

This command uninstalls the currently installed native VMware Tools and installs the open VMware Tools.

utils vmtools switch open

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils vmtools switch native

This command uninstalls the currently installed open VMware Tools and installs the native VMware Tools.

utils vmtools switch native

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils system boot status

This command shows the location where the system boot messages are to be sent. The location is either console or serial port one.

utils system boot status

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection