Administration Console User Guide for Cisco Unified Intelligence Center, Release 12.6(1)

First Published: 2021-05-14

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2010–2021 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Preface** 1

About This Guide 1

Audience 1

Related Documentation 1

Communications, Services, and Additional Information 1

Documentation Feedback 2

CHAPTER 2 **User Interface** 3

Administration Console 3

Access Administration Console 3

Home Page 4

Users in the Administration Console 5

Super Users 5

System Application User 5

System Administration User 6

Unified Intelligence Center Cluster 6

Nodes in the Unified Intelligence Center Cluster 6

Unified Intelligence Center Cache 7

Unified Intelligence Center—User Sessions 7

CHAPTER 3 **User Management** 9

Manage All Super Users 9

Super Users and Security 10

Edit Configuration Data for Super User 10

CHAPTER 4 **Device Configuration** 15

Device Configuration 15
Create or Edit Device Information 16

CHAPTER 5 Log and Trace Settings 19
View List of Host Addresses for Configured Devices 19
Logging for Unified Intelligence Center 19
Logging and Tracing for OAMP 19
Edit Syslog Server Connection Settings for Unified Intelligence Center 20
Edit Syslog Server Connection Settings for OAMP 20
Subsystem Trace Definitions - OAMPServer 21
OAMP 21
OAMP-BO 21
WSM-BO 21
IP Address and Hostname of Cisco Unified Intelligence Center Nodes 22
IP Address Change Checklist 22
Prepare for IP Address Change 22
Change Cluster IP Addresses for Subscriber Servers Defined by IP Addresses 24
Change Cluster IP Address for Publisher Server Defined by IP Address 25
Change Cluster IP Addresses for Subscriber Servers Defined by Host Name 26
Change Cluster IP Address for Publisher Server Defined by Host Name 29
Change Hostname for Unified Intelligence Center Publisher (Controller) Node 31
Change Hostname for Unified Intelligence Center Subscriber (Member) Node 32
Verify IP Address Change 33
Configure IPv6 34
Set up IPv6 using CLI 34
Set up IPv6 using Cisco Unified Communications Operating System Administration 35

CHAPTER 6 Control Center 37
Control Center 37

CHAPTER 7 Cluster Configuration 39
Configure Active Directory Settings 39
Configure Active Directory with SSL 43
Configure SMTP Settings 43

Upload Self-Signed Certificates 44
Unified CCE User Integration 45
Configure Unified CCE User Integration 46
Cluster Configuration for JVM Using Hazelcast 47
Troubleshooting Cluster Configuration 49

CHAPTER 8 Tools 51
Real Time Monitoring Tool 51
Launch RTMT 52
RTMT Client Support Services 52
RTMT Integration 53
The RTMT Interface 55
Cisco Unified Intelligence Center Services 56
Unified IC performance objects and counters 56
Cisco Unified Intelligence Center Counters 58
CUIC Tomcat Connector 58
CUIC Tomcat JVM 59
CUIC Tomcat Web Application 59
DB Change Notification Client 60
DB Change Notification Server 60
DB Change Notification Subscriptions 61
DB Local DSN 61
DB User Host Information Counters 61
DBPerformance Info 61
Enterprise Replication DBSpace Monitors 62
Enterprise Replication Perfmon Counters 62
Intelligence Center General Information Section 62
Intelligence Center JVM Statistics 62
Intelligence Center System Condition Table 63
Intelligence Center Tomcat Connector - HTTPS 65
IP 65
IP6 66
Memory 68
Network Interface 69

Number of Replicates Created and State of Replication 70
Partition 71
PermalinkInfo 72
Process 72
Processor 73
Ramfs 74
Reporting Engine Info 74
RESTInfo 75
SchedulerInfo 76
System 76
TCP 77
Thread 78
Disaster Recovery System 78
Backup and Restore Overview 78
Backup Prerequisites 79
Backup Procedure Taskflow 80
Configure backup devices 80
Configure a Schedule Backup 81
Start a Manual Backup 82
View Current Backup Status 83
Estimate Size of Backup Tar 84
View Backup History 84
Network Management 84
Configure SNMP-Associated Settings 84
Unified Intelligence Center SNMP MIBs 85
MIB Objects 85
MIB Notifications (CUIC TRAPs) 88
Cisco Unified Intelligence OS Administration 93
Configure Custom Logon Messages 93

CHAPTER 9 **Manage Certificates** 95
Install Certificate Authority (CA) Certificate 95
CUIC Server Certificates 96
Access Platform Web Applications using Chrome Browser 96

Download the Server Certificate from CUIC Node 96
Add Certificate to Trusted Root Certification Authorities on Windows Client System 97
Add Certificate to Keychain Access in Mac Client Machine 97

APPENDIX A **Command Line Interface** 99
Unset Command 100
unset cuic properties 100
unset ipsec 100
unset network dns 100
unset_host-to-ip 100
Utils Command 101
utils auditd 101
utils core 101
utils create report 101
utils cuic 102
utils cuic cpudiagnostics 102
utils cuic mbeans 102
utils cuic nmon 103
utils cuic purge 103
utils cuic restorepub 103
utils cuic cors 104
utils cuic session 106
utils cuic cluster show 107
utils cuic cluster mode 107
utils cuic cluster refresh 107
utils cuic logging 107
utils cuic logging config set 107
utils cuic logging config show 108
utils cuic logging config clear 108
utils cuic logging list 108
utils cuic logging reset 109
utils cuic logging update 109
utils cuic user make-admin 109
utils dbreplication 110

utils dbreplication clusterreset 110
utils dbreplication dropadmindb 110
utils dbreplication rebuild 110
utils dbreplication repair 110
utils dbreplication reset 110
utils dbreplication runtimestate 111
utils dbreplication setrepltimeout 111
utils dbreplication status 111
utils dbreplication stop 111
utils diagnose 112
utils disaster_recovery 112
utils disaster_recovery backup 112
utils disaster_recovery cancel_backup 113
utils disaster_recovery device 113
utils disaster_recovery estimate_tar_size 113
utils disaster_recovery history 114
utils disaster_recovery jschLogs 114
utils disaster_recovery prepare 114
utils disaster_recovery restore 114
utils disaster_recovery show_backupfiles 115
utils disaster_recovery show_registration 115
utils disaster_recovery show_tapeid 115
utils disaster_recovery status 115
utils firewall 115
utils firewall ipv4 116
utils firewall ipv6 116
utils import config 117
utils iostat 118
utils iothrottle 118
utils netdump 118
utils netdump client 119
utils network 119
utils network arp 119
utils network capture 120

utils network connectivity 120
utils network host 120
utils network ping 120
utils network tracert 121
utils network ipv6 121
utils ntp 121
utils raid disk maintenance 122
utils remote_account 123
utils_reset 123
utils restore_application_ui_administrator_account 123
utils service 124
utils service list 124
utils service restart 124
utils service start 124
utils service stop 124
utils snmp 124
utils snmp get 124
utils snmp test 125
utils snmp walk 125
utils snmp configure 125
utils soap realtimeservice test 127
utils system 127
utils system restart 127
utils system shutdown 127
utils system switch-version 128
utils system upgrade 128
utils vmtools 128
utils vmtools refresh 128
Show Commands 129
show account 129
show accountlocking 129
show cert 129
show cli 129
show cuic-properties 130

show cuic component-status 131
show diskusage 131
show environment 132
show hardware 132
show ipsec 132
show logins 132
show memory 133
show myself 133
show network 133
show network all 133
show network cluster 133
show network dhcp eth0 status 133
show network failover 134
show network ip_conntrack 134
show network ipprefs 134
show network ipv6 134
show network max_ip_conntrack 134
show network ntp 134
show network route 135
show network status 135
show open 135
show open files 135
show open ports 136
show packages 136
show password 136
show perf 137
show perf counterhelp 137
show perf list 137
show perf query 137
show process 138
show process list 138
show process load 138
show process name 139
show process open-fd 139

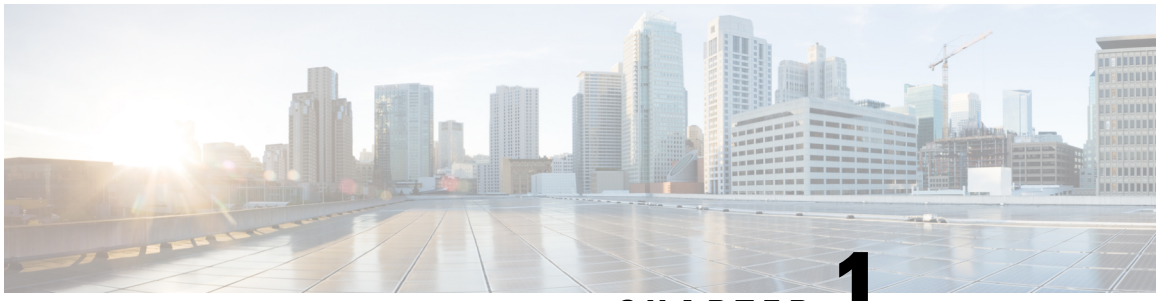
show process search 139
show process user 140
show process using-most 140
show registry 140
show smtp 140
show stats io 141
show status 141
show tech 141
show tech activesql 141
show tech all 141
show cuic tech 141
show tech database 142
show tech dberrorcode 142
show tech dbintegrity 142
show tech dbinuse 143
show cuic tech dbschema 143
show tech dbstateinfo 143
show tech dumpCSVandXML 143
show tech network 143
show tech notify 144
show tech params 144
show cuic tech procedures 144
show tech repltimeout 144
show tech sqlhistory 144
show cuic tech systables 145
show tech system 145
show cuic tech table 145
show cuic tech triggers 145
show tech version 146
show timezone 146
show tls server cert_type 146
show ups status 146
show version 147
show web-security 147

show workingdir 147
Set Commands 147
set account 147
set accountlocking 147
set cert 148
set cli 148
set commandcount 148
set cuic properties 149
set ipsec 152
set logging 152
set network 152
set network cluster publisher 152
set network dhcp eth0 152
set network dns options 153
set network dns {primary | secondary} 153
set network domain 153
set network failover 153
set network gateway 153
set network hostname 154
set network IP eth0 154
set network ipv6 154
set network max_ip_conntrack 155
set network mtu 155
set network nic eth0 155
set network pmtud 155
set network restore 155
set network status eth0 156
set password 156
set smtp 157
set cuic syslog 158
set timezone 158
set tls server cert_type 158
set tls min-version 159
set web-security 159

set workingdir 160
Run Commands 160
run loadxml 160
run cuic sql 160
run loadcsv 160
file commands 161
file check 161
file delete 161
file dump 161
file get 162
file list 162
file search 163
file tail 163
file view 163
Delete Commands 164
delete account 164
delete dns 164
delete ipsec 164
delete process 164
delete smtp 165
Use CLI 165

APPENDIX B **Load Balance** 167
Load Balance 167

APPENDIX C **Unrestricted Resource Access** 169
Unrestricted Resource Access 169



CHAPTER 1

Preface

- About This Guide, on page 1
- Audience, on page 1
- Related Documentation, on page 1
- Communications, Services, and Additional Information, on page 1
- Documentation Feedback, on page 2

About This Guide

This document explains the Unified Intelligence Center Administration console.

The Administration console, available an all deployments, is a web-based, centralized interface for setting and displaying configuration information about the cluster.

The Administration application is one of two web interfaces for Unified Intelligence Center. The other is the Unified Intelligence Center Reporting application.

Audience

This guide is prepared for Super Users who sign in to the Administration interface to administer, provision, monitor, and troubleshoot the Unified Intelligence Center.

Related Documentation

Guides for the Cisco Unified Intelligence Center

The Developers' Forum for the Cisco Unified Intelligence Center

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

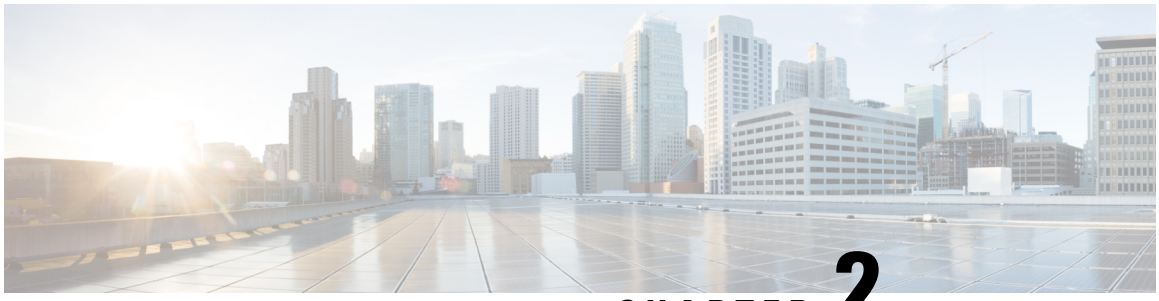
Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

You can provide comments about this document by sending email to the following address:

contactcenterproducts_docfeedback@cisco.com.

We appreciate your comments.



CHAPTER 2

User Interface

- Administration Console, on page 3
- Access Administration Console, on page 3
- Home Page, on page 4
- Users in the Administration Console, on page 5
- Unified Intelligence Center Cluster, on page 6
- Unified Intelligence Center Cache, on page 7
- Unified Intelligence Center—User Sessions, on page 7

Administration Console

Unified Intelligence Center is installed on a Cisco Unified Operating System platform as a cluster with a maximum of eight nodes: one Controller node and up to seven Member nodes.

The Controller node is mandatory and provides both the Administration and the Unified Intelligence Center Reporting web applications. A cluster can consist of the Controller node only.

Member nodes are optional and have the Unified Intelligence Center Reporting application only. (Unified Intelligence Center Administration is not available on a Member node.)

The Administration console manages all components in a unified deployment and also provides links to:

- Cisco Unified Serviceability and SNMP
- Disaster Recovery System
- Real Time Monitoring Tool (RTMT)

Related Topics

Configure SNMP-Associated Settings, on page 84
Real Time Monitoring Tool, on page 51
Disaster Recovery System, on page 78

Access Administration Console

The System Application User who is defined during the installation is by default the initial Super User who can sign in to the Administration Application.

This initial Super User can then create other Super Users in the **Admin Users** page. For more information, see *Manage All Super Users*.

Note When you log in to the Admin Console site and you do not have any scheduled backup configured and enabled, Unified Intelligence Center returns the message "No active backup schedule is available. Set up a new schedule now." Unified Intelligence Center displays this message only for the administrator.

To access the Administration console:

Procedure

Step 1 Direct your browser to the URL *https://<HOST ADDRESS>/oamp* where *HOST ADDRESS* is the IP Address or Hostname of your server.

Step 2 Sign in using your Super User (system application user) ID and password. A successful sign-in launches the OAMP application.

What to do next

See *Home Page*.

The session timeout for inactivity is thirty minutes. It is not configurable.

See also: *Users in the Administration Console*.

Related Topics

System Application User, on page 5
Home Page, on page 4
Users in the Administration Console, on page 5
Manage All Super Users, on page 9

Home Page

The Home page appears by default after a successful sign-in.

Table 1: Actions From This Page

To	Do this
Display the values for a function	Click a menu in the left navigation pane.
Open the Unified Intelligence Center reporting interface on a member node	• Open a new browser window and enter this URL: *https://<HOST ADDRESS>:8444/* where *HOST ADDRESS* is the IP Address or Hostname of your server.
Verify your signed on identity	This shows as protected text after *Signed on as*. Displays **Administrator** on the top-right corner of your screen.

To	Do this
Sign Out	Click **Administrator** > **Sign Out** on the top-right corner of your screen.
Return to this Home page	Click **Home** in the left navigation pane.

Users in the Administration Console

There are three user accounts that have access to the Administration console:

- Super Users
- System Application User
- System Administration User

Super Users

This user role is defined in the Administration console. It is the only user role for Administration.

The initial and default Super User is the *System Application User* who is configured during installation.

The initial Super User (the System Application User) can sign in to the Unified Intelligence Center Reporting console and has *all* User Roles and *full permissions* for all drawers in Unified Intelligence Center Reporting. Those credentials cannot be removed from the initial Super User.

Additional Super Users who are added in the Administration Console can also sign in to Unified Intelligence Center Reporting and are considered to be IMS users. They have limited Login User role only, until the Unified Intelligence Center Reporting security administrator gives them additional roles and flags them as Active users.

Local users can log in using their IMS username and password. After logging in for the first time, the users are listed on the User List Page. The username is not case sensitive, but the password is case sensitive.

System Application User

This user role is defined during installation. Although it is possible to define unique application user names and passwords during the installation of each node, you must use the same credentials for all installations.

The application user defined during the installation of the *Controller* is the only System Application User recognized by Unified Intelligence Center.

This user has full rights to all functions in the Administration and Unified Intelligence Center Reporting applications, as described below:

- Can log in to the Administration application and becomes the initial Super User for Administration.
- Can create additional Super Users in the Administration application.
- Can log in to Unified Intelligence Center and has full rights to all functions in Unified Intelligence Center.
- Is the initial Security Administrator user in the Unified Intelligence Center Reporting application.

- Can create additional Security Administrator users in the Unified Intelligence Center Reporting application.
- Cannot have any role taken away from them.
- Cannot take any role away from himself.
- This user can log in to the Reporting application and is the initial System user.

System Administration User

The System Administrator account User ID and password are configured at installation for each node. You must enter the same user name and password for all nodes.

The System Administrator for the *Controller* can access:

- The Cisco Systems tools on the Navigation drop-down menu in the Administration console: Disaster Recovery System, Cisco Unified Serviceability, and Cisco Unified OS Administration interfaces.
- The CLI for the Controller.

The System Administrator has no access to functions in the Unified Intelligence Center Reporting application.

Note If you configure unique System Administrator credentials for Member nodes, use those credentials to access the CLI for those Member servers.

Unified Intelligence Center Cluster

Unified Intelligence Center is installed as a cluster of at least one and up to eight nodes.

Nodes in the Unified Intelligence Center Cluster

The first node in the Unified Intelligence Center cluster is the Controller. For database replication, this node is referred to as the “publisher”. This means that it *publishes* or replicates, its databases to Member nodes.

The Member nodes are referred to as *subscribers* of the database replication. Members receive data from the publisher.

Each node on which reporting functionality is processed (the Controller node and each member node) has a Unified Intelligence Center database which is constantly accumulating and removing records; for example, when a dashboard is added or a user record is removed.

When all nodes are up, changes to the Unified Intelligence Center databases replicate synchronously among the Controller/publisher and all Member/subscribers by means of an “update anywhere” model. For more information, see *Database Replication*.

The Disaster Recovery System performs the database maintenance. For more information, see *Disaster Recovery System*.

Related Topics

utils dbreplication, on page 110

utils disaster_recovery, on page 112

Unified Intelligence Center Cache

Unified Intelligence Center uses a cache to optimize access to the local Cisco Unified Intelligence Center database and it is built on top of the local configuration database. Unified Intelligence Center is designed to provide a highly scalable cluster in which every node manages its own local cache independently of other nodes.

When an item stored in the local cache (such as a report template or a dashboard) is modified, a message is sent to other nodes in the cluster indicating that the item has been modified and that their version of that item is stale. On receipt of this message, each node invalidates its own references to the stale item in the local cache. In this manner, all nodes remain synchronized.

In a few exceptional cases where, stale data can be re-cached or become out of synch in the cluster. Therefore, the Unified Intelligence Center System Configuration administrator has access to the **Synchronize Cluster** link below the username on the top-right corner of your user interface screen.

Click and confirm. This action notifies all nodes in the cluster to clear their local cache, and it synchronizes and empties all caches in the cluster. Clearing the locale cache forces each node to go directly to the database for the requested information.

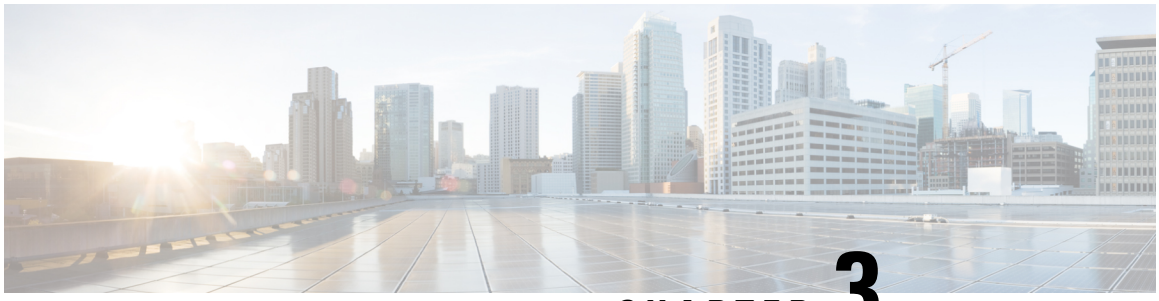
Each node gets fresh data from the database. The data is automatically put into the local cache and accessed during future requests. Data will be consistent in the database, and there will be no loss of information.

Note It is best to perform this action during off-hours.

Unified Intelligence Center—User Sessions

You can configure the maximum number of concurrent sessions a Unified Intelligence Center user can log in to. If a user reaches the configured limit, further login attempts are rejected. The maximum number of concurrent sessions is configured by using the **set webapp session maxlimit** command. For more information about this command, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html.

If a Unified Intelligence Center user reaches the maximum configured session count, that user can log in to another session only after signing out from an active session or if an active session times out due to inactivity. The session timeout duration is configured by using the **set cuic properties session-timeout** command. For more information about this command, see set cuic properties.



CHAPTER 3

User Management

Choose User Management in the left navigation pane to access the User Management page, where you view and maintain the Super Users for the Administration console.

Super Users are authorized to add and maintain the functions that are controlled in the Administration console, such as adding devices and starting or stopping services.

Note Super Users can also sign in to Unified Intelligence Center Reporting.

- Manage All Super Users, on page 9
- Edit Configuration Data for Super User, on page 10

Manage All Super Users

The **User Management** page is a list of the names for all configured Super Users in the system. This list always contains at least one row that shows the System Application User who is configured during installation and who becomes the initial Super User for Unified Intelligence Center. See Users in the Administration Console.

Table 2: Actions From This Page

To	Do This
Configure Policy	Click **Policy**. For more information, see *Edit Configuration Data for Super User*.
Add a new Super User	Click **New**. For more information, see *Edit Configuration Data for Super User*. You can add as many Super Users as you need.
Refresh the page	Click the Refresh icon.

To	Do This
Delete a Super User	From the **Actions** column > Ellipsis (...) button, click **Delete** against the user to be deleted. You cannot delete: • the Super User defined in the installation. • the Super User who is currently signed in.
Edit an existing Super User	From the **Actions** column > Ellipsis (...) button, click **Edit** against the user to be edited. For more information, see *Edit Configuration Data for Super User*.

Related Topics

Users in the Administration Console, on page 5
Edit Configuration Data for Super User, on page 10

Super Users and Security

There is no limit to the number of additional Super Users that the default Super User (the System Application User) can create.

Although only the initial, default Super User (the System Application User) has full permissions in Unified Intelligence Center Reporting, *all* Super Users have *identical permissions in the Administration console*.

Be aware that any Super User can delete or change the password of another Super User, even if that other Super User is currently logged in.

Edit Configuration Data for Super User

Use this page to create configuration data for a new Super User or to edit the configuration data for an existing Super User.

Table 3: General Tab

Field	Description
Administrator Password	Password to authenticate changes made to the **General** and **Credentials** tabs.
User Name	The user Id for the user.
User Password	User Password. To require a secure password, enable **Check for Trivial Passwords** on the **Policy** information screen. When you modify a user password, the changes are logged in the **CCBU-oamp.<timestamp>.log** file with `PASSWORD_RESET_AUDIT_LOG` as prefix to the log.
Confirm User Password	The same User password as above to confirm spelling.

Note The values on the **General** tab apply to the specific Super User being added or edited.

Table 4: Credentials Tab

Field	Description
Locked by Administrator	If checked, this Super User is locked out.
User Cannot Change / Must Change at Next Sign On	This pertains to the user password. Select either **User Cannot Change** or **User Must Change at Next Sign On**. You cannot select both.
Does Not Expire	This pertains to the user password. If the **Credential Expires After (days)** field on the **Policy** information screen is checked, then this field is disabled. If the **Credential Expires After (days)** field on the **Policy** information screen is clear, check **Does Not Expire** to enable a persistent password for the Super User. **Note** DO NOT check the **Does Not Expire** box if you have checked **User Must Change at Next Sign On**, as the user will not be prompted to change the password at the next sign in.
Reset Hack Count	Check this box to reset the hack count for this user and clear the **Time Locked Due to Failed Login Attempts** field. After the counter resets, the user can try logging in again. **Note** If the user is locked out of the account due to failed logins exceeding the number set for **Failed SignOn** (on the **Policy** information screen), then you can unlock the account by checking this box and clicking **Save**.
Failed Sign On Attempts	Displays the number of failed logon attempts since the last successful logon, since the hack count was reset for this Super User credential, or since the reset failed logon attempts time has expired.
Time Last Changed	Displays the last time this user's credentials were changed.
Time of Last Failed **Sign On** Attempt	Displays the date and time of the last sign on attempt by the user.
Time Locked by Administrator	Displays the date and time that this user account was locked.
Time Locked Due to Failed **Sign On** Attempts	Displays the date and time that the system last locked this user account due to failed logon attempts.

Note The values on the **Credentials** tab apply to the specific Super User being added or edited.

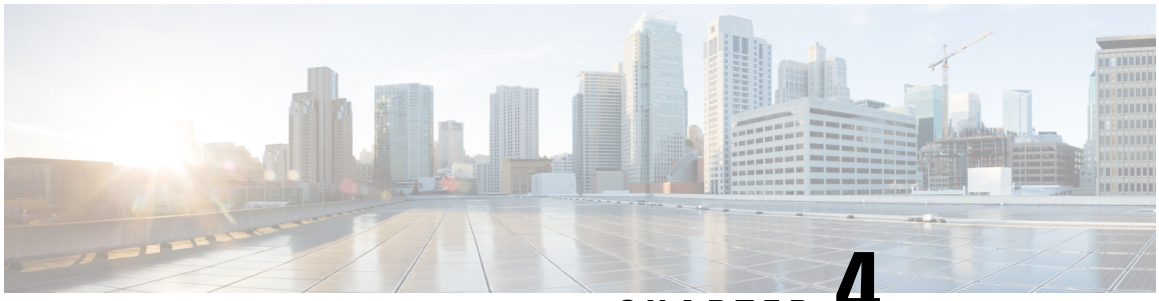
The credentials for Administration Super Users are encrypted into the local database. Super Users are not authenticated through Active Directory.

Table 5: Policy Information

Field	Description
Failed Sign On*	Specify the number of allowed failed logon attempts. When this threshold is reached, the system locks the account. By default, Unified Intelligence Center allows maximum five login attempts and the **No Limit For Failed Sign On** check box is unchecked. If you want to allow unlimited logon attempts, enter a value of zero or check the **No Limit For Failed Sign On** check box.
Reset Failed Sign On Attempts every (minutes)*	Specify the number of minutes before the counter is reset for failed sign on attempts. After the counter resets, the user can try logging in again. Allowed range is zero to 120; default is 30.
Lockout Duration (minutes)	Specify the number of minutes an account remains locked when the number of failed sign on attempts exceeds the specified threshold. Allowed range is zero to 120; default is 30. Checking the **Administrator Must Unlock** check box means that the account must be unlocked manually.
Minimum Duration Between Credential Changes (minutes)*	Specify the number of minutes that are required before a user can change credentials again. Allowed range is zero to 120; default is zero.
Credentials Expires After (days)*	Enter an integer here to define in how many days this user's credentials shall expire. After this many days has elapsed, the user will no longer be able to sign on. Optionally you can check **Never Expires** to have the credentials never expire.
Minimum Credential Length*	Minimum number of characters for the password.
Stored Number of Previous Credentials	Specify the number of previous passwords that the system stores. The system does not allow changing the password if the new password matches with any of the stored passwords. The maximum permissible value for this field is 15; the default value is 5, indicating that the new password should not be the same as the last 5 passwords.
Inactive Days Allowed*	Specify the number of days that a password can remain inactive before the account gets locked. Allowed range is zero to 5000; default is zero.
Expiry Warning Days*	Specify the number of days before a user password expires to start warning notifications. Allowed range is zero to 90; default is zero.

Field	Description
Check for Trivial Passwords	Check this check box for the system to disallow credentials that are easily hacked, such as common words, repeated character patterns, and so on.

Note The Policy information is applicable to all Super Users.



CHAPTER 4

Device Configuration

Devices are the physical machines servers on which the Cisco Unified Intelligence Center Administration Console and the Cisco Unified Intelligence Center reporting applications are installed.

- Device Configuration, on page 15

Device Configuration

This page lists all the currently configured devices (nodes) in the cluster that contain the Unified Intelligence Center reporting process.

A cluster can contain a maximum of eight such devices:

- One Controller (which runs both Administration and Unified Intelligence Center reporting)
- Seven Members (which run Unified Intelligence Center)

This list always contains at least one row for the Controller, added during the installation. You cannot delete the Controller from this page. To delete the Controller, you must uninstall it.

Table 6: Columns on This Page

Field	Description
Name	The name of the device. The software assigns default alias names - for the Controller, *CUIC1*; for the members, *Member1*, *Member2*, and so forth. Click the member row to edit the default aliases of members to names that are more meaningful for you.
Host Address	The IP address or Host name or FQDN for the device.
Description	The description of the device.

Field	Description
Type	The type of the device: Controller or Member. • There is only one Controller. It runs both the Administration console and Unified Intelligence Center Reporting. • There can be a maximum of seven Members. Members run the Unified Intelligence Center Reporting.

Table 7: Actions from This Page

To	Do This
Create New Device Configuration	Click **New**. For more information, see *Create or Edit Device Information*.
Delete a device	Click the Ellipsis button (...) and click **Delete** against the device member to be deleted. You cannot delete the Controller. The interface allows you to delete Members, but you must reinstall a Member device to add it back to the cluster.
Edit an existing device	Click the Ellipsis button (...) and click **Edit** against the device to be edited. *Create or Edit Device Information*.

Related Topics

Create or Edit Device Information, on page 16

Create or Edit Device Information

Use this page to define information about a new device or to edit information about an existing device.

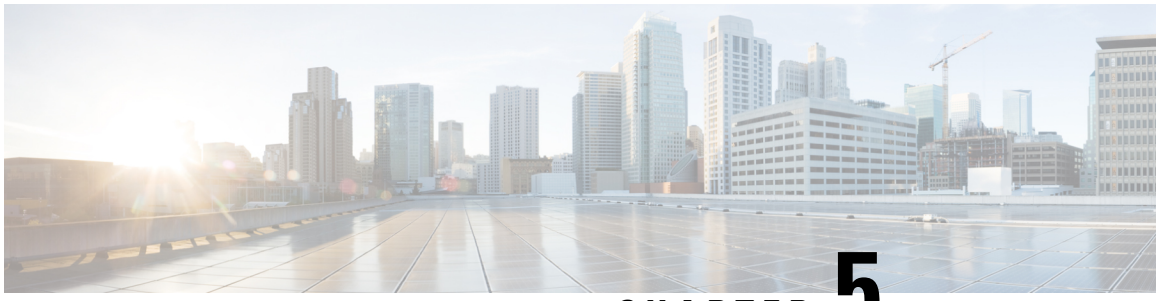
Table 8: Fields on this Page

Field	Description
Type	Displays the type of the server you are adding or editing.
Name*	The name of the device.
Host Address*	The IP address or hostname of the device. You cannot edit the IP address of the Controller on this page. You can edit the IP address of a Member on this page, but changing it here does not effect a change in the cluster. The cluster continues to recognize the original IP address for replication, and the replication will fail. For more information on the procedure to change the IP address of Unified Intelligence Center nodes in a cluster, see *Changing the IP Address and hostname in Unified Intelligence Center*.
Description	The description of the device.

Actions on this page are Save (changes) and Cancel (changes).

Related Topics

IP Address and Hostname of Cisco Unified Intelligence Center Nodes, on page 22



CHAPTER 5

Log and Trace Settings

- View List of Host Addresses for Configured Devices, on page 19
- IP Address and Hostname of Cisco Unified Intelligence Center Nodes, on page 22

View List of Host Addresses for Configured Devices

Use the **Log and Trace Settings** page to see the Host Address of OAMP server and to configure log and trace settings for this device.

The host address for the Controller displays OAMPServer process.

From the **Actions** column, click the ellipsis icon (...) to edit the Log, Syslog, and Subsystem server connection settings for that server process.

For configuring the log settings of the Unified Intelligence Center Reporting server process, see utils cuic logging, on page 107.

Logging for Unified Intelligence Center

For more information about Unified Intelligence Center logging, see utils cuic logging, on page 107.

Logging and Tracing for OAMP

Use the **Log and Trace Settings** page to configure log and trace settings for the OAMPServer.

For configuring the log settings of the Unified Intelligence Center Reporting server process, see utils cuic logging, on page 107.

Logging and Tracing are two mechanisms for application monitoring and management and are differentiated as follows:

- Logs contain predefined, higher-level messages that can indicate everything from general system behavior to severe error conditions.
- Traces are free-form, developer-oriented, detailed information that is not printed to the logs by default, but only when increased logging is enabled to debug problems.

You configure log levels to be *Basic* or *Detailed*. *Basic* is the default. When you change the log levels to *Detailed*, you have the opportunity to select specific trace level definitions.

There are two ways to review log and tracing information:

- The *Command Line Interface*. Using the show trace command.
- The *Real Time Monitoring Tool* (RTMT).

Related Topics

Real Time Monitoring Tool, on page 51
Command Line Interface, on page 99

Edit Syslog Server Connection Settings for Unified Intelligence Center

For more information about the Unified Intelligence Center logging, see utils cuic logging, on page 107.

Edit Syslog Server Connection Settings for OAMP

From the **Log and Trace Settings** list page > **Actions** column, click the ellipsis icon (...) and click **Edit** to edit the Log, Syslog, and Subsystem settings.

Caution Modify the settings on this page only under the direction of, and with the assistance of, your support provider.

Log Settings

Use the following required fields to define the maximum size of the log directory and of each log file.

Field	Description
Maximum Log Directory Size	Enter a numeric value between 50 and 50,000. The default is 1,500. When the directory size exceeds 50,000, the oldest log files are deleted.
Maximum Log File Size	Enter a numeric value between 1 and 50. The default is 50. When a log size exceeds 50, a new log file is created.

Syslog Settings

Use the following fields to identify the server where the log files are stored.

Field	Description
Primary Host	The host address of the primary syslog server that stores the log files. **Note** The port is fixed at 514.
Backup Host	The host address of the backup syslog server that stores the log files. **Note** The port is fixed at 514.

Subsystem Settings

Click the **Subsystem** tab to set the log levels for each subsystem.

Actions on this page

- **Save** - Save the changes you have made.
- **Cancel** - Undo all changes you have made since the last save.

Related Topics

View List of Host Addresses for Configured Devices, on page 19

Subsystem Trace Definitions - OAMPServer

OAMP

Operation Administration Maintenance and Provisioning (OAMP) Subsystem Specific Trace Definitions

Trace	Definition
TRACE_BULK	To control logging for looping/bulk operations
TRACE_GENERAL_UI	For tracing the general OAMP UI
TRACE_EXCEPTION	For tracing Exceptions
TRACE_PARAM	For tracing Parameters
TRACE_DBACCESS	Trace DB Access for db fetch and modify such as Save, Update, Delete
TRACE_METHOD	For tracing of Entry/Exit of Methods

OAMP-BO

OAMP-BO Subsystem Specific Trace Definitions

Trace	Description
TRACE_BULK	To control logging for looping/bulk operations
TRACE_EXCEPTION	For tracing Exceptions
TRACE_GENERAL_BO	General Traces for OAMP back-end
TRACE_PARAM	For tracing Parameters
TRACE_DBACCESS	Trace DB Access for db fetch and modify such as Save, Update, Delete
TRACE_METHOD	For tracing of Entry/Exit of Methods

WSM-BO

WSM-BO Subsystem Specific Trace Definitions

Trace	Description
TRACE_EXCEPTION	For tracing Exceptions
TRACE_GENERAL_BO	General Traces for OAMP back-end
TRACE_PARAM	For tracing Parameters
TRACE_DBACCESS	Trace DB Access for db fetch and modify such as Save, Update, Delete
TRACE_METHOD	For tracing of Entry/Exit of Methods

IP Address and Hostname of Cisco Unified Intelligence Center Nodes

Warning Perform the IP address change only during a maintenance window.

This section provides the steps to change the IP address or hostname on a Cisco Unified Intelligence Center server. You may want to change this IP address for a variety of reasons, which include moving the server from one segment to another or resolving a duplicate IP address problem.

IP Address Change Checklist

Perform the following tasks to ensure that your system is prepared for a successful IP address change.

If you have a DNS configured anywhere on the Unified Intelligence Center servers, ensure the following before changing the IP address:

- There is a forward and reverse lookup zone configured.
- The DNS is reachable and working.

Note If you do not receive the results that you expect when you perform these tasks, do not continue with this procedure until after you resolve any problems that you find.

Prepare for IP Address Change

You must perform the following tasks before changing the IP address.

Procedure

Step 1 List all servers in the cluster and note whether the nodes are defined by using IP addresses or host names.

a) From the Administration console on the first node, navigate to **Device Configuration**. System displays a list of all servers in the cluster.
b) Capture this list of servers for later reference.

Step 2 Ensure that you have saved an inventory of both the host name and IP address of each node in your cluster.

Step 3 Ensure that all servers in the cluster are up and available by checking for any active ServerDown alerts. You can check by using either the Real Time Monitoring Tool (RTMT) or the Command Line Interface (CLI) on the first node.

- To check by using RTMT, access Alert Central and check for ServerDown alerts.
- To check by using the CLI on the first node, enter the following command and inspect the application event log:

```
file search activelog syslog/CiscoSyslog ServerDown
```

Step 4 Check the DB replication status on all the Unified Intelligence Center nodes in the cluster to ensure that all servers are replicating database changes successfully. You can check by using either RTMT or a CLI command.

- To check by using RTMT, access the Database Summary and inspect the replication status.
- To check by using the CLI, enter the command that is shown in the following example:

```
admin: show perf query class "Number of Replicates Created and State of Replication"
==>query class :
- Perf class (Number of Replicates Created and State of Replication)
has instances and values:
ReplicateCount -> Number of Replicates Created = ###
ReplicateCount -> Replicate_State = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

- 0-Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service is not running and has not been running since the subscriber was installed.
- 1-Replicates have been created, but their count is incorrect.
- 2-Replication is good.
- 3-Replication is bad in the cluster.
- 4-Replication setup did not succeed.

Step 5 To check network connectivity and DNS server configuration, enter the CLI command that is shown in the following example:

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1log
Starting diagnostic test(s)
===================================
test - validate network : Passed
Diagnostics completed
admin:
```

Step 6 Run a manual DRS backup and ensure that all nodes and active services are backed up successfully. For more information, see *Disaster Recovery System*.

Related Topics

Disaster Recovery System, on page 78

Change Cluster IP Addresses for Subscriber Servers Defined by IP Addresses

Use this procedure to change the IP address of a subscriber server if your cluster servers are defined by an IP address. To successfully change the IP address, you must complete all steps in this procedure.

Procedure

Step 1 Change the IP address of the subscriber server by performing the following tasks:

Note When you are logging in to the subscriber server to perform this step, ensure that you use the original IP address of the subscriber server and not the IP address that you changed in the publisher node.

a) Enter the CLI command `set network ip eth0 ip_address netmask` where `ip_address` specifies the new server IP address and `netmask` specifies the new server network mask.

The following output displays:

```
***   W A R N I N G   ***
If there are Member(Subscriber) IP addresses (not hostnames)
configured in Cisco Unified Intelligence Center Administration
under Device Management -> Device Configuration
then you must change the IP address there BEFORE
changing it here .
This will cause the system to restart
======================================================
 Note: To recognize the new IP address all nodes within
       the cluster will have to be manually rebooted.
======================================================
```

b) Enter `Yes` and press **Enter**.

Note You can also change the IP address of the default gateway and the subscriber server by using the Cisco Unified Communications Operating System. From Cisco Unified Communications Operating System Administration, choose **Settings** > **IP** > **Ethernet**.

Step 2 If you are moving the subscriber server to a different subnet that requires a new default gateway address, change the default gateway by using the set network gateway CLI command, as shown in the following example:

```
admin: set network gateway 10.3.90.2
*** W A R N I N G ***
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to stop
yes
executing...
admin:
```

Step 3 Ensure that your updated subscriber server restarts after this step. If it does not, manually reboot the server for the changes to take effect.

Note These files get updated only during system startup; the system needs to restart core network services, a Cisco DB and Cisco Tomcat, after the files are updated. Restarting the servers ensures the proper update and service-restart sequence for the IP address changes to take effect.

Step 4 When changing the IP address of more than one subscriber server, do the following:

a) Change the IP address for one server.
b) Reboot the cluster.
c) Check the replication status.

If the changed IP address reflects properly, follow the same procedure on the next subscriber server. Otherwise do not change the IP address of the other servers.

Caution: Avoid doing the changes in parallel in several servers at the same time, as it can lead to .rhosts, sqlhosts files being out of sync in the cluster.

Change Cluster IP Address for Publisher Server Defined by IP Address

Use this procedure to change the IP address of a publisher server if your cluster servers are defined by an IP address.

Note You cannot use this procedure to change a subscriber's host publisher server from one publisher server to another publisher server.

Procedure

Step 1 From the Cisco Unified Operating System Administration window of each subscriber server in the cluster, perform the following tasks:

a) Navigate to **Settings** > **IP** > **Publisher.**
b) Change the IP address of the publisher server.

Step 2 If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the set network gateway CLI command, as shown in the following example:

```
admin: set network gateway 10.3.90.2
*** W A R N I N G ***
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to stop
yes
executing...
admin:
```

Step 3 To change the IP address of the publisher server, perform one of the following tasks:

To change the IP address from Cisco Unified Operating System Administration:

a. Choose **Settings** > **IP** > **Ethernet.**

b. Enter the new IP addresses.

c. Click **Save**. The server reboots automatically.

To change the IP address by using a CLI command

a. Enter the CLI command `set network ip eth0 ip_address netmask` where `ip_address` specifies the new server IP address and `netmask` specifies the new server network mask.

The following output displays:

```
WARNING: Changing this setting will invalidate software license
               on this server. The license will have to be re-hosted.
Continue (y/n)? Enter y
***   W A R N I N G   ***
If there are Member(Subscriber) IP addresses (not hostnames)
configured in Cisco Unified Intelligence Center Administration
under Device Management -> Device Configuration
then you must change the IP address there BEFORE
changing it here.
This will cause the system to restart.
======================================================
 Note: To recognize the new IP address all nodes within
       the cluster will have to be manually rebooted.
======================================================
Continue (y/n)?
Enter y to continue and restart at both places.
```

b. Enter **yes** and press **Enter.**

Step 4 Ensure that the IP address change is replicated to the subscriber server database by entering the CLI command run sql select * from mmca_device on all nodes in the cluster. The following example shows the command output:

```
name                nodeid
=================== ======
EnterpriseWideData    1
10.3.90.21            4
10.3.90.5             2
```

Step 5 After the publisher server reboots automatically, reboot all subscriber servers to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.

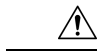
Note These files get updated only during system startup, and the system needs to restart core network services, such as Cisco DB and Cisco Tomcat, after the files are updated. Restarting the servers ensures the proper update and service-restart sequence for the IP address changes to take effect.

Step 6 Only for Virtual Machine based deployments, obtain and apply a new license for the publisher node.

Step 7 Run a manual DRS backup and ensure that all nodes and active services get backed up successfully. For more information, refer the Disaster Recovery System section.

Change Cluster IP Addresses for Subscriber Servers Defined by Host Name

Use this procedure to change the IP address of a subscriber server if your cluster servers are defined by a host name.



Caution Be aware that a DRS backup that you take from a server with a particular host name cannot be restored on a server (either a publisher or subscriber node) with a different host name, even after you reinstall that node.

Procedure

Step 1 Change the DNS record of the subscriber server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records. You must refresh your DNS cache to ensure that the records get correctly updated.

Note DNS servers comprise part of the network infrastructure. Unified Intelligence Center servers do not and cannot run DNS services.

Step 2 Verify that the DNS change propagates to other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all the cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
admin:show tech network hosts
-------------------- show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 3 If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the `set network gateway` CLI command, as shown in the following example:

```
admin:set network gateway 10.3.90.2
               *** W A R N I N G ***
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to stop
yes
executing...
admin:
```

Step 4 Change the IP address of the subscriber server by performing the following tasks:

a) Enter the CLI command `set network ip eth0 ip_address netmask` where `ip_address` specifies the new server IP address and `netmask` specifies the new server network mask.

The following output displays:

```
*** W A R N I N G ***
```

```
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
======================================================
Note: To recognize the new IP address all nodes within
the cluster will have to be manually rebooted.
======================================================
Do you want to continue?
Enter "yes" to continue and restart or any other key to stop
```

b) Enter `yes` and press **Enter**.

Note You can also change the IP address of the default gateway and the server by using the Cisco Unified Communications Operating System. From Cisco Unified Communications Operating System Administration, choose **Settings** > **IP** > **Ethernet**.

Step 5 Reboot all other servers in the cluster, including the publisher server, to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.

Note These files only get updated during system startup; you need to restart core network services, such as Cisco DB and Cisco Tomcat, after the files are updated. Restarting the servers ensures that the proper update and service-restart sequence for the IP address changes take effect.

Step 6 Do the following if you want to change the IP address of more than one subscriber server:

a) Change the IP address for one server.
b) Reboot the cluster.
c) Check the replication status. If the changed IP address reflects properly, follow the same procedure on the next subscriber server. Otherwise do not change the IP address of the other servers.

Warning Avoid making the changes in parallel in several servers at the same time, because doing so can lead to .rhosts, sqlhosts files being out of sync in the cluster.

Step 7 Verify that the DNS change propagates to other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all the cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
admin:show tech network hosts
-------------------- show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 8 Run a manual DRS backup and ensure that all nodes and active services get backed up successfully. For more information, refer the Disaster Recovery System section.

Change Cluster IP Address for Publisher Server Defined by Host Name

Use this procedure to change the IP address of a publisher server if your servers are defined by a host name.

Caution Be aware that a DRS backup that you take from a server with a particular host name cannot be restored on a server (either a publisher or subscriber node) with a different host name, even after you reinstall that node.

Procedure

Step 1 Change the DNS record of the publisher server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records.

Note DNS servers comprise part of the network infrastructure. Unified Intelligence Center servers do not and cannot run DNS services.

Step 2 Verify that the DNS change propagates to other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all the cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
admin:show tech network hosts
-------------------- show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 3 From the Cisco Unified Communications Operating System Administration window (`https://subscriber_ip_address/cmplatform`) of each subscriber server in the cluster, perform the following tasks:

a) Navigate to **Settings** > **IP** > **Publisher**.
b) Change the IP address of the publisher server.

Step 4 If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the `set network gateway` CLI command, as shown in the following example:

```
admin:set network gateway 10.3.90.2
*** W A R N I N G ***
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to stop
yes
executing...
admin:
```

Step 5 Change the IP address of the publisher server by using the CLI by performing the following tasks:

a) Enter the complete CLI command `set network ip eth0 ip_address netmask gateway` where `ip_address` specifies the new server IP address, `netmask` specifies the new server network mask and `gateway` specifies the new server network gateway.

The following output displays:

```
*** W A R N I N G ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
======================================================
Note: To recognize the new IP address all nodes within
the cluster will have to be manually rebooted.
======================================================
Do you want to continue?
Enter "yes" to continue and restart or any other key to stop
```

b) Enter `Yes` and press **Enter**.

Note You can also change the IP address of the default gateway and the server by using the Cisco Unified Communications Operating System. From Cisco Unified Communications Operating System Administration, choose **Settings** > **IP** > **Ethernet**.

Step 6 After the publisher server reboots automatically as a result of the `set network ip` command, reboot all subscriber servers to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.

Note These files only get updated during system startup, and you need to restart core network services, such as Cisco DB and Cisco Tomcat, after the files are updated. Restarting the servers ensures that the proper update and service-restart sequence for the IP address changes take effect.

Step 7 Ensure that local resolution of the subscriber node also resolves to the new IP address by running the `utils network host` and `show tech network hosts` CLI commands:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
admin:show tech network hosts
-------------------- show platform network --------------------
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
```

```
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 8 Run a manual DRS backup and ensure that all nodes and active services get backed up successfully. For more information, see *Disaster Recovery System*.

Related Topics

Disaster Recovery System, on page 78

Change Hostname for Unified Intelligence Center Publisher (Controller) Node

This section describes how to change the hostname for the Unified Intelligence Center Publisher (Controller) Node that is defined by an IP address.

Procedure

Step 1 Change the DNS record of the subscriber server to point to the new IP address. If the IP address is being changed at the same time, ensure that the DNS servers also reflect the IP address. Ensure that forward (A) and reverse (PTR) records update correctly.

Note: DNS servers comprise part of the network infrastructure. Unified Intelligence Center servers don't and can't run DNS servers.

Step 2 If the server for which you're changing the hostname is a publisher server, log on to each subscriber server in the cluster and change the hostname mapping of the cluster Publisher server. You can perform this task from Cisco Unified Operating System Administration or by using a CLI command.

To change the mapping from Unified Intelligence Center Operating System Administration, log in to each subscriber server in the cluster and perform the following tasks:

Step 3 Change the hostname of the server from Cisco Unified Operating System Administration:

a) Navigate to **Settings** > **IP** > **Ethernet**.
b) Change the hostname to the new hostname.
c) Click **Save**. The server automatically reboots with the new changes.

Note Changing the hostname triggers an automatically self-signed certificate regeneration. If your cluster is using CA-signed certificates, you must have them re-signed. For regenerating SAML certificate, refer to the **Hostname or IP Address Change** section in the Cisco Unified Contact Center Enterprise Features Guide.

Step 4 If the IP address changes along with the hostname and the server moves to a new subnet, change the server Default Gateway to the new address by using the `set network gateway ip address` CLI command.

If the default gateway changes, before the next step, ensure that the server moves to the new subnet and has access to the default gateway. During Unified Intelligence Center server startup, the Verify Network script checks server access to the default gateway. If the server can't communicate with the default gateway at startup time, the Verify Network script fails and start up may be delayed. If you're using Manual DHCP configuration

and the DHCP server isn't reachable or doesn't give out an IP address to the server, the system won't boot; instead, the system continues to wait at the Verify Network startup phase.

Step 5 Reboot all other servers in the cluster twice, including the publisher.

Step 6 Verify that the name-IP association change that was made in Step 4 propagates to the other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all cluster nodes.

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
admin:show tech network hosts
-------------------- show platform network -------------------- /etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

You can also use the `utils diagnose module validate_network` command on all cluster nodes. This diagnostics module checks that you configured DNS client services correctly, that the server can connect to the DNS server, and that Forward (A) and Reverse (PTR) records are present and match the server IP address and hostname.

Note Don't proceed until the change propagates to all nodes.

Step 7 From the publisher server, run the CLI `utils dbreplication stop all` to stop the automatic setup of database replication and to stop ongoing setup of replication.

Step 8 For all the nodes in the cluster, run `utils dbreplication dropadmindb`.

Step 9 From the publisher server, run `utils dbreplication reset all` to set up replication across the whole cluster again.

Change Hostname for Unified Intelligence Center Subscriber (Member) Node

This section describes how to change the hostname for Unified Intelligence Center Subscriber (Member) Nodes that are defined by an IP address in Unified Intelligence Center.

Procedure

Step 1 Change the DNS record of the subscriber server to point to the new IP address. If the IP address is being changed at the same time, ensure that the DNS servers also reflect the IP address. Ensure that forward (A) and reverse (PTR) records update correctly.

Note DNS servers comprise part of the network infrastructure. Unified Intelligence Center servers do not and cannot run DNS services.

Step 2 To change the hostname of Unified Intelligence Center subscriber (Member) node, log in to Cisco Unified Operating System Administration page on each subscriber node in the cluster and perform the following tasks:

a) Navigate to **Settings** > **IP** > **Ethernet**.
b) Change the hostname to the new hostname.
c) Click **Save**. The server automatically reboots with the new changes.

Step 3 To change the hostname using a CLI command:

a) Enter the CLI command `set network hostname hostname`.
b) Enter **Yes** and press **Enter**. This command automatically reboots this server with the new hostname.

Step 4 Reboot all other servers in the cluster twice, including the publisher.

Step 5 Verify that the name-IP association change that was made in Step 3 propagates to the other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all cluster nodes.

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11admin
.
.
.
cups114.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Note You can also use the `utils diagnose module validate_network` command on all cluster nodes. This diagnostics module checks that you configured DNS client services correctly, that the server can connect to the DNS server, and that Forward (A) and Reverse (PTR) records are present and match the server IP address and hostname.

Note Do not proceed until the change propagates to all nodes.

Step 6 From the publisher server, run the CLI `utils dbreplication stop all` to stop the automatic setup of database replication and to stop ongoing setup of replication.

Step 7 From the publisher server, run `utils dbreplication reset all` to set up replication across the whole cluster again.

Verify IP Address Change

After you finish changing the IP addresses of your cluster, complete the following tasks.

Procedure

Step 1 Ensure that all servers in the cluster are up and available by checking for any active ServerDown alerts. You can check by using either the Real Time Monitoring Tool (RTMT) or the Command Line Interface (CLI) on the first node.

a) To check by using RTMT, access Alert Central and check for ServerDown alerts.
b) To check by using the CLI on the first node, enter the following command and inspect the application event log: `file search activelog syslog/CiscoSyslog ServerDown`

Step 2 Check the DB replication status on all Unified Intelligence Center nodes in the cluster to ensure that all servers are replicating database changes successfully. You can check by using either RTMT or a CLI command.

To check by using RTMT, access the Database Summary and inspect the replication status.

To check by using the CLI, enter the command that the following example shows:

```
admin: show perf query class "Number of Replicates Created and State of Replication"
==>query class :
- Perf class (Number of Replicates Created and State of Replication)
has instances and values:
ReplicateCount -> Number of Replicates Created = 344
ReplicateCount -> Replicate_State = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

- 0 - Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service has not been running since the subscriber was installed.
- 1- Replicates have been created, but their count is incorrect.
- 2 - Replication is good.
- 3 - Replication is bad in the cluster.
- 4 - Replication setup did not succeed.

Step 3 Run a manual DRS backup and ensure that all nodes and active services backed-up successfully.

Step 4 Update RTMT custom alerts and saved profiles:

- RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure these custom alerts.
- RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and re-add these counters and then save the profile to update it to the new IP address.

Configure IPv6

Cisco Unified Intelligence Center supports IPv6 using dual stack (IPv4 and IPv6). You can enable IPv6 after installation using the either Cisco Unified Communications Operating System Administration or CLI.

With IPv6 enabled, the Unified Intelligence Center Administration Console and REST APIs can connect to the Unified Intelligence Center server using IPv4 or IPv6.

Note After installation, if you are not using IPv6 or IPv6 address is not assigned, disable the IPv6 service.

Set up IPv6 using CLI

To set up IPv6 using the CLI, perform the following procedure on the primary and secondary servers of Unified Intelligence Center.

Procedure

Step 1 Access the CLI on the Unified Intelligence Center server.

Step 2 To enable or disable IPv6, enter: **set network ipv6 service {enable | disable}**.

Step 3 Set the IPv6 address and prefix length : **set network ipv6 static_address** *addr mask*. Example: set network ipv6 static_address 2001:db8:2::a 64

Step 4 Set the default gateway : **set network ipv6 gateway** *addr*

Step 5 Restart the system for the changes to take effect : **utils system restart**

Step 6 To display the IPv6 settings, enter : **show network ipv6 settings**

The IPv6 configured is global.

Set up IPv6 using Cisco Unified Communications Operating System Administration

To set up IPv6 using Cisco Unified Operating System Administration, perform the following procedure on both the primary and secondary Unified Intelligence Center servers.

Procedure

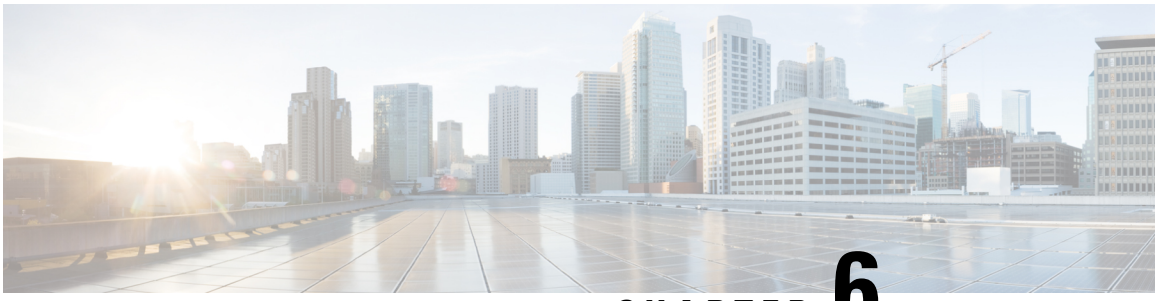
Step 1 Sign in to Cisco Unified Operating System Administration on the Unified Intelligence Center server (https://*host or IP address*/cmplatform, where *host or IP address* is the hostname or IP address of the Unified Intelligence Center server).

Step 2 Navigate to **Settings** > **IP** > **Ethernet IPv6**.

Step 3 To enable IPv6, check the **Enable IPv6** check box (or uncheck the box to disable IPv6).

Step 4 Enter values for **IPv6 Address**, **Subnet Mask**, and **Default Gateway**.

Step 5 To restart after you save the changes, check the **Update with Reboot** check box. Click **Save**



CHAPTER 6

Control Center

• Control Center , on page 37

Control Center

Choose **Control Center** from the navigation menu to open the Control Center page, where you can check the status of each device, and start, stop, or restart devices.

As soon as you add a device on the **Device Configuration** page (see *Device Configuration*), this **Control Center** page also shows a row for that Cisco Unified Intelligence Center Reporting Server device.

Table 9: Rows on This Page

Field	Description
Name	The name of the device. For the Controller, this field is populated by default. For each member, this field shows the name of the device from the Device Management page.
Host Address	The IP address for the device.
Device Type	A description of the device (Controller or Member).
Status	The current state of the device. Possible values are: • Starting - the server is in the process of starting up. • Unknown - the server or subsystem that communicates with the Administration Console could not be reached. • Stopped - the server is not running. • Running (in service) - the server is running and active. • Running (partial service) - the server is running, but is not ready to work. The server may be starting up. • Stopping - the server is in the process of stopping.

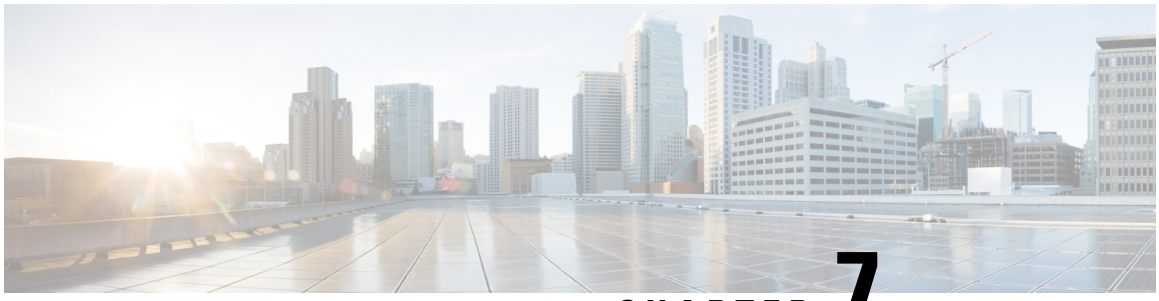
Actions from this page

Note Start, Shutdown, and Restart refer to the application process running on the server, and not the hardware or operating system.

To	Do This
Start	Start the device.
Shutdown	Shut down the device. Respond **OK** or **Cancel** to the confirmation message.
Restart	Restart the device.

Related Topics

Device Configuration, on page 15



CHAPTER 7

Cluster Configuration

- Configure Active Directory Settings, on page 39
- Configure SMTP Settings, on page 43
- Unified CCE User Integration, on page 45
- Cluster Configuration for JVM Using Hazelcast, on page 47
- Troubleshooting Cluster Configuration, on page 49

Configure Active Directory Settings

Fields on the Active Directory tab configure the Active Directory server to authenticate reporting users as they log in to the Unified Intelligence Center Web application.

Configure Active Directory for the Unified ICM/CC supervisors so that they can sign in as Unified Intelligence Center Reporting users.

Note Cisco Unified Intelligence Center uses LDAP V2 which does not support all Unicode characters that are used in the first name or surname of LDAP users.

Active Directory is not used to authenticate Administration Super Users. These Super Users can only be authenticated through the local database. The first Super User is added during installation. All other Super Users are added through the **User Management** interface, and their credentials are encrypted into the local database.

To navigate to this page, choose **Cluster Configuration** > **Active Directory Settings**.

Table 10: Fields on This Tab

Field	Description
Host Address and Port for Primary Active Directory Server	Provide the hostname or IP address and the port of the Primary Active Directory server. The port defaults to 389.

Field	Description
Host Name and Port for Secondary Active Directory Server	Provide the hostname or IP address and the port of the Secondary Active Directory server. The port defaults to 389.
Use SSL	Check these boxes if you want the connection from the Unified device to the Active Directory connection to be encrypted with SSL while doing authentication.
Manager Distinguished Name	Enter the Manager Distinguished Name used to sign in to the Active Directory server. For example, on a default installation of Microsoft AD: `CN=Administrator, CN=users, DC=MYSERVER, DC=COM`. Replace *MYSERVER* and *COM* with your respective hostname. **Note** If users other than the LDAP administrator are configured as Manager Distinguished Name in the OAMP LDAP configurations, they should have the following rights: 1. User search permissions on the domain. 2. Read access to the user objects and their attributes. 3. Read access to the base DN 4. Permission to bind to LDAP.
Manager Password	Enter the Active Directory manager password.
User Search Base	Specify the user search base. For example, on a default installation of Microsoft AD, `CN=users, DC=MYSERVER, DC=COM`, replace *MYSERVER* and *COM* with your respective hostname. **Note** This example assumes that you placed the users in the USERS subtree of AD. If you created a new organizational unit within your subtree, then the syntax would be: `OU=MYUSERS, DC=MYSERVER, DC=COM`, instead of "CN=MYUSERS".

Field	Description
Attribute for User ID	Whenever a user signs in, Unified Intelligence Center searches for that user in the LDAP (Lightweight Directory Access Protocol) using the sign-in attribute specified in the LDAP configuration. After the user is found, the full DNS of the user is extracted and used for authenticating the user. The sign-in attribute specified in the LDAP configuration is the property against which LDAP search is issued to find the matching username. If you do not know which attribute to use, use *sAMAccountName*, which is the default Microsoft username attribute. Different organizations settle on different LDAP attributes to identify the username across the organization, depending on the tools used to administer LDAP within their organizations. This attribute allows you to customize the sign-in depending on the attribute used. Even a custom attribute can be specified using this dialog. *sAMAccountName* indicates the user attribute to search the user for is the *userPrincipalName*. *sAMAccountName* contains just the short username. For example, jDoe for the user John Doe. *userPrincipalName* indicates the user attribute to search the user for is the *userPrincipalName*. This attribute contains the username in the email format, **`user@compay.com`**. This entire string becomes the username and not just user. Therefore when this attribute is selected, the user has to type the full email format in as the username in the sign-in box. **Custom User Attribute** allows you to specify the attribute used for searching the user in LDAP. **Note** Custom User attributes are not validated and are used as is. Ensure that the correct case and attribute name are used. Contact your Active Directory Administrator for the correct attribute to use.

Field	Description
User Name Identifiers	Users are stored in Unified Intelligence Center in the format <UserName Identifier>\<username> The username Identifiers are used to identify the different kinds of users within Unified Intelligence Center. For example, local, LDAP, user-synced user, users from different LDAP domains, nETBIOSName, and so on. Before you can use it, the username identifier has to be declared for use on this page. When LDAP is configured, at least one identifier must be configured and set as default to enable the system to identify LDAP users. UserSychronization brings in users in format <syncdomain>\username and collections have users in the same format. Therefore, these users must sign in to Unified Intelligence Center using the <syncdomain>\user syntax. To enable, add <syncdomain> or @<syncdomain> (if you are using *userPrincipalName*) to the list of valid identifiers. The maximum allowed length of a username identifier is 128 characters. **Example:** When nETBIOSName and userPrincipalName are same or different: *For sAMAccountName:* Configure in Username Identifiers: <UserNameIdentifier> Login in cuic : UserNameIdentifier\user *For userPrincipalName:* Configure in Username Identifiers: @<UserNameIdentifier> Login in cuic : userPrincipalName This list box is pre-populated with the username Identifiers based on the list of usernames stored in the Unified Intelligence Center database. The most frequently occurring identifier in the list of username is auto-selected as the default. **Note** You cannot save LDAP configuration unless you choose a default Identifier from the **User Name Identifiers** list box and clicking the **Set Default** button.
Default User Name Identifier	Default identifiers allow users to sign-in without typing the full domain identifier (<domain>\user) or the *userPrincipalName* suffixes to usernames (user <@company.com>) on the sign-in page. It can be set by choosing one of the Identifiers from the list box and by clicking the **Set Default** button. Users who use any other identifier can still sign-in by typing their full identifier in the sign-in box. For example, domain2\user or netbiosname\user, provided those identifiers are already configured.

Field	Description
Test Connection	Click to test the connection to the primary and secondary LDAP servers and display the connection status.

- **Save** saves the configuration information you entered for the Active Directory. Clicking **Save** *does not validate the configuration*.

Configure Active Directory with SSL

Perform the following steps if you want the connection from the Unified Intelligence Center to the Active Directory server to be encrypted with SSL while doing authentication.

Procedure

Step 1 Perform the tasks outlined in the Microsoft Active Directory documentation to set up and generate the Certificate Authority.

Step 2 Save the certificate in *Base-64 encoded X.509 (CER)* file format.

Step 3 Log in to the Cisco Unified Operating System Administration User Interface.

Step 4 From the **Security** menu, select **Certificate Management**.

Step 5 Select the certificate name as `tomcat-trust`.

Step 6 Click **Browse** to browse and select the certificate that you have generated from the AD server.

Note You can leave the **Root Certificate** field as blank. This is an optional field.

Step 7 Click **Upload File** to upload the certificate.

Step 8 Use the `utils service restart Cisco Tomcat` and the `utils service restart Intelligence Center Reporting Service` CLI commands to restart the *Cisco Tomcat* and *Intelligence Center Reporting* services respectively.

Configure SMTP Settings

Use SMTP Settings to configure the email server used to email scheduled reports.

The actual schedules for reports (for example, schedule daily at 10AM) are defined and maintained from the Unified Intelligence Center web application. The report scheduler emails scheduled reports at the exact time they are scheduled.

To navigate to this page, choose **Cluster Configuration** > **SMTP Settings**.

Table 11: Fields on This Tab

Field	Description
SMTP Host Name / IP Address	Enter the Hostname or IP address of the SMTP Server.

Field	Description
From Email Address	Enter the email address that is to appear in the From field of emails sent by the Scheduler.
Use SMTP Authentication	Check this if your SMTP server expects to receive username / password credentials.
SMTP User Name	If you check the **Use SMTP Authentication** check box, enter the user name that is to be authenticated.
SMTP Password	If you check the **Use SMTP Authentication** check box, enter the password that is to be authenticated.
Test Connection	Click to test the connection. Unified Intelligence Center attempts to send an email to check for open connections. The connection status displays next to the button.

- **Save** saves the configuration information you entered for SMTP settings.

Note Clicking **Save** *does not validate the configuration*. Use the **Test Connection** button to test the connection.

Note To manage the TLS version used by Unified Intelligence Center to connect with the SMTP server, refer **set tls client min-version**. By default, it uses TLSv1.2. For more information, see Set Commands, on page 147.

Upload Self-Signed Certificates

If you are using a self-signed certificate in your email server, upload the certificate to **tomcat-trust** using *cmplatform*. Perform the following steps:

Procedure

Step 1 Log in to *cmplatform* and navigate to **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate Chain**. The **Upload Certificate/Certificate Chain** dialog box opens.

Step 3 To upload the certificate chain, select **tomcat-trust** from the **Certificate Purpose** list.

Step 4 Select the file to upload. Click the **Choose File** button and navigate to the file; then, click **Open**.

Step 5 Click **Upload File**.

Step 6 Use the `utils service restart Cisco Tomcat` and the `utils service restart Intelligence Center Reporting Service` CLI commands to restart the *Cisco Tomcat* and *Intelligence Center Reporting* services respectively.

Unified CCE User Integration

Note The **UCCE User Integration** option is not applicable for Packaged CCE deployments.

The Unified CCE User Integration feature imports supervisors and their teams from Unified ICM/CCE from the Unified ICM Configuration Manager and database into Unified Intelligence Center.

Supervisors are automatically given Unified Intelligence Center user roles and can log in to Unified Intelligence Center to access collections for - and run reports for - their agent team(s).

Note There are five tasks in the initial setup for Unified CCE User Integration. Some are performed in the Administration interface. Some are performed in the Reporting interface. As Super Users have access to both interfaces, it is efficient for a Super User to set up Unified CCE User Integration.

- Enable Unified CCE User Integration in the Administration interface.
- Complete the configuration of the Unified CCE Historical Data Source in the **Configure** > **Data Sources** of the Reporting Interface.
- Synchronize Users in the Administration Interface.
- Validate Collections of Agents and Agent Teams in the Reporting Interface.
- Set up a synchronization schedule in the Administration Interface.
- Integrated Supervisors can sign in to Unified Intelligence Center Reporting (provided their Active Directory authentication has been configured.
- Integrated Supervisors are added to the Unified Intelligence Center Reporting User List with the User Roles of Report Designer and Dashboard Designer.
- The Unified Intelligence Center Value Lists page is updated with *Agents* and *Agent Teams* collections.
- Integrated Supervisors can view their *Agents* and *Agent Teams* collections (**Unified Intelligence Center Reporting** > **Value Lists**).
- Integrated Supervisors are granted permissions to *Agents* and *Agent Teams* collections only .

After Unified CCE User Integration schedule is set up, Unified Intelligence Center is updated with changes to supervisors and their teams every time the synchronization updates.

Note Renaming an existing Unified CCE user to a name that is identical to the locally created Unified Intelligence Center user and performing user integration results in the following:

- All the entities that are owned by the locally created Unified Intelligence Center user are assigned to the synched Unified CCE user in Unified Intelligence Center.
- The locally created Unified Intelligence Center user is deleted.

Related Topics

Configure Unified CCE User Integration, on page 46

Configure Unified CCE User Integration

Note After upgrading to Cisco Unified Intelligence Center 12.6, perform the User Integration operation (Cluster Configuration > UCCE User Integration) manually to import the Supervisors with the required roles. This setting is required to view gadgets in the Cisco Finesse Desktop for Supervisors.

If the changes made to the Supervisors or teams are to be reflected immediately, then manually synchronize using the **Synchronize Now** option.

To navigate to this page, choose **Cluster Configuration** > **UCCE User Integration**.

The User Integration feature facilitates the automatic import of reporting supervisors who are added or modified in Unified ICM Configuration Manager and stored in the Unified ICM/CCE/CCH database.

Once integrated (imported), supervisors are added as users to the Unified Intelligence Center database and can sign into Unified Intelligence Center with their User ID and Password. They are created as users in Unified Intelligence Center with the User Roles of Dashboard Designer and Report Designer and with the rights to view the collection(s) for their agent team(s).

When Unified CCE User Integration runs, data is retrieved from the Unified CCE Data Source and two stock Value Lists (Agents and Agent Teams) are updated.

Warning Schedule Unified CCE User Integration at off-peak hours and several hours after the database purge. By default, the purge runs at midnight (12:00:00 AM). Database tables are locked during the purge and are unlocked when the purge completes. If the Unified CCE User Integration runs at the same time as the purge, the user integration will fail.

Table 12: Fields on this Tab

Field	Description
Enable UCCE User Integration at...	Check this to: • Enable Unified CCE User Integration • Set the time and the day of week when it is to occur. **Note** Leave this field blank if you do not want to run Unified CCE User Integration. For more information, see *Unified CCE User Integration*.
Hour | Minute | AM or PM	Click the arrows to the right of the Hour, Minute, and AM|PM fields to select the time of day you want the Unified CCE Integration synchronization to occur.

Field	Description
Day of the week	Select one, several, or all days that you want the Unified CCE User Integration synchronization to occur.
Last Run Status	Shows the status of the last synchronization. Shows PENDING if the that synchronization is still in progress.
Duration (HH:MM:SS)	Shows how long the synchronization process took.
Unified CCE Supervisors imported	Shows the number of new supervisors imported since the last import. You can view supervisors on the **Configure** > **Users** in the Unified Intelligence Center Reporting Interface . Supervisors are imported with their Active Directory credentials and can sign in to Unified Intelligence Center Reporting with those credentials.
Team Collections Updated	Shows a count of all teams updated. Teams are re-synchronized on each run. Supervisors can view their Agents and Agent Teams collections in Value Lists in the Unified Intelligence Center Reporting interface.
Synchronize Now	Click this to run the user integration immediately. If the scheduled integration is configured to run later in the day, this action runs the job now and still runs it at the scheduled time. Clicking this button changes its appearance to *Cancel Active Synchronization*. A message appears if another user is already running a synchronization.
Save	Click to save your time and date settings.

Cluster Configuration for JVM Using Hazelcast

Cisco Unified Intelligence Center uses Hazelcast for application clustering. Hazelcast provides a second-level cache for the Unified Intelligence Center application layer. When any entity (for example: report, report definition, and so on) cached by Hazelcast is updated in one of the Unified Intelligence Center nodes, it must be invalidated and reloaded in all the other Unified Intelligence Center nodes in the cluster. The Hazelcast cluster automatically takes care of it by publishing clusterwide notifications containing the identifiers of such entities which must be invalidated.

In Unified Intelligence Center, the default mechanism for Hazelcast cluster discovery or formation is UDP multicast. Unified Intelligence Center uses the Multicast group IP address 224.2.2.3 and port 54327. You cannot change these settings in Unified Intelligence Center.

The UDP multicast based discovery mechanism will not work for the customer in the following scenarios:

- When the network has multicasting disabled.
- If the nodes in the Unified Intelligence Center cluster are in different subnets.

In such scenarios, you can change the discovery mechanism to TCP/IP. You can form the CUIC application cluster using TCP/IP instead of the default UDP Multicast based discovery mechanism.

Use the following CLI commands to manage the cluster mode (UDP Multicast vs TCP/IP). That is, use the following CLI commands to switch to TCP/IP only if the customer's network does not support Multicasting:

- **utils cuic cluster show**—This command shows the current cluster mode that is enabled on this node and the other member details.

Note The member details are available only in the TCP/IP mode. The member details displayed are of the configured members and does not represent the cluster in real time.

- **utils cuic cluster mode**—This command is used to switch the Hazelcast cluster join configuration from Multicast to TCP/IP and the opposite way.

Note After changing the cluster mode in all the nodes, restart "Intelligence Center Reporting Service" in all the nodes starting from the publisher sequentially.

- **utils cuic cluster refresh**—This command refreshes the cluster member information only when run in the TCP/IP mode. Run this command when there is an addition or deletion of nodes to the CUIC cluster, which is already in TCP/IP.

Usage

You can use these commands using to switch to TCP/IP only when the customer's network does not support the Multicasting requirements that are specified in *Port Utilization Guide for Cisco Unified Contact Center Solutions* > *Intracluster Ports Between Cisco Unified Intelligence Center* section available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Note

- Stop the "Intelligence Center Reporting Service" on all the Unified Intelligence Center nodes before performing cluster configuration changes using these CLI commands.
- When you have completed the cluster configuration changes on all nodes, use the "utils cuic cluster show" command to ensure that all nodes have identical configuration before starting "Intelligence Center Reporting Service" on any one of them.
- Unified Intelligence Center cluster / application will work only if all the nodes use the same mode–that is, either Multicast or TCP/IP. Mixed mode is not allowed.
- If the network is disconnected and after the cluster nodes retain the network, ensure to perform "synchronize cluster" from all the nodes after logging into the Unified Intelligence Center reporting application.

Steps

Run the following CLIs on all nodes in the given sequence starting from the Publisher node:

Note Run every step on all nodes before performing the subsequent step.

Procedure

Step 1 utils service stop Intelligence Center Reporting Service

Step 2 utils cuic cluster mode

Step 3 utils cuic cluster show

Note Ensure that all nodes have identical configuration.

Step 4 utils service start Intelligence Center Reporting Service

Troubleshooting Cluster Configuration

Verify the Hazlecast Cluster Formation using Hazelcast REST client. To verify, replace <CUIC-IP> with the IP address of any CUIC member in the following URL.

http://<CUIC-IP>:57011/hazelcast/rest/cluster

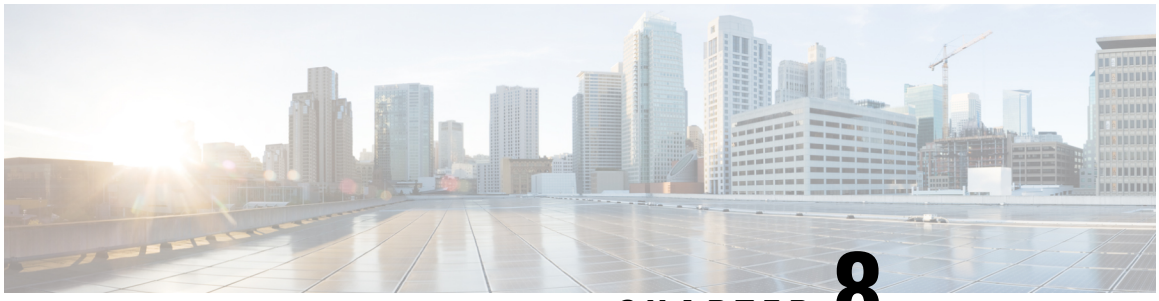
The Unified Intelligence Center application cluster can be down in the following cases:

- Common Cases:
  - Node is not reachable
  - Unified Intelligence Center Reporting Service is down
  - Member/subscriber node is added in OAMP and the node installation is in progress
  - Hazelcast default Port 57011 is not enabled in Unified Intelligence Center nodes in the customer environment, which is used to communicate between cluster members.
- When multicasting is being used for the member discovery (Default method):
  - Network has UDP multicast disabled
  - UDP port 54327 used for Hazelcast member discovery is disabled
  - Multicast default group IP 224.2.2.3 is not allowed in the network
  - CUIC nodes are distributed across different subnets

Note If any of the above mentioned cases cause issue because of the restrictions on multicasting in the customer environment, you can use TCP/IP for Hazelcast discovery.

- When TCP/IP is being used for the member discovery:
  - Member/subscriber node is added in OAMP, but the cluster mode in the newly added node is not switched to TCP/IP from the default method ‘multicasting’.

For more information, contact Cisco support to troubleshoot and reset the cluster.



CHAPTER 8

Tools

- Real Time Monitoring Tool, on page 51
- Disaster Recovery System, on page 78
- Network Management, on page 84
- Cisco Unified Intelligence OS Administration, on page 93

Real Time Monitoring Tool

For Cisco Unified Intelligence Center, Live Data, and Cisco Identity Service (Cisco IdS), download the Real Time Monitoring Tool (RTMT) from the Cisco Unified Intelligence Center Administration page (**Tools > RTMT Plugin Download**).

Live Data and the Cisco IdS do not host the RTMT installer. For this reason, always connect to the Cisco Unified Intelligence Center Server and sign in to the Administration page to download the RTMT installer. You can, however, run the same RTMT client to connect to any of the Cisco Unified Intelligence Center, Live Data, or Cisco IdS servers (standalone or coresident).

RTMT runs as a client-side application. You can install RTMT on a Windows workstation or a Linux machine. RTMT is cluster-aware. RTMT provides critical service and performance monitoring (perfmon), trace/log collection and viewing, and Alert Management on the node for the IP address you request at launch. RTMT does not provide the status of all critical applications on all the nodes at the same time.

Use RTMT to:

- Monitor the health of the system by generating email alerts for objects whose values go above or below a threshold
- Collect and view traces
- View syslog messages
- Monitor performance counters

RTMT has extensive online help. Refer to it for information on alerts, schedule collection, performance monitoring, and collecting and downloading tracing and logging data.

Launch RTMT

Procedure

Step 1 In the left navigation pane, choose **Tools** and then click **RTMT Plugin Download**.

Step 2 In the **RTMT Plugin** dialog box:

a) Select the **Windows** platform.
b) Click **Download.**
c) Run the file or save the **CuicServRtmtPlugin** executable file and then run it from the saved location.
d) Follow the prompts and click the buttons on the installation screens.

Step 3 To launch:

a) Launch RTMT from the desktop icon.

Figure 1: RTMT Desktop Icon

b) In the **Host IP Address** field, enter the IP address for the node you want to monitor.
c) Accept the default port (8443).
d) Check **Secure Connection**. You see an error if the Host IP Address is not found or there is no network connection.
e) Click **Yes** to accept the certificate.
f) Enter the **User Name** and **Password** for a Super User. (Only a Super User can install RTMT.)
g) Click **OK** to accept the default configuration.

RTMT Client Support Services

RTMT uses the following services/servlets:

- Cisco AMC service
- Cisco CallManager Serviceability RTMT
- Cisco RIS Data Collector
- Cisco Tomcat Stats Servlet
- Cisco Trace Collection Service
- Cisco Log Partition Monitoring Tool
- Cisco SOAP-Real_Time Service APIs
- Cisco-SOAP-Performance Monitoring APIs
- Cisco RTMT Reporter Servlet

RTMT Integration

Tracing and Logging

To expose tracing and logging information go to RTMT **Tools** > **Trace & Log Central** . The RTMT tool gives you the ability to browse through a trace file and supports on-demand or scheduled downloading of the file.

Figure 2: RTMT TraceLog for CUIC

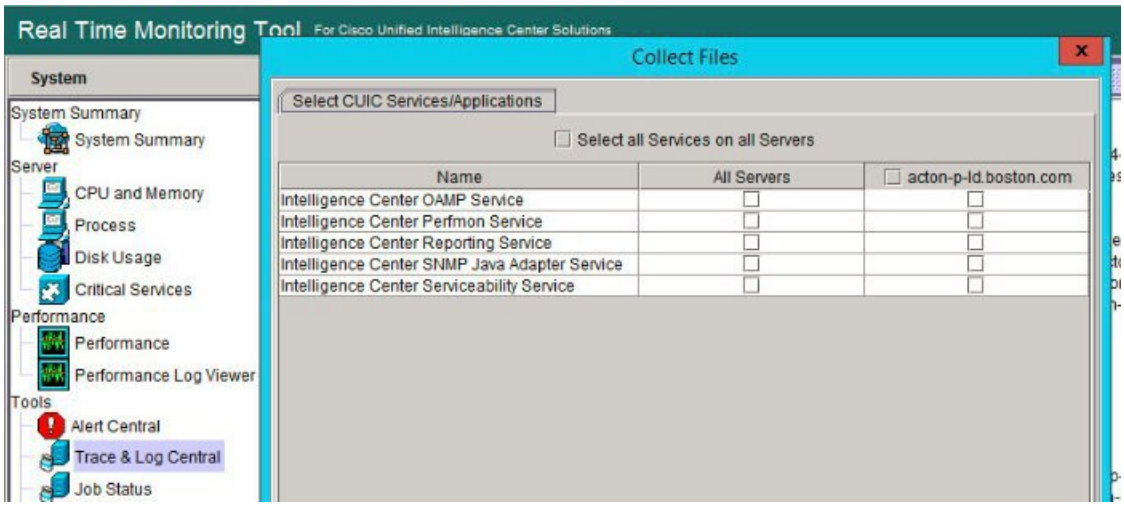
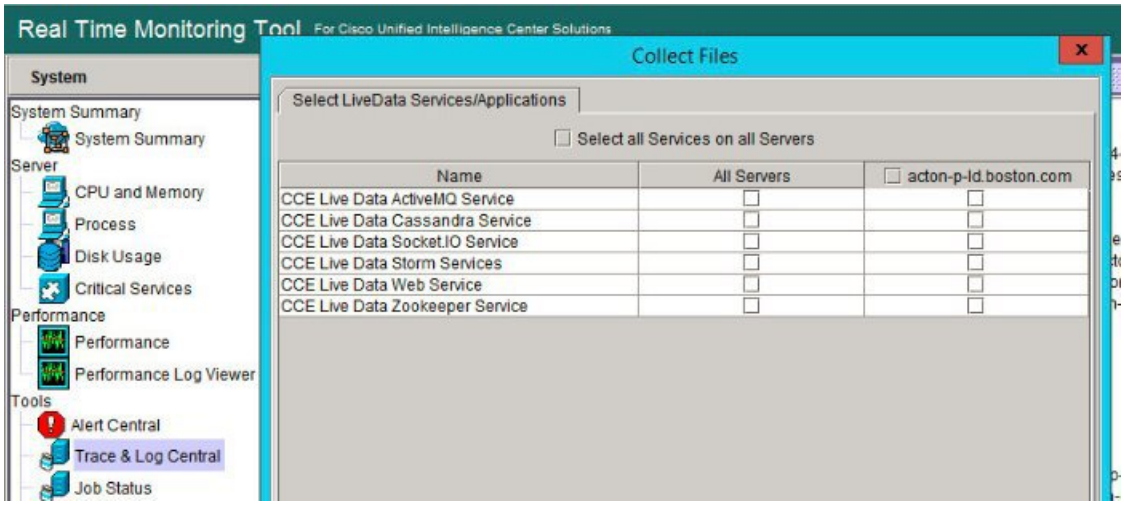


Figure 3: RTMT TraceLog for Live Data



Critical Services

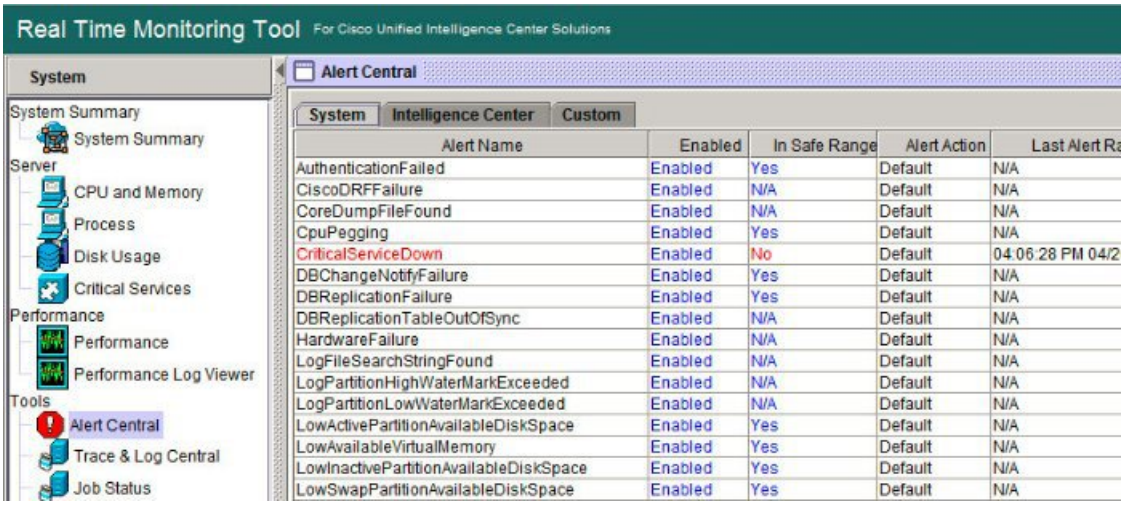
To expose service information go to RTMT **Server** > **Critical Services**.

Figure 4: RTMT Critical Services

Alerts

To expose Alert Central go to RTMT **Tools** > **Alert Central** .

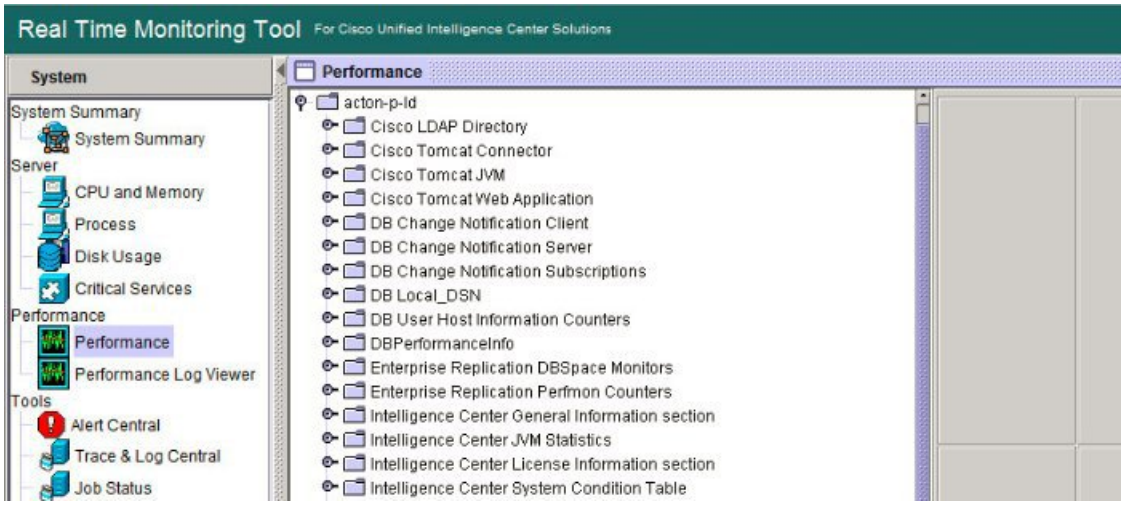
Figure 5: RTMT Alerts



Performon and Statistics

To expose perfmon information and statistics go to the RTMT**Tools** > **Alert Central**.

Figure 6: RTMT Performance Interface



The RTMT Interface

The following RTMT system monitoring objects are available in the left pane of the RTMT page:

- **System Summary**

  Displays information on Virtual Memory usage, CPU usage, Common Partition usage, and the alert history log.

- **Server**

  Server objects are:

  - **CPU and Memory** - Displays information on Virtual memory usage and CPU usage for the server.
  - **Process** - Displays information on the processes running on the server.
  - **Disk Usage** - Displays information on the disk usage on the server.
  - **Critical Services** - Displays the name of the critical service, the status (whether the service is up, down, activated, stopped by the administrator, starting, stopping, or in an unknown state), and the elapsed time during which the services have existed in a particular state for the server or for a particular server in a cluster (if applicable).

    The Cisco Unified Intelligence Center services are listed under the **Intelligence Center** tab. The Live Data and Cisco IdS services are listed, along with the System services, under the **System** tab.

- **Performance**

  Performance objects are:

  - **Performance** - Performance monitoring allows you to monitor performance counters related to the Unified Intelligence Center server. You can continuously monitor a set of preconfigured objects and receive notification in the form of an email message. You can associate counter threshold settings to alter notification. Up to six perfmon counters in one chart for performance comparisons can be displayed. Performance queries can be used to add a counter to monitor. You can also save and

restore settings, such as counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.

- **Performance Log Viewer** - Displays data for counters from perfmon CSV log files in a graphical format.

- **Tools**

  Tools objects are:

  - **Alert Central** - Displays the history and status of every alert in the system. Click the **Intelligence Center** tab to see Unified Intelligence Center alerts, including those related to Cisco IdS.
  - **Trace & Log Central** - Allows you to browse or download trace and log files for a specific date range or absolute time.
  - **Job Status** - Shows the status of trace collection events.
  - **Syslog Viewer** - Allows you to view (by node) the system, application, and security logs.
  - **VLT** - Not applicable.
  - **AuditLog Viewer** - Allows you to view system audit logs.

Related Topics

Cisco Unified Intelligence Center Counters, on page 58

Cisco Unified Intelligence Center Services

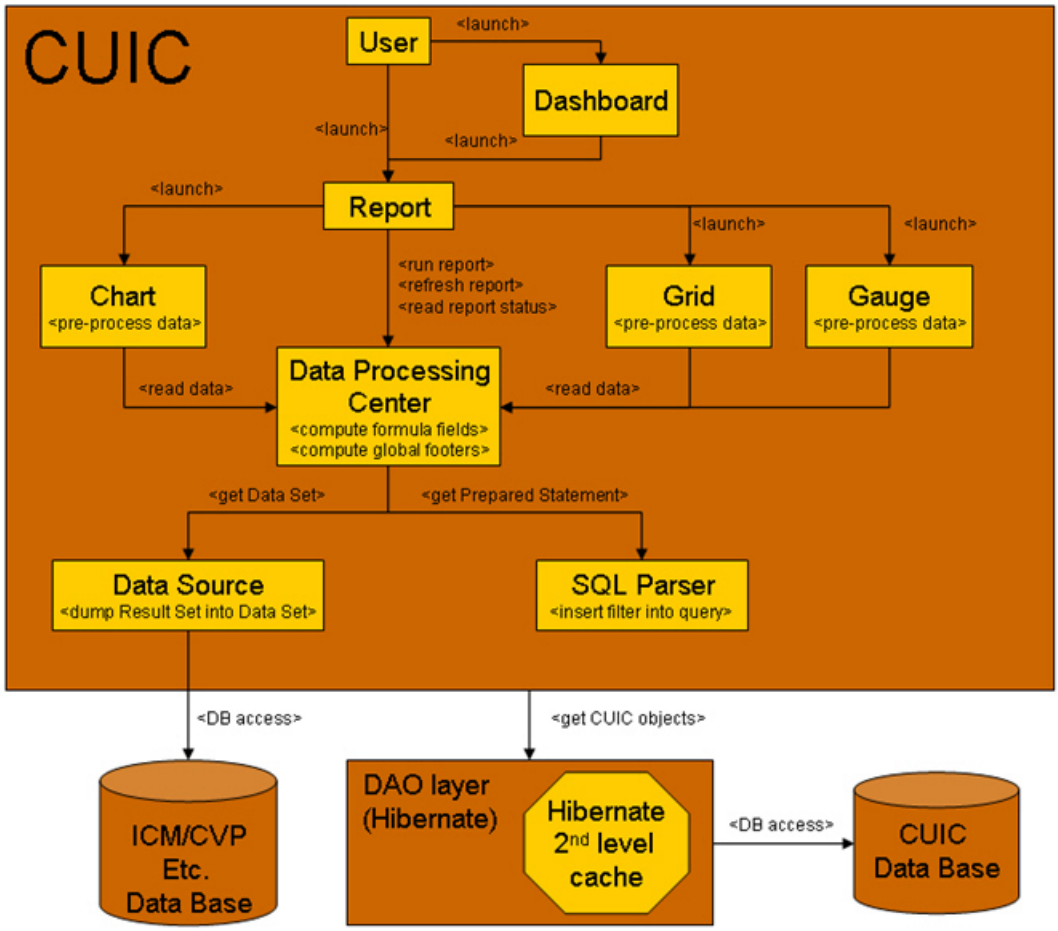
- **Intelligence Center Perfmon Service**—Performance data collection process, which persists counters relating to Unified Intelligence Center report execution and live data statistics from Unified Intelligence Center, Socket.IO, and CCE Live Data ActiveMQ Service process, which will be helpful in debugging performance issues.
- **Intelligence Center Reporting Service**— Core service for the Unified Intelligence Center reporting functionality.
- **Intelligence Center SNMP Java Adapter Service**—SNMP service that interfaces between JMX counters and the SNMP Primary Agent.
- **Intelligence Center Serviceability Service**— Services that exposes RTMT counters from the Unified Intelligence Center server.

Unified IC performance objects and counters

Unified Intelligence Center performance *objects* are named for system components that generate data. Each performance object provides performance *counters* that represent data specific to that object. The Unified Intelligence Center Reporting object has counters for the number of reports that are running and the number of reports that have failed. The counters for each object display when the folder expands.

Reporting Counters. The following diagram illustrates the runtime interactions and the relationship among the components involved on the execution of a report. The diagram provides a simple structure that defines the reporting engine performance counters.

Figure 7: Report Execution



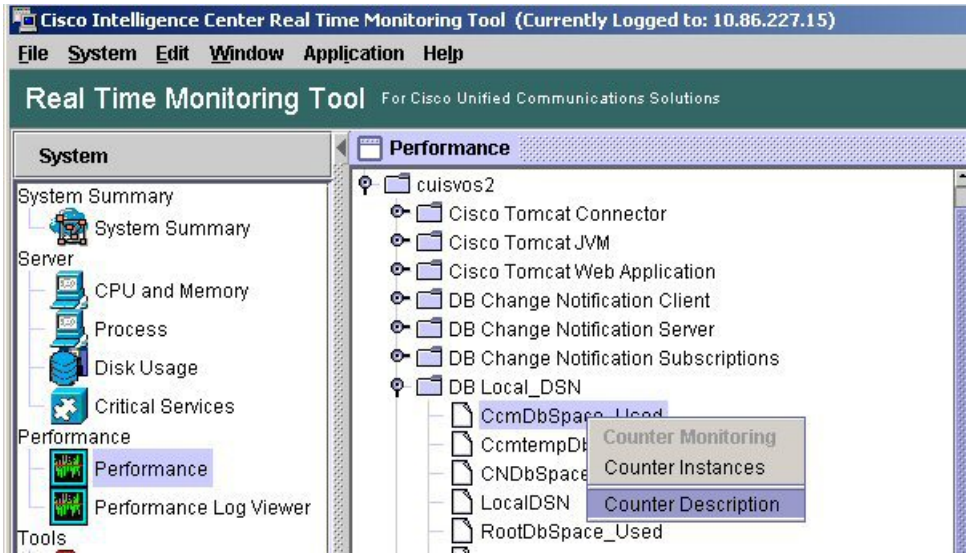
When the data for the report is available, the Data Processing Center computes the formula fields and global report footers. The gauge, grid, and chart managers in the engine pre-process the data to generate subsets of information that will be consumed by their corresponding peer components on the User Interface. The diagram shows which processes have a high cost of execution and the importance of closely monitoring the operations performed by charts, grids, data processing center, the data sources, and so forth. Monitor these components to track the behavior of each component and its total contribution to the cost of executing a report.

Aggregating the costs of all components provides a holistic view of the system performance. Keeping counters at the component level allows the system and application administrator to drill down into the details to determine what each component is doing and to perform any necessary corrective actions that.

This section lists all the performance objects monitored for Unified Intelligence Center and explains the counters for each.

Note Online help is available for each counter. Right-click the counter and select **Counter Description**.

Figure 8: RTMT Counter Help



For information on the objects and counters that are kept for the operating system, refer to the RTMT online help.

Intelligence Center Perfmon Service

Logs the performance counters from the critical processes in the system related to the Live Data Reporting services. This service collects data from the following services if they are up and running:

- Intelligence Center Reporting Service
- CCE Live Data ActiveMQ Service

Performance counter values are stored to the logs in the directory: `/opt/cisco/cuic/logs/perfmon`. The Intelligence Center Perfmon Service is configured to retain approximately 10 days of data at any given time. This service is independent of other services and is not required by other processes in the system.

Cisco Unified Intelligence Center Counters

Counters:

CUIC Tomcat Connector

The Tomcat Connector object provides information about Tomcat secure Hypertext Transport Protocol (HTTP) connectors. A Tomcat Connector represents an endpoint that receives requests and sends responses.

The Connector handles HTTP requests and sends HTTP responses that occur when Cisco Unified Intelligence Center web pages are accessed.

Counter	Description
Errors	The total number of HTTP errors (for example, 401 Unauthorized) encountered by the Connector.

Counter	Description
MBytes Received	The total number of data received by the Connector.
MBytes Sent	The total number of data that the Connector has sent.
Requests	The total number of requests that have been handled by the Connector.
ThreadsBusy	The Connector's current number of busy/in-use request processing threads.
ThreadsMax	The Connector's maximum number of request processing threads.
ThreadsTotal	The Connector's current total number of request processing threads, including available and in-use threads.

CUIC Tomcat JVM

The Tomcat Java Virtual Machine (JVM) object provides information about the Tomcat JVM, which represents, among other things, a pool of common resource memory used by Unified Intelligence Center.

Counter	Description
KBytesMemoryFree	The amount of free dynamic memory block (heap memory) in the Tomcat Java Virtual Machine. The dynamic memory block stores all objects created by Tomcat and its web applications such as Unified Intelligence Center. When the amount of free dynamic memory is low, more memory is automatically allocated and total memory size (represented by the KbytesMemoryTotal counter) increases up to the maximum (represented by the KbytesMemoryMax counter). You can determine the amount of memory in use by subtracting KBytesMemoryFree from KbytesMemoryTotal.
MemoryMax	The maximum dynamic memory block size for the Unified Intelligence Center Tomcat Java Virtual Machine.
MemoryTotal	This current total dynamic memory block size - including free and in-use memory - for the Tomcat Java Virtual Machine.

CUIC Tomcat Web Application

The Tomcat Web Application object provides information about running Cisco Unified Intelligence Center. The instance name for each Tomcat Web Application is based on the URL for the web application.

Counter	Description
Errors	The total number of HTTP errors (for example, 401 Unauthorized) encountered by a Cisco Unified Intelligence Center related web application.
Requests	The total number of requests handled by the web application. Each time a web application is accessed, its Requests counter increments accordingly.

Counter	Description
Sessions Active	The number of currently active (in use) sessions the web application currently has.

DB Change Notification Client

Counter	Description
MessagesProcessed	The number of database change notifications that have been processed. This counter refreshes every 15 seconds by default.
MessagesProcessing	The number of change notification messages in the change notification queue for this client that are currently being processed or are waiting to be processed. This counter refreshes every 15 seconds by default.
QueueHeadCounter	The head pointer of the change notification queue. The head pointer is the starting point in the change notification queue. To determine the number of notifications in the queue, subtract the head pointer value from the tail pointer value. This counter refreshes every 15 seconds by default.
QueueMax	The largest number of change notification messages to be processed for this client. This counter is cumulative since the last restart of the Cisco Database Layer Monitor service.
QueueTailPointer	The tail pointer of change notification queue. The tail pointer represents the ending point in the change notification queue. To determine the number of notifications in the queue, subtract the head pointer value from the tail pointer value. This counter refreshes every 15 seconds by default.
TablesSubscribed	The number of tables to which this client has subscribed.

DB Change Notification Server

Counter	Description
Clients	The total number of change notification clients.
CNProcessed	The total number of change notification messages processed by server since reboot.
QueueDelay	The number of seconds that the change notification process has messages to process, but is not processing them. This condition is true if either Change Notification Requests Queued in Database (QueuedRequestsInDB) and Change Notification Requests Queued in Memory (QueuedRequestsInMemory) are non-zero or if the Latest Change Notification Messages Processed count is not changing. This condition is checked every 15 seconds.
QueuedRequestsInDB	The number of records from DBCNQueue table.

Counter	Description
QueuedRequestsInMemory	The number of change notification requests queued in memory.

DB Change Notification Subscriptions

Counter	Description
SubscribedTable	The table(s) for which the service or servlet will receive change notifications. This information is provided for informational purposes only; no counter will increment.

DB Local DSN

Counter	Description
CcmDbSpace_Used	The amount of ccm dbspace consumed.
CcmtempDbSpace_Used	The amount of ccmtemp dbspace consumed.
CNDbSpace_Used	The percentage of CN dbspace consumed.
Local DSN	The data source name (DSN) that is being referenced from the local machine.
RootDBSpaceUsed	The amount of root dbspace consumed.
SharedMemory_Free	Total shared memory that is free.
SharedMemory_Used	Total shared memory that is used.

DB User Host Information Counters

Counter	Description
DB:User:Host Instances	The number of connections that are present for each instance of DB:User:Host.

DBPerformance Info

Counter	Description
CuicDbSpace_Used	The amount of Unified Intelligence Center dbspace consumed.
CuicSbSpace_Used	The amount of Unified Intelligence Center Blob Space consumed.
CuicTempDbSpace_Used	The amount of Unified Intelligence Center Temp dbspace consumed.
RootDbSpace_Used	The amount of root dbspace consumed.

Enterprise Replication DBSpace Monitors

Counter	Description
ERDbSpace_Used	The amount of enterprise replication DbSpace consumed.
ERSBDbSpace_Used	The amount of ERDbSpace consumed.

Enterprise Replication Perfmon Counters

Counter	Description
ReplicationQueueDepth	Displays the replication queue depth.

Intelligence Center General Information Section

Counter	Description
DeviceType	The number id of the device type.
Global StatisticInterval	Size in milliseconds of the global statistics interval.
InetAddress Type	The type of the ip address of the device, either IPv4 or IPv6.
Time Zone Offset Hours	The hours component of the offset of the default configured time zone.
Time Zone Offset Minutes	The minutes component of the offset of the default configured time zone.
Uptime (sec)	Null.

Intelligence Center JVM Statistics

Counter	Description
EnvMaxThreadsUsed	The real-time maximum threads used object is a real-time snapshot metric indicating the peak amount of threads used simultaneously in the runtime environment since startup. The maximum number of threads used by the runtime environment includes all Unified Intelligence Center standalone and thread pool threads as well as threads created by the web application server running within the same runtime environment.
EnvRtCommitMemUsed	The real-time current memory used object is a real-time snapshot metric indicating the memory committed by the runtime environment. This memory is guaranteed to be available to the runtime environment. This can change dynamically over time but is never less than EnvRtCurrMemUsed. The object value is expressed as a count of megabytes.

Counter	Description
EnvRtCurrMemAvail	The real-time current memory available object is a real-time snapshot metric indicating the amount of system memory not being used. The object value is expressed as a count of Mega bytes and indicates the amount of current system memory that is not currently being used.
EnvRtCurrMemUsed	The real-time current memory used object is a real-time snapshot metric indicating the current memory usage by the runtime environment. The object value is expressed as a count of Mega bytes and indicates the current amount of memory used by this runtime environment.
EnvRtCurrThreadsInUse	The real-time current threads in use object is a real-time snapshot metric indicating a count of threads that are in use in the runtime environment. The number of threads in use by the runtime environment include all of the Unified Intelligence Center standalone and thread pool threads as well as those threads created by the web application server running within the same runtime environment.
EnvRtMaxMemAvail	The real-time maximum memory available object is a real-time snapshot metric indicating the maximum amount of System memory available. The object value is expresses as a count of megabytes.
EnvRtMaxMemUsed	The real-time maximum memory used object is a real-time snapshot metric indicating the peak memory allocated to the runtime environment. The object value is expressed as a count of megabytes and indicates the high water mark of memory that can be used by the runtime environment.
EnvRtUpTime	The real-time up time object is a real-time snapshot metric indicating how long the Unified Intelligence Center application has been running. The object value is expressed as a count of milliseconds that have elapsed since the application began executing.

Intelligence Center System Condition Table

Counter	Description
CUIC_DATASOURCE _UNAVAILABLE	This counter is no longer valid with the counter value -1. It has been rendered obsolete by the Await Write Time counter.
CUIC_DB_REPLICATION _FAILED	Database replication failed.
CUIC_REPORT_ EXECUTION_FAILED	Could not run the report. Could be because associated data source is offline.

Counter	Description
CUIC_SERVICE_UNAVAILABLE	Service going down.
Infrastructure_DEADLOCK_DETECTED	A deadlock between two or more application threads has been detected. This is an unrecoverable error and the server must be restarted. Detailed information about the deadlock can be found in the logs.
Infrastructure_ LOG_PURGER_ERROR	An error occurred while log files were being purged.
Infrastructure_ PERSISTENT_STORE_SIZE_ALMOST_FULL	The message store that persists reporting data during a connection loss is approaching capacity. If it fills completely, reporting data will be lost.
Infrastructure_ PERSISTENT_STORE_SIZE_FULL	The message store that persists reporting data during a connection loss is at capacity. Reporting data will be lost until the connection with the reporting server is restored.
Infrastructure_ PERSISTENT_STORE_SIZE_WARN	The message store that persists reporting data during a connection loss is more than half full. If it fills completely, reporting data will be lost.
Infrastructure_ PORT_SECURITY_MANAGER_ERROR_LOADING	Error manipulating PortSecurityManager firewall rules.
Infrastructure_ SC_JMX_CONFIGURATION_ERROR	There is a configuration problem with JMX ports.
Infrastructure_ SERVER_NOT_READY	The Server state is not ready.
Infrastructure_ SNMP_CONNECTION_ERROR	The connection to SNMP Subagent Failed.
Infrastructure_ SOFTWARE_CONFIGURATION_ERROR	There is an error in the files configuring the software on the disk.
Infrastructure_ SUBSYSTEM_HEARTBEAT_FAILED	Heartbeats from one or more subsystems have stopped.
Infrastructure_ SUBSYSTEM_START_FAILURE	One or more subsystems failed to start.
Infrastructure_ SUBSYSTEM_STOP_FAILURE	One or more subsystems failed to stop.
Infrastructure_SYSTEM_SHUT_DOWN	One or more subsystems shut down.
RS_CONFIG_ UNAVAILABLE	System detected critical error accessing configuration.
RS_DATABASE_ UNAVAILABLE	System detected critical error with database.
RS_MAINTENANCE_ IN_PROGRESS	System has detected maintenance in progress on Reporting Server.

Counter	Description
RS_SYSTEM_ THRESHOLD_REACHED	System has detected a critical system threshold reached on Reporting Server.
RS_UNRECOVERABLE _ERROR	System has detected an internal error within Reporting Server which may prevent it from functioning correctly. Restart may be required.

Intelligence Center Tomcat Connector - HTTPS

The Unified Intelligence Tomcat Connector object provides information about a secure Hypertext Transport Protocol (HTTPS) Tomcat connector. A Tomcat Connector represents an endpoint that receives requests and sends responses.

The Connector handles HTTPS requests and sends HTTPS responses that occur when Cisco Unified Intelligence Center web pages are accessed. There is an instance of this object based on the Secure Sockets Layer (SSL) status of the URLs for web applications: **http-8444** for SSL (HTTPS) connections.

Counter	Description
Errors	The total number of errors (for example, 401 Unauthorized) encountered by the Connector.
MBytes Received	The total number of data received by the Connector.
MBytes Sent	The total number of data that the Connector has sent.
Requests	The total number of requests that have been handled by the Connector.
ThreadsBusy	The Connector's current number of busy/in-use request processing threads.
ThreadsMax	The Connector's maximum number of request processing threads.
ThreadsTotal	The Connector's current total number of request processing threads, including available and in-use threads.

IP

The IP object provides information on the IPv4-related statistics on your system.

Counter	Description
Frag Creates	The number of IP datagrams fragments that have been generated at this entity.
Frag Fails	The number of IP datagrams that were discarded at this entity because the datagrams could not be fragmented, such as datagrams where the Do not Fragment flag was set.
Frag OKs	The number of IP datagrams that were successfully fragmented at this entity.

Counter	Description
In Delivers	The number of input datagrams that were delivered to IP user protocols. This includes Internet Control Message Protocol (ICMP).
In Discards	The number of input IP datagrams where no problems were encountered, but which were discarded. Lack of buffer space provides one possible reason. This counter does not include any datagrams that were discarded while awaiting reassembly.
In HdrErrors	The number of input datagrams that were discarded with header errors. This includes bad checksums, version number mismatch, other format errors, time-to-live exceeded, and other errors that were discovered in processing their IP options.
In Receives	The number of input datagrams that were received from all network interfaces. This counter includes datagrams that were received with errors.
In UnknownProtos	The number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.
InOut Requests	The number of incoming IP datagrams that were received and the number of outgoing IP datagrams that were sent.
Out Discards	The number of output IP datagrams that were not transmitted and were discarded. Lack of buffer space provides one possible reason.
Out Requests	The total number of IP datagrams that local IP user-protocols (including ICMP) supply to IP in requests transmission. This counter does not include any datagrams that were counted in ForwDatagrams.
Reasm Fails	The number of IP reassembly failures that the IP reassembly algorithm detected, including time outs, errors, and so on. This counter does not represent the discarded IP fragments because some algorithms, such as the algorithm in RFC 815, can lose track of the number of fragments because it combines them as they are received.
Reasm OKs	The number of IP datagrams that were successfully reassembled.
Reasm Reqds	The number of IP fragments that were received that required reassembly at this entity.

IP6

The IP6 object, which supports Cisco Unified Communications Manager, provides information on the IPv6-related statistics on your system.

Counter	Description
Frag Creates	The number of IP datagrams fragments that have been generated at this entity.

Counter	Description
Frag Fails	The number of IP datagrams that were discarded at this entity because the datagrams could not be fragmented, such as datagrams where the Do not Fragment flag was set.
Frag OKs	The number of IP datagrams that were successfully fragmented at this entity.
In Delivers	The number of input datagrams that were delivered to IP user protocols. This includes Internet Control Message Protocol (ICMP).
In Discards	The number of input IP datagrams where no problems were encountered, but which were discarded. Lack of buffer space provides one possible reason. This counter does not include any datagrams that were discarded while awaiting reassembly.
In HdrErrors	The number of input datagrams that were discarded with header errors. This includes bad checksums, version number mismatch, other format errors, time-to-live exceeded, and other errors that were discovered in processing their IP options.
In Receives	The number of input datagrams that were received from all network interfaces. This counter includes datagrams that were received with errors.
In UnknownProtos	The number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.
InOut Requests	The number of incoming IP datagrams that were received and the number of outgoing IP datagrams that were sent.
Out Discards	The number of output IP datagrams that were not transmitted and were discarded. Lack of buffer space provides one possible reason.
Out Requests	The total number of IP datagrams that local IP user-protocols (including ICMP) supply to IP in requests transmission. This counter does not include any datagrams that were counted in ForwDatagrams.
Reasm Fails	The number of IP reassembly failures that the IP reassembly algorithm detected, including time outs, errors, and so on. This counter does not represent the discarded IP fragments because some algorithms, such as the algorithm in RFC 815, can lose track of the number of fragments because it combines them as they are received.
Reasm OKs	The number of IP datagrams that were successfully reassembled.
Reasm Reqds	The number of IP fragments that were received that required reassembly at this entity.

Memory

The memory object provides information about the usage of physical memory and swap memory on the server.

Counter	Description
% Mem Used	Displays the system physical memory utilization as a percentage. The value of this counter equals (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes) / Total KBytes, which also corresponds to the Used KBytes/Total KBytes.
% Page Usage	The percentage of active pages.
% VM Used	The system virtual memory utilization as a percentage. The value of this counter equals (Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes + Used Swap KBytes) / (Total KBytes + Total Swap KBytes), which also corresponds to Used VM KBytes/Total VM KBytes.
Buffers KBytes	The capacity of buffers in your system in kilobytes.
Cached KBytes	The amount of cached memory in kilobytes.
Free KBytes	The total amount of memory that is available in your system in kilobytes.
Free Swap KBytes	The amount of free swap space that is available in your system in kilobytes.
HighFree	The amount of free memory in the high region. Linux kernel splits the virtual memory address space into memory regions. The high memory is memory above a certain physical address, and its amount depends on the total memory and the type of kernel on the system.
HighTotal	The total amount of memory in the high region.
LowFree	The free low (non-paged) memory for kernel.
LowTotal	The total low (non-paged) memory for kernel.
PageFaultsPerSec	This represents the number of page faults (major + minor) made by the system per second (post 2.5 kernels only). This is not a count of page faults that generate I/O, because some page faults can be resolved without I/O.
PageMajorFaultsPerSec	This represents the number of major faults the system has made per second, those which have required loading a memory page from disk (post 2.5 kernels only).
Pages	The number of pages that the system paged in from the disk plus the number of pages that the system paged out to the disk.
Pages Input	The total number of pages that the system paged in from the disk.

Counter	Description
Pages Input Per Sec	The total number of kilobytes the system paged in from disk per second.
Pages Output	The total number of pages that the system paged out to the disk.
Pages Output Per Sec	This represents the total number of kilobytes the system paged out to disk per second.
Shared KBytes	The amount of shared memory in your system in kilobytes.
SlabCache	This represents all memory used by created slabcaches by various kernel components, as a macroscopic counter representing the sum of all the individual entries in the proc's slab info.
SwapCached	This represents the amount of Swap used as cache memory. Memory that once was swapped out, is swapped back in, but is still in the swapfile.
Total KBytes	The total amount of memory in your system in kilobytes.
Total Swap KBytes	The total amount of swap space in your system in kilobytes.
Total VM KBytes	The total amount of system physical and memory and swap space (Total Kbytes + Total Swap Kbytes) that is in use in your system in kilobytes.
Used KBytes	The amount of system physical memory that is in use on the system in kilobytes. The value of the Used KBytes counter equals Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes. The Used KBytes value differs from the Linux term that displays in the top or free command output. The Used value that displays in the top or free command output equals the difference in Total KBytes - Free KBytes and also includes the sum of Buffers KBytes and Cached KBytes.
Used Swap KBytes	The amount of swap space that is in use on your system in kilobytes.
Used VM KBytes	The system physical memory and the amount of swap space that is in use on your system in kilobytes. The value equals Total KBytes - Free KBytes - Buffers KBytes - Cached KBytes + Shared KBytes + Used Swap KBytes. This corresponds to Used Mem KBytes + Used Swap KBytes.

Network Interface

The Network Interface object provides information about the network interfaces on the system.

Counter	Description
RxBytes	The number of bytes, including framing characters, that was received on the interface.

Counter	Description
Rx Dropped	This represents the number of inbound packets that was chosen to be discarded even though no errors had been detected. Discarding packets prevents the packet from being delivered to a higher layer protocol, for example, to free up buffer space.
Rx Errors	This represents the number of inbound packets (for packet-oriented interfaces) and the number of inbound transmission units (for character-oriented or fixed-length interfaces) that contained errors that prevented them from being deliverable to a higher layer protocol.
Rx Multicast	This represents the number of multicast packets that was received on this interface.
Rx Packets	This represents the number of packets that this sublayer delivered to a higher sublayer. This does not include the packets that were addressed to a multicast or broadcast address at this sublayer.
Total Bytes	This represents the total number of received (Rx) bytes and transmitted (Tx) bytes.
Total Packets	This represents the total number of received (Rx) packets and transmitted (Tx) packets.
Tx Bytes	This represents the total number of octets, including framing characters, that was transmitted out of the interface.
Tx Dropped	This represents the number of outbound packets that was chosen to be discarded even though no errors were detected. Discarding a packet prevents the packet from being delivered to a higher layer protocol, for example, to free up buffer space.
Tx Errors	This represents the number of outbound packets (for packet-oriented interfaces) and the number of outbound transmission units (for character-oriented or fixed-length interfaces) that could not be transmitted because of errors.
Tx Packets	This represents the total number of packets that the higher level protocols requested for transmission, including those that were discarded or not sent. This does not include packets that were addressed to a multicast or broadcast address at this sublayer.
Tx QueueLen	This represents the length, measured in packets, of the output packet queue.

Number of Replicates Created and State of Replication

The Number of Replicates Created and State of Replication object provides real-time replication information for the system.

Counter	Description
Number or Replicates Created	Displays the number of replicates that were created by Informix for the DB tables. This counter displays information during Replication Setup.
Replicate_State	This counter represents the state of replication. The following list provides possible values: • 0 = Initializing. The counter equals 0 when the server is not defined or when the server is defined but realizes the template has not completed. • 1 = Replication setup script fired from this node. You can run utils dbreplication status on the CLI to determine the location and cause of the failure. • 2 = Good Replication. • 3 = Replication. A counter value of 3 indicates replication in the cluster is bad. It does not mean that replication failed on a particular server in the cluster. You can run utils dbreplication status on the CLI to determine the location and cause of the failure. • 4 = Replication setup did not succeed.

Partition

The Partition object provides information about the file system, its usage in the system, and the disk utilization on a per-partition basis on the system.

Counter	Description
% CPU Time	The percentage of CPU time that is dedicated to handling IO requests that were issued to the disk.
% Used	The percentage of disk space that is in use on this file system.
% Wait in Read	Not used. It has been rendered obsolete by the Await Read Time counter.
% Wait in Write	Not used. It has been rendered obsolete by the Await Write Time counter.
Await Read Time	The average time, measured in milliseconds, for read requests issued to the device to be served.
Await Time	The average time, measured in milliseconds, for I/O requests that were issued to the device to be served. This includes the time that the requests spent in queue and the time that was spent servicing them.
Await Write Time	The average time, measured in milliseconds, for write requests that are issued to the device to be served.

Counter	Description
Queue Length	The average queue length for the requests that were issued to the disk.
Read Bytes Per Sec	The amount of data in bytes per second that was read from the disk.
Total Mbytes	The amount of total disk space in megabytes that is on this file system.
Used Mbytes	The amount of disk space in megabytes that is in use on this file system.
Write Bytes Per Sec	The amount of data that was written to the disk in bytes per second.

PermalinkInfo

Counter	Description
DashboardPermalinksViewed	Total number of dashboard permalink views.
DashboardPermalinksViewedInterval	Total number of dashboard permalinks viewed over the last interval.
ExcelPermalinksViewed	Total number of excel permalink views.
ExcelPermalinksViewedInterval	Total number of excel permalinks viewed over the last interval.
HTMLPermalinksViewed	Total number of HTML permalink views.
HTMLPermalinksViewedInterval	Total number of HTML permalinks viewed over the last interval.
TotalPermalinksViewed	The sum of report and dashboard permalinks viewed.
TotalPermalinksViewedInterval	The sum of report and dashboard permalinks viewed over the last interval.
XMLPermalinksViewed	Total number of XML permalink viewed.
XMLPermalinksViewedInterval	Total number of XML permalinks viewed over the last interval.

Process

Counter	Description
% CPU Time	Expressed as a percentage of total CPU time, represents the task's share of the elapsed CPU time since the last update.
% Memory Usage	The percentage of physical memory that a task is currently using.
Data Stack Size	The stack size for task memory status.
Nice	The nice value of the task. A negative nice value indicates that the process has a higher priority. A positive nice value indicates that the process has a lower priority. If the nice value equals zero, do not adjust the priority when you are determining the dispatchability of a task.

Counter	Description
Page Fault Count	The number of major page faults that a task encountered that required the data to be loaded into memory.
PID	The task's unique process ID, which periodically wraps, though never restarting at zero.
Process Status	The task's process status: 0 - Running, 1 - Sleeping, 2 - Uninterruptible disk sleep, 3 - Zombie, 4 - Traced or stopped (on a signal), 5 - Paging, 6 - Unknown.
Shared Memory Size	The amount of shared memory, in KB, that a task is using. Other processes could potentially share the same memory.
STime	The amount of system time (STime), measured in jiffies, for which this process has been scheduled in kernel mode. A jiffy corresponds to a unit of CPU time and gets used as a base of measurement. One second is equal to 100 jiffies.
Thread Count	The number of threads that are currently grouped with the task. A negative value -1 indicates that this counter is currently not available because thread statistics (including all performance counters in the Thread object as well as the Thread Count counter in the Process object) have been turned off because the system's total processes and threads have exceeded the default threshold value.
Total CPU Time Used	The total CPU time, measured in jiffies, that the task has consumed in user mode and kernel mode since the start of the task. One second is equal to 100 jiffies.
UTime	The amount of time, measured in jiffies, that the task has been scheduled for in user mode. One second is equal to 100 jiffies.
VmDate	The virtual memory usage of the heap for the task in kilobytes (KB).
VmRSS	The virtual memory (Vm) resident set size (RSS) that is currently in physical memory in kilobytes (KB), including Code, Data, and Stack.
VmSize	The total amount of virtual memory, in KB, that the task is using. It includes all code, data, shared libraries, and pages that have been swapped out: Virtual I

Processor

Counter	Description
% CPU Time	The processor's share of the elapsed CPU time excluding the idle time since last update, expressed as a percentage of CPU time.
Idle Percentage	The percentage of time that the CPU or CPUs were idle and the system did not have an outstanding disk I/O request.

Counter	Description
IOwait Percentage	The percentage of time that the CPU or CPUs were idle, during which the system had an outstanding disk I/O request.
Irq Percentage	The percentage of time that the processor is executing the interrupt request which is assigned to devices for interrupt, or sending a signal to the computer when it is finished processing.
Nice Percentage	The percentage of CPU utilization that occurred while running at the user level with nice priority.
Softirq Percentage	The percentage of time that the processor is executing the softirq, which means that task switching is deferred until later to achieve better performance.
System Percentage	The percentage of CPU utilization that occurred while running at the system level (kernel).
User Percentage	The percentage of CPU utilization that occurred while running at the user level (application).

Ramfs

Counter	Description
FilesTotal	The total number of files in the ram-based filesystem (ramfs).
SpaceFree	The amount of free data blocks in the ram-based filesystem (ramfs). A block is a uniformly sized unit of data storage for a filesystem. The block size specifies the size that the filesystem will use to read and write data.
SpaceUsed	The amount of used data blocks in the ram-based filesystem (ramfs). A block is a uniformly sized unit of data storage for a filesystem. The block size specifies the size that the filesystem will use to read and write data.

Reporting Engine Info

Counter	Description
Report (H/RT) Completed	Total number of reports that have been successfully run.
Report (H/RT) CompletedInterval	Change of counter Report (H/RT) Completed over the last interval.
Report (H/RT) ExecutionQueryTime	Time taken to run the database query against (H/RT) report (milliSeconds)

Counter	Description
Report (H/RT) ExecutionQueryTimeInterval	Change of counter Report (H/RT) ExecutionQueryTime over the last interval.
Report (H/RT) Failed	The total number of reports that have failed. The total number of times that Unified Intelligence Center has tried to fetch data from a Data Source but it has not been able to.
Report (H/RT) FailedInterval	The interval measurement of the Report (H/RT) Failed counter.
Report (H/RT) Running	The number of (H/RT) reports that are currently running. A report is currently running when the Runnable object has been assigned a thread from the pool. It does not include those that are waiting in a queue for a thread to become available.
Report (H/RT) Running Interval	The interval measurement of the Report (H/RT) Running counter.
Report (H/RT) Runtime	Total amount of seconds spent running reports.
Report (H/RT) RuntimeInterval	Change of counter Report (H/RT) Runtime over the last interval.
Report (H/RT) Waiting	Total number of reports that are currently queued for run.
ReportsUsersLoggedin	Total number of users that are currently logged in.

RESTInfo

Counter	Description
ConfigurationCalls	Total number of configuration REST calls made to Unified Intelligence Center.
ConfigurationCallsInterval	Total number of configuration REST calls made to Unified Intelligence Center over the last interval.
ReportCalls	Total number of Report REST calls made to Unified Intelligence Center.
ReportCallsInterval	Total number of Report REST calls made to Unified Intelligence Center over the last interval.
ReportDefinitionCalls	Total number of Report Definition REST calls made to Unified Intelligence Center.
ReportDefinitionCallsInterval	Total number of Report Definition REST calls made to Unified Intelligence Center over the last interval.
TotalRESTCalls	Total number of REST calls made to Unified Intelligence Center.
TotalRESTCallsInterval	Total number of REST calls made to Unified Intelligence Center over the last interval.

SchedulerInfo

Counter	Description
SchedulerJobsFailedCount	The number of jobs that the scheduler service has failed to complete successfully.
SchedulerJobsRunningCount	The number of jobs that the scheduler service is currently running.
EmailExcelCount	The number of jobs which send provided report execution results as Excel in email.
EmailHTMLCount	The number of jobs which send provided report execution results as HTML in email.
EmailPDFCount	The number of jobs which send provided report execution results as PDF in email.
SFTPCount	The number of jobs which saves report execution results to the given remote location.

System

The System object provides information for file descriptors (FD), total processes and threads, total CPU time measured on the system.

Counter	Description
Allocated FDs	Represents the total number of allocated file descriptors.
Being Used FDs	Represents the number of file descriptors that is currently in use in the system.
Freed Fds	Represents the total number of allocated file descriptors on the system that is freed.
IOAwait	The average time, in milliseconds, for I/O requests issued to all devices to be served. This includes the time spent by the requests in queue and the time spent servicing the requests.
IOCpuUtil	The percentage of CPU time during which I/O requests were issued to the device (bandwidth utilization for the device) on this server.
IODeviceReqQueueSize	The average queue length of the requests that were issued to all devices on this server.
IODeviceReqSectorSize	The average size in sectors of the requests that were issued to all devices on this server.
IOKBytesReadPerSecond	The total number of KBytes read per second from all devices on this server.
IOKBytesWrittenPerSecond	The total number of KBytes written per second to all devices on this server.

Counter	Description
IOPerSecond	The total number of input/output operations on all disk partitions per second on this server. If you experience a system performance issue, use the information in this counter to measure the impact of the aggregate I/O operations on this server.
IOReadReqPerSecond	The total number of read requests per second that were issued to all devices on this server.
IOReadQueueMergedPerSecond	The total number of read requests merged per second that were queued to all devices on this server.
IOSectorsReadPerSecond	The total number of sectors read per second from all devices on this server.
IOSectorsWrittenPerSecond	The total number of sectors written per second to all devices on this server.
IOServiceTime	The average service time, in milliseconds, for I/O requests that were issued to all devices on this server.
IOWriteReqPerSecond	The total number of write requests per second that were issued to all devices on this server.
IOWriteReqQueueMergedPerSecond	The total number of write requests merged per second that were queued to all devices on this server.
Max Fds	Represents the maximum number of file descriptors that is allowed on the system.
Total CPU Time	Represents the total time, measured in jiffies, that the system has been up and running. A jiffy corresponds to a unit of CPU time and gets used as a base of measurement. One second is equal to 100 jiffies.
Total Processes	Represents the total number of processes on the system.
Total Threads	Represents the total number of threads on the system.

TCP

Counter	Description
Active Opens	The number of times that TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Attempt Fails	The number of times that TCP connections have made a direct transition to the CLOSED stated from either the SYN-RCVD state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYS-RCVD state.

Counter	Description
Curr Estab	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
Estab Resets	The number of times that the TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
In Segs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
InOut Segs	The total number of segments that were sent and the total number of segments that were received.
Out Segs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Passive Opens	The number of times that TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
RetransSegs	The total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

Thread

Counter	Description
% CPU Time	The thread's share of the elapsed CPU time since the last update, expressed as a percentage of total CPU time.
PID	The thread's leader process ID.

Disaster Recovery System

Backup and Restore Overview

The Disaster Recovery System (DRS) provides full data backup for all servers in a Cisco Unified Intelligence Center cluster. It allows you to perform regularly scheduled automatic or user-invoked data backups.

The Disaster Recovery System performs a cluster-level backup, which means that it collects backups for all servers in a Cisco Unified Intelligence Center cluster to a central location and archives the backup data to physical storage device. Backup files are encrypted and can be opened only by the system software.

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. DRS backs up the drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup functions.
- Scheduled backups or manual (user-invoked) backups.

Backup Prerequisites

To back up data to a remote device on the network, you must have an SFTP server that is configured. You can use an SFTP server product that is certified with Cisco Technology Partners. Technology partners certify their products with specified versions of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, see the *Solutions Catalog* on the Cisco Developer Network at https://marketplace.cisco.com.

Ensure that all cluster nodes are running the same version of Cisco Unified intelligence Center. If different nodes are running different versions, the certificates will not match and your backup or restore could fail.

Note Retest the DRS with your SFTP server after you upgrade your Unified Communications Manager, upgrade your SFTP server, or you switch to a different SFTP server. Perform this step to ensure that these components operate correctly together. Additionally, perform a backup and restore on a standby or backup server.

Use the information in the following table to determine which SFTP server solution to use in your system.

Table 13: SFTP Server Information

SFTP Server	Information
SFTP Server on Cisco Prime Collaboration Deployment	This server is provided and tested by Cisco, and supported by Cisco TAC. Version compatibility depends on your version of Unified Communications Manager and Cisco Prime Collaboration Deployment. See the *Cisco Prime Collaboration Deployment Admin Guide* before you upgrade its version (SFTP) or Unified Communications Manager to ensure that the versions are compatible.
SFTP Server from a Technology Partner	These servers are third party provided, third party tested, and jointly supported by TAC and the Cisco vendor. Version compatibility depends on the third party test. See the Technology Partner page if you upgrade their SFTP product and/or upgrade Unified Communications Manager for which versions are compatible: https://marketplace.cisco.com

SFTP Server	Information
SFTP Server from another Third Party	These servers are third party provided, have limited Cisco testing, and are not officially supported by Cisco TAC. Version compatibility is on a best effort basis to establish compatible SFTP versions and Unified Communications Manager versions. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH
- Cygwin
- Titan

Cisco does not support using the SFTP product freeFTPd. This is because of the 1GB file size limit on this SFTP product.

For Cygwin to function properly as your backup SFTP server, you must add the following lines to the `sshd_config` file:

The cipher key: **`ciphers aes128-cbc`**

The Unified Communications Algorithm: **`KexAlgorithms diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1`**

For details on how to set up third-party SFTP products, contact the third-party vendor for support. For issues with third-party products that have not been certified through the Cisco Technology Developer Program process, contact the third-party vendor for support

Note While a backup or restore is running, you cannot perform any OS Administration tasks, because Disaster Recovery System blocks all OS Administration requests by locking the platform API. However, Disaster Recovery System does not block most CLI commands, because only the CLI-based upgrade commands use the Platform API locking package.

Backup Procedure Taskflow

Configure backup devices

You can configure up to 10 backup devices. Perform the following steps to configure the location where you want to store backup files.

Before you begin

- Ensure you have write access to the directory path in the SFTP server to store the backup file.

- Ensure that the username, password, server name, and directory path are valid as the DRS Primary Agent validates the configuration of the backup device.

Note Schedule backups during periods when you expect less network traffic.

Procedure

Step 1 From Disaster Recovery System, select **Backup** > **Backup Device**.

Step 2 In the **Backup Device List** window, do either of the following:

- To configure a new device, click **Add New**.
- To edit an existing backup device, enter the search criteria, click Find, and **Edit Selected**.
- To delete a backup device, select it in the **Backup Device** list and click **Delete Selected**.

You cannot delete a backup device that is configured as the backup device in a backup schedule.

Step 3 Enter a backup name in the **Backup Device Name** field.

The backup device name contains only alphanumeric characters, spaces (), dashes (-) and underscores (_). Do not use any other characters.

Step 4 In the **Select Destination** area, under **Network Directory** perform the following:

- In the **Host name/IP Address** field, enter the hostname or IP address for the network server.
- In the **Path name** field, enter the directory path where you want to store the backup file.
- In the **User name** field, enter a valid username.
- In the **Password** field, enter a valid password.
- From the **Number of backups to store on Network Directory** drop-down list, choose the required number of backups.

Step 5 Click **Save**.

What to do next

Estimate Size of Backup Tar, on page 84

Configure a Schedule Backup

You can create up to 10 backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, the set of features to back up, and a storage location.

Caution Schedule backups during off-peak hours to avoid service interruptions.

Before you begin

Configure backup devices

Procedure

Step 1 From the Disaster Recovery System, choose **Backup Scheduler**.

Step 2 In the **Schedule List** window, do one of the following steps to add a new schedule or edit an existing schedule.

- To create a new schedule, click **Add New**.
- To configure an existing schedule, click the name in the Schedule List column.

Step 3 In the **scheduler** window, enter a schedule name in the **Schedule Name** field.

Note You cannot change the name of the default schedule.

Step 4 Select the backup device in the **Select Backup Device** area.

Step 5 Select the features to back up in the **Select Features** area. You must choose at least one feature.

Step 6 Choose the date and time when you want the backup to begin in the **Start Backup at** area.

Step 7 Choose the frequency at which you want the backup to occur in the **Frequency** area. The frequency can be set to Once Daily, Weekly, and Monthly. If you choose **Weekly**, you can also choose the days of the week when the backup will occur.

Tip To set the backup frequency to **Weekly**, occurring Tuesday through Saturday, click **Set Default**.

Step 8 To update these settings, click **Save**.

Step 9 Choose one of the following options:

- To enable the selected schedules, click **Enable Selected Schedules**.
- To disable the selected schedules, click **Disable Selected Schedules**.
- To delete the selected schedules, click **Delete Selected**.

Step 10 To enable the schedule, click **Enable Schedule**.

The next backup occurs automatically at the time that you set.

Note Ensure that all servers in the cluster are running the same version of Cisco Unified Intelligence Center and are reachable through the network. Servers that are not reachable at the time of the scheduled backup will not get backed up.

What to do next

(Optional) View Current Backup Status

Start a Manual Backup

Before you begin

- Ensure that all cluster nodes have the same installed version of Cisco Unified Intelligence Center.

- Ensure that there is adequate space in the remote server.
- Ensure that there are no network interruptions.
- Configure backup devices
- Be aware that your backup .tar files are encrypted by a randomly generated password. This password is then encrypted by using the cluster security password and gets saved along with the backup .tar files. You must remember this security password or take a backup immediately after the security password change/reset.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Manual Backup**.

Step 2 In the **Manual Backup** window, select a backup device from the **Backup Device Name** area.

Step 3 Choose a feature from the **Select Features** area.

Step 4 Click **Start Backup.**

What to do next

(Optional) View Current Backup Status

View Current Backup Status

Perform the following steps to check the status of the current backup job.

Caution Be aware that if the backup to the remote server is not completed within 20 hours, the backup session times out and you must begin a fresh backup.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Current Status**.

Step 2 To view the backup log file, click the log filename link.

Step 3 To cancel the current backup, click **Cancel Backup**.

Note The backup cancels after the current component completes its backup operation.

What to do next

View Backup History, on page 84

Estimate Size of Backup Tar

Cisco Unified Intelligence Center will estimate the size of the backup tar, only if a backup history exists for one more selected features.

The calculated size is not an exact value but an estimated size of the backup tar. Size is calculated based on the actual backup size of a previous successful backup and may vary if the configuration changed since the last backup.

You can use this procedure only when the previous backups exist and not when you back up the system for the first time.

Follow this procedure to estimate the size of the backup tar that is saved to a SFTP device.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Manual Backup**.

Step 2 In the **Select Features** area, select the features to back up.

Step 3 Click **Estimate Size** to view the estimated size of backup for the selected features.

What to do next

View Backup History, on page 84

View Backup History

Perform the following steps to view the backup history.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **History**.

Step 2 From the **Backup History** window, you can view the backups that you have performed, including filename, backup device, completion date, result, version, features that are backed up, and failed features.

Note The **Backup History** window displays only the last 20 backup jobs.

Network Management

Configure SNMP-Associated Settings

This page launches the Cisco Unified Serviceability application, which gives menu access for configuring SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3.

Open online help for SNMP configuration from within the Serviceability application.

Note You cannot click the **Back** button on this page to return to the Unified Intelligence Center Administration console.

To return to the Administration console:

- Close the Cisco Unified Serviceability page, or
- Select Cisco Unified Intelligence Center in the Navigation drop-down menu at the top right of the screen. Then click **Go**.

Unified Intelligence Center SNMP MIBs

The Unified Intelligence Center SNMP sub-agent captures the following in a Management Information Base (MIB). All are scalar objects.

MIB Objects

CuicGeneralInfo

This table contains a list of Unified Intelligence Center servers. An entry in this table represents a Unified Intelligence Center server in this cluster.

A row is created in this table whenever a new server is added to the cluster. A row is deleted when a server is removed from the cluster.

MIB	Description
cuicGeneralInfoSystemStatus	The last known status of the application. Status of the reporting service: • 'inService' = The service is up and running optimally, accepting connections. • 'partialService' = Some of the components comprising the application are not running; the service is in warning state. • 'notresponding' = The service is either shut down or not responding. • 'unknown' = The service status is unknown.
cuicGeneralInfoEnableNotifications	This object specifies the notification status to management station, to disable and alternatively enable outbound notifications on this server.

CuicReporting

The CuicReporting table lists the statistics of the Cisco Unified Intelligence Center Reporting nodes. A row is created in the CuicReporting table when a new server is added to the cluster. A row is deleted when a server is removed from this cluster.

MIB	Description
cuicReportingDataSourceCount	The number of Data Sources that are configured in the Cisco Unified Intelligence Center Reporting application.
cuicReportingEngineStatus	The last known status of the reporting engine: • 'running' = Service is running and can fetch data from the data source. • 'stopped' = Service is shutdown. • 'unknown' = The status is unknown.
cuicReportingHistoricalReportDefinitionCount	The number of historical report definitions installed on the Cisco Unified Intelligence Center application. A report definition is a template for a report. Each report has an association with a report definition.
cuicReportingRealTimeReportDefinitionCount	The number of real time report definitions installed on the Unified Intelligence Center application.
cuicReportingHistoricalReportRunning	The number of historical reports that are currently running.
cuicReportingHistoricalReportWaiting	The number of historical reports that are currently waiting to be run.
cuicReportingRealTimeReportRunning	Number of real time reports currently running.
cuicReportingRealTimeReportWaiting	The number of real time reports that are currently waiting to be run.

CuicDbInfo

This table gives the status of the Cisco Unified Intelligence Center database (cuic_data) and some performance monitoring counters.

The Cisco Unified Intelligence Center database exists on each node in the cluster and stores reports and configurations. The system replicates each Cisco Unified Intelligence Center database to other servers in a cluster.

Add a new row in the following table whenever a server is added to the cluster. Likewise, delete a row when a server is removed from the cluster.

MIB	Description
cuicDbInfoStatus	The status of the database server: • 'running' = The database server is up and running. • 'stopped' = The database server is shutdown. • 'unknown' = The database server is unknown.
cuicDbInfoReplicationStatus	The status of the last replication operation: • 'success' = Replication performed successfully. 'fail' = Replication failed. • 'unknown' = Failed to get replication status.
cuicDbInfoTmpSpaceUsed	The amount of temporary space used. The value is displayed in percentage.
cuicDbInfoSpaceUsed	The amount of disk space used. The value is displayed in percentage.

CuicClusterInfo

The table gives information about the Cisco Unified Intelligence Center cluster.

MIB	Description
cuicClusterName	The unique name of the cluster, which helps in associating a device with the cluster.
cuicClusterServerCount	Number of Cisco Unified Intelligence Center servers in the cluster.
cuicClusterFirstNodeName	The hostname of the first node in the cluster. This is the Controller (publisher) node.

CuicSecurity

This table gives information about Users and User Groups.

MIB	Description
cuicSecurityUsersConfigured	The number of users that have been created to access Unified Intelligence Center.
cuicSecurityUsersLoggedIn	The number of users currently signed in.
cuicSecurityGroupsConfigured	The number of user groups created on this server.

CuicDataSourceInfo

This table gives information for the data source from that populates a report.

An entry in this table describes a data source configured on the Unified Intelligence Center server. A row is created in this table when a new data source is configured on the server. A row is deleted when a configured data source is removed from the server.

cuicDatasourceName	The name of the data source configured.
cuicDatasourceStatus	The status of the data source: • 'online' = The data source is connected, and it is online. • 'offline' = The data source is disconnected, and it is offline. • 'unknown' = The data source connectivity status is unknown.
cuicDatasourceHost	The host name of the database server.
cuicDatasourceType	The data source type: • 'mssql' = MS SQL datasource. • 'informix' = IBM Informix datasource. • 'other' = Unknown datasource.

MIB Notifications (CUIC TRAPs)

Trap notifications are sent by Unified Intelligence Center when unusual conditions occur that can potentially affect the functioning of a Unified Intelligence Center service. Each Notification describes the operation state information of a service when the condition occurs. Review traps to review information on issues occurring on the network element without polling for SNMP objects.

cuicEventId	The unique notification message identifier assigned by the Unified Intelligence Center application. This identifier is unique for each different notification but consistent for each instance of the same notification.
cuicEventHostName	The host name or the fully qualified domain name of the Unified Intelligence Center server from which this event originated.
cuicEventAppName	The service-specific name of the functional service that generated this notification.
cuicEventName	The service-specific name of the Unified Intelligence Center service notification message, used to group and correlate similar notifications.
cuicEventState	The state (not to be confused with severity) of the notification and potentially the current state of the functional component that generated the notification. Values are: • 'raise' = Identifies a notification received as a result of a health-impacting condition, such as a process failure. A subsequent clear state notification will follow when the error condition is resolved. • 'clear' = Indicates that the condition which generated a previous raise notification has been resolved.

cuicEventSeverity	The severity level of this notification. The severity levels are: • 'emergency'= A devastating failure has occurred; the system or service is unusable. Immediate operator intervention is required. • 'alert' = A devastating failure is imminent that will render the system unusable. Immediate operator attention is necessary. • 'critical' = A service-impacting failure is likely to occur soon; an error has occurred that was not appropriately handled by the system. Operator attention is needed as soon as possible. • 'error' = Contains important operational state information and may indicate that the system has experienced a temporary impairment or an error that was appropriately handled by the system. An operator should review the notification soon to determine if action is needed. • 'warning' = Contains important operational state information that may be a precursor to an error occurrence. An operator should review the notification soon to determine if action is needed. • 'notice' = Contains health or operational state information that may be pertinent to the health of the system but does not require the attention of the administrator at this time. • 'informational' = Contains interesting system-level information that is valuable to an administrator, however, the event itself does not indicate a failure or impairment condition. • 'debug' = Provides supplemental information that may be beneficial toward diagnosing or resolving a problem but does not in itself provide operational health status.
cuicEventTimestamp	The date and time that the notification was generated on the originating device.
cuicEventText	The full text of the notification. This text includes a description of the event that was generated, component state information, and potentially a brief description of administrative action that may be necessary to correct the condition that caused the event to occur.

Event Name: CUIC_REPORT_EXECUTION_FAILED

Event Hostname	Hostname of the CUIC application.
Event Timestamp	Time when the SNMP trap was raised or cleared.
Event Severity	CRITICAL (3)
Event ID	61900
Event App Name	CUIC_DATA_PROCESSING
Event State	**1.** When the SNMP trap is raised. **2.** When the SNMP trap is cleared.

Event Text	The reporting server could not run a report. This could be because the associated datasource is offline - Worker thread: Error running report. Encountered a critical error trying to produce DataSet. Please check logs for more information.
Impact to Solution	You will not be able to run the report unless the underlying issue is resolved.
Recommended Action	**1.** Check if datasource used by report is online. **2.** Check if there is no error in the RD query or filter passed.

Event Name: CUIC_DB_REPLICATION_FAILED

Event Hostname	Hostname of the CUIC application.
Event Timestamp	Time when the SNMP trap was raised or cleared.
Event Severity	CRITICAL (3)
Event ID	61901
Event App Name	CUIC
Event State	**1.** When the SNMP trap is raised. **2.** When the SNMP trap is cleared.
Event Text	Database replication failed - Database replication service error.
Impact to Solution	Data across the nodes in the cluster may not be synchronized.
Recommended Action	**1.** Check the informix logs to see the cause of failure.

Event Name: CUIC_DATABASE_UNAVAILABLE

Event Hostname	Hostname of the CUIC application.
Event Timestamp	Time when the SNMP trap was raised or cleared.
Event Severity	CRITICAL (3)
Event ID	61902
Event App Name	CUIC
Event State	**1.** When SNMP trap is raised. **2.** When SNMP trap is cleared.
Event Text	System detected critical error with database - Informix DB server is unavailable: <informix error message>

Impact to Solution	User will not be able to run CUIC application.
Recommended Action	**1.** Check if the DB service is up and running. **2.** Check the informix logs to see the cause of failure.

Event Name: CUIC_INITIAL_REPORT_IMPORT_FAILED

Note Applicable only for CCX.

Event Hostname	Hostname of the CUIC application.
Event Timestamp	Time when the SNMP trap was raised or cleared.
Event Severity	CRITICAL (3)
Event ID	61905
Event App Name	CUIC_DATA_PROCESSING
Event State	**1.** When SNMP trap is raised. **2.** When SNMP trap is cleared.
Event Text	Failing to import initial setup stock report. This can be because the associated datasource is offline.
Impact to Solution	Few or all UCCX Stock reports will not be imported.
Recommended Action	**1.** Check the CUIC error logs to see the cause of failure. **2.** Check if datasource is offline. **3.** Check if there is no template issue. **4.** After correcting the issue try to re-import the templates manually.

Event Name: CUIC_MSG_DASHBOARD_MIGRATION_FAILED

Event Hostname	Hostname of the CUIC application.
Event Timestamp	Time when the SNMP trap was raised or cleared.
Event Severity	CRITICAL (3)
Event ID	61906
Event App Name	CUIC_DATA_PROCESSING

Event State	**1.** When the SNMP trap is raised. **2.** When the SNMP trap is cleared.
Event Text	Dashboard migration has failed for some widgets. Please check dashboard-migration-failures.log for more information.
Impact to Solution	Few of the widgets can be missing in the dashboard, post-upgrade to 11.6+.
Recommended Action	**1.** Check /opt/cisco/cuic/logs/dahsboard-migration-failures.log. **2.** Manually create missing widgets.

Event Name: CUIC_HAZELCAST_CLUSTER_BROKEN

Event Hostname	Hostname of the CUIC application.
Event Timestamp	Time when the SNMP trap was raised or cleared.
Event Severity	CRITICAL (3)
Event ID	61907
Event App Name—	CUIC
Event State	**1.** When the SNMP trap is raised. **2.** When the SNMP trap is cleared.
Event Text	Hazelcast cluster is broken.
Impact to Solution	Data across the nodes in the cluster may not be synchronized.
Recommended Action	**1.** Check the CUIC catalina log at the path - /opt/cisco/cuic/cuicsrvr/logs/catalina.outto identify the root cause for same.

ThreadPool Events

The thread pool information group defines the set of objects for the Unified reporting engine thread pool. All servers populate these objects.

Object	Description
ThreadsMaxAvailable	The maximum number of threads available to the Unified Intelligence Center web server thread pool manager.
ThreadsRunning	The number of threads that are currently running tasks. This counter is useful in monitoring performance of the server. If the number of threads is close to the maximum available, then the next reporting request must wait until a thread becomes free.

Object	Description
QueuedTasks	the number of queued tasks. A task is a job, performed by one or more thread.
QueuedTasksMax	The maximum number of queued tasks.

EnvInfo Events

The EnvInfo group defines the set of objects for the Runtime tomcat info. All servers populate these objects.

Object	Description
WaErrors	The total number of HTTP errors (for example, *401 Unauthorized*) encountered by a Unified Intelligence Center web application.
WaSessionsActive	The number of currently active (in use) sessions for the web application.
JvmPercentCPUTime	The percentage of CPU utilized by the Tomcat JVM. This object is for the Unified Intelligence Center Tomcat JVM object .
JvmMemoryFree	The amount of free dynamic memory in the Unified Intelligence Center Tomcat Java Virtual Machine.
JvmMemoryTotal	The Tomcat Java Virtual Machine current total dynamic memory, including free and in-use memory.
JvmMemoryMax	The Unified Intelligence Center Tomcat Java Virtual Machine maximum dynamic size.
TomcatThreadsBusy	The Unified Intelligence Center Tomcat Connector current number of busy/in-use request processing threads.
TomcatThreadsTotal	The Unified Intelligence Center Tomcat Connector current total number of request processing threads, including available and in-use threads.
TomcatThreadsMax	This object indicates the Connector maximum number of request processing threads. Each incoming request on a Unified Intelligence Center web page requires a thread for the duration of that request. If more simultaneous requests are received than can be handled by the currently available request processing threads, additional threads will be created up to the configured maximum shown in this counter.

Cisco Unified Intelligence OS Administration

Configure Custom Logon Messages

With release 12.6(1), Cisco Unified Intelligence Center lets the administrator configure the custom logon messages displayed when the users sign in.

To configure the custom message using Cisco Unified OS Administration console, perform the following steps:

Note The custom message can be uploaded to the server as a text file.

By default, there is no custom message configured. However, it is not mandatory to configure the message.

Procedure

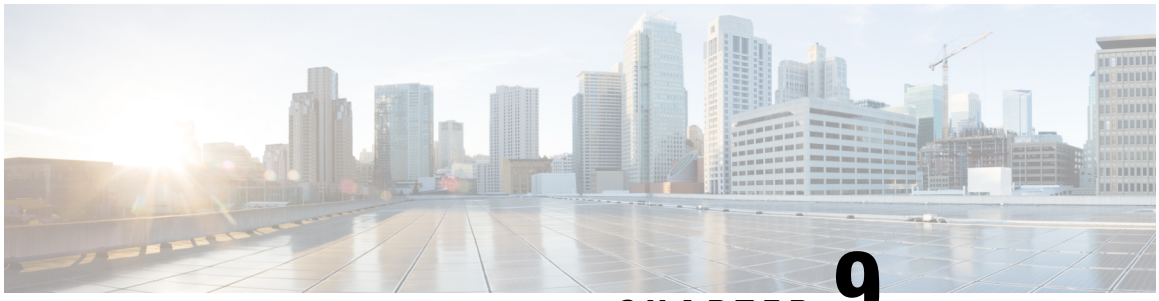
Step 1 Log in to **Cisco Unified OS Administration**.

Step 2 Navigate to **Software Upgrades** > **Custom Logon Message**.

Step 3 Click **Choose File**, to upload the customized message file.

Step 4 Select the file and click **Open**.

Step 5 Click **Upload File**.



CHAPTER 9

Manage Certificates

- Install Certificate Authority (CA) Certificate, on page 95
- CUIC Server Certificates, on page 96
- Access Platform Web Applications using Chrome Browser, on page 96

Install Certificate Authority (CA) Certificate

To install or upload certificates on the Cisco Unified Intelligence Center server, perform the following steps:

Procedure

Step 1	Log in to Cisco Unified Operating System Administration.
Step 2	Navigate to **Security** > **Certificate Management**. The **Certificate List** window appears.
Step 3	Click **Generate CSR**. The **Generate Certificate Signing Request** dialog box opens.
Step 4	Select **tomcat** from the Certificate Purpose list.
Step 5	Click **Generate** to generate a certificate from a custom or third-party certificate authority.
Step 6	Click **Close**.
Step 7	Click **Download CSR**.
Step 8	In the **Download Certificate Signing Request** screen, click **Download CSR** to download the Certificate Signing Request to your computer.
Step 9	Use this CSR to obtain the Public certificate and Primary certificate from the Certificate Authority.
Step 10	Log in to OS platform again and navigate to **Security** > **Certificate Management**.
Step 11	Click **Upload Certificate/Certificate chain**. The **Upload Certificate/Certificate chain** dialog box opens.
Step 12	To upload the certificate chain, select **tomcat** from the **Certificate Purpose** list.
Step 13	Select the file to upload. Click the **Choose File** button and navigate to the file; then, click **Open**.
Step 14	Click **Upload**.
Step 15	After successfully uploading the certificate, navigate to **Security** > **Certificate Management**.
Step 16	Click **Find** to open the list of certificates.
Step 17	Click on the uploaded certificate to view **Certificate File Data**.
Step 18	Restart the node(s) using the CLI command *utils system restart*.

Note

- To upload a custom certificate with alternate hostname, set the alternate hostname using the CLI command *set web-security*. Configure the alternate hostname and use the procedure above to generate Certificate Signing Request (CSR) and to upload the certificates. You can access Cisco Unified Intelligence Center by using the alternate hostname as well.
- To avoid the certificate exception warning, you must access the servers using the Fully qualified domain name (FQDN) name. That is, leave the **Distribution** field in the CSR as the FQDN of the server.
- Ensure that the Certificate Authority (CA) certificate is RSA-signed.
- Cisco Unified Intelligence Center CSR certificates are signed with *sha1WithRSAEncryption* using a 2048-bit RSA public key.
- Cisco Unified Intelligence Center does not support wildcard certificates.

CUIC Server Certificates

Two server certificates — *intelligencecenter-jms* and *intelligencecenter-srvr*, even though available, are not used anymore. There is no impact even if these certificates expire, and it is not required to regenerate them.

Access Platform Web Applications using Chrome Browser

This section is applicable only if you are using Chrome based browsers (Google Chrome or Edge Chromium) to access the Platform web applications, such as Cisco Unified OS Administration, Cisco Unified Serviceability or Disaster Recovery System.

This section is also applicable for Cisco Unified Intelligence Center Administration web application on CUIC nodes.

If you are using self-signed certificates, add the certificates to the Client OS trust store to access the administrative web applications.

Note Chrome needs the self-signed certificate to have **Subject Alternative Name** extension to load the administrative web applications. If the self-signed certificate does not have **Subject Alternative Name**, regenerate the certificate from Cisco Unified OS Administration.

Download the Server Certificate from CUIC Node

This section provides instructions to download the server certificate from CUIC node.

Before you begin

Run the *show server tls cert_type* command on your server and identify the certificate type that your server uses. For more information see show tls server cert_type, on page 146

Procedure

Step 1 Log in to the **Cisco Unified OS Administration** page using the URL: *https://<FQDN>:8443/cmplatform*

Step 2 Go to **Security** and select **Certificate Management**.
The **Certificate List** screen appears.

Step 3 In **Find Certificate List where** do the following:

a) Select **Common Name** in the first dropdown.
b) Select **begins with** in the second dropdown.
c) Enter the host name of the node in the search box.
d) Click **Find**.
The list of **Certificates** is displayed with their **Common Name** and **Key Type**. For ECDSA, the **Key Type** is **EC** and for RSA, the **Key Type** is **RSA**.

Step 4 Based on the certificate type required for your server, click the **Common Name** link of the **tomcat-trust** certificate in the search result.

Step 5 In the new window, click **Download .DER File** or **Download .PEM File** and save it.

Add Certificate to Trusted Root Certification Authorities on Windows Client System

To add the certificate to the Trusted Root Certification Authorities on Windows Client system, do the following:

Procedure

Step 1 In the **Control Panel** search for **Manage User Certificates** and click **Manage User Certificates**.
The **certmgr - [Certificates - Current User]** window appears.

Step 2 Select **Certificates - Current User** > **Trusted Root Certification Authorities** > **Certificates**.

Step 3 Right-click **Certificates** and click **All Tasks** > **Import** and then click **Next**.

Step 4 Browse and select the downloaded certificate file, click **Next** and then click **Finish**.

Step 5 In the **Security Warning** window, click **Yes**.

A window pops up to confirm that the import was successful.

Close the **Manage User Certificates** window and close all browser sessions.

Reopen the Chrome browser and clear the browser cache. Log in to the platform web application.

For example: *https://<FQDN>:8443/cmplatform*. The Chrome browser now shows the lock symbol to indicate that it is a trusted connection.

Add Certificate to Keychain Access in Mac Client Machine

This section is applicable for Mac OS Catalina version 10.15 and above. To add the certificate to Keychain Access in Mac Client machine, do the following:

Procedure

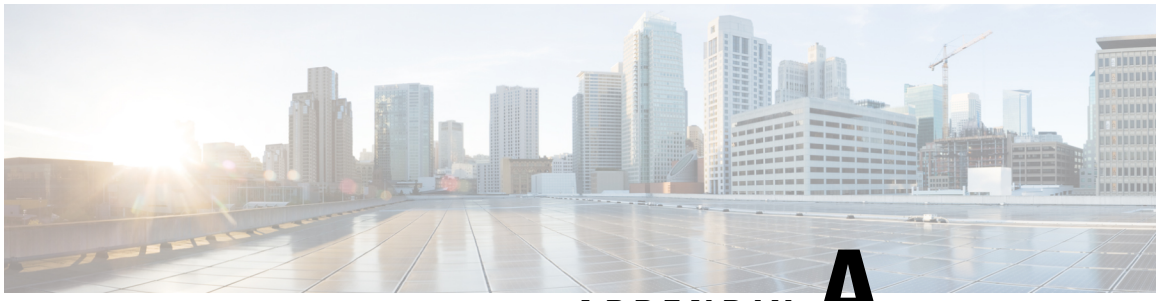
Step 1 On the Mac client machine, under **Applications** > **Utilities** select **Keychain Access**.

Step 2 In the left pane, select **System** and from the center pane, select the **Certificates** tab.

Step 3 Drag and drop the downloaded certificate on to the list of displayed certificates. (Provide the credentials for authentication, if prompted.)

Step 4 Double-click the newly imported certificate and click the expand icon beside **Trust**.

Step 5 In **When using this certificate** dropdown, select **Always trust** and close the window.



APPENDIX A

Command Line Interface

The Command Line Interface (CLI) provides a set of commands applicable to the operating system, to the Unified Intelligence Center database (*cuic_data*) and to the system database (*ccm_<version>*).

These commands allow basic maintenance and failure recovery and also enable some system administration when the Unified Intelligence Center operations console is unavailable.

You can access the CLI directly, using the monitor and keyboard at the server console:

1. Enter the ID for the System Administration user (the one created during install).
2. When prompted, enter the password for the System Administration user.

In addition to the CLI commands listed in this chapter, you can also enter:

- **help** - to display the list of all supported commands. For example, to display help for a specific command, type `help delete dns` and press Enter.
- **quit** - to close the CLI.

In the command syntax descriptions:

bold is used for the base command.

italics are used for mandatory parameters, when the syntax includes them.

[ ] brackets are used for options, when the syntax includes them.

- Unset Command, on page 100
- Utils Command, on page 101
- Show Commands, on page 129
- Set Commands, on page 147
- Run Commands, on page 160
- file commands, on page 161
- Delete Commands, on page 164
- Use CLI, on page 165

Unset Command

unset cuic properties

Use this command to remove the translation of host-to-ip setting.

Command Syntax
unset cuic properties host-to-ip *hostname*

unset ipsec

Use these commands to disable ipsec policies.

Command Syntax
unset ipsec policy_group [{*groupall*}]
Use to disable all policies within a group or all groups.

Command Syntax
unset ipsec policy_name [*policy_group*] [*policy_name*]
Use to disable a policy with a given policy name and group. For example, set ipsec policy_name group1 name1.

unset network dns

Command Syntax
unset network dns options [*options*]
This command removes the DNS options setting and causes a temporary loss of network connections.

OPTIONS:

[timeout] sets the wait time before the system considers a DNS query failed to the default.

[attempts] sets the number of DNS attempts to make before failing to the default.

[rotate] sets the method for selecting a nameserver to the default. This affects how loads are distributed across nameservers.

Command Syntax
unset ipv6 [*policy_group*] [*policy_name*]
These commands disable the policy group or all groups, or a policy with a specified group and name.

unset_host-to-ip

Use this command to remove any host-to-ip configurations that were defined with the command set cuic properties, on page 149.

Running this command removes the node-specific override for the IP address of the Unified CCE databases and reverts to the default for the Unified CCE databases as configured in the Data Sources page.

Command Syntax
unset_host-to-ip

Utils Command

utils auditd

These commands display enable, disable, and show the status of the audit daemon.

When enabled, auditd log files for the system are retrievable through RTMT. The auditd system monitors for specific security sensitive system calls at the OS kernel level and provides a record-keeping trail for such activities as file permission changes, failures to manipulate files due to permission settings, and changes to the system time and name.

Command Syntax
utils auditd disable
utils auditd enable
utils auditd status

utils core

These commands display information for core files.

Command Syntax
utils core analyze *core_file_name*
This command displays backtrace for the specified core file.

PARAMETER *core_file_name*.

Command Syntax
utils core list
This command lists existing core files.

utils create report

These commands create a system report. If you specify hardware, the report contains disk array, remote console, diagnostic, and environmental data.

If you specify platform, the system collects the platform configuration files and copies them to a common log location.

As these reports take time to complete, the system prompts for a confirmation.

Command Syntax
utils create report hardware
utils create report platform

utils cuic

utils cuic cpudiagnostics

This command is to monitor cuic tomcat process continuously and report the CPU usage per thread. It uses a combination of top and jstack commands to find out CPU usage at thread level and merge the results into the standard jstack output.

Command Syntax
utils cuic cpudiagnostics enable <max_cpu>

This command is to enable cpu diagnostic process.

PARAMETERS:

Max CPU usage at which to log thread details, max_cpu should be between 50 to 90. Default value is "50"

Command Syntax
utils cuic cpudiagnostics disable

This command line is to disable the cpudiagnostics process.

utils cuic mbeans

Command Syntax
utils cuic mbeans *[_c] [_e] [_i <val>] [_l <val>] [_n] [_o <val>] [_p <val>] [_u <val>] [_v <val>] [_x <val>]*

PARAMETERS:

_e,__exitonfailure With this flag, terminal exits for any Exception

_i,__input <val> Input script file. There can only be one input file. Default value is "stdin"

_l,__url <val> Location of MBean service. It can be <host>:<port> or full service URL.

_n,__noninteract Non interactive mode. Use this mode if input doesn't come from human or jmxterm is embedded

_o,__output <val> Comma separated output list, file and/or stdout. Default value is "stdout".

_p,__password <val> Password for user/password authentication

_u,__user <val> User name for user/password authentication

_v,__verbose <val> Verbose level, could be silent|brief|verbose. Default value is "brief".

_x,__execute <val> Executes a command (a connection must be opened first with _l)

Note Without any option, this command opens an interactive command line based console. With a given input file, commands in file are run and process ends after file is processed. The execute option may be used to run a command directly, without opening the interactive command line. If the command requires an open connection, it must be opened with _l. Quotes may be used to group words in the command and any dashed arguments use underscore instead.

utils cuic nmon

Command Syntax
utils cuic nmon start *s [seconds] c [count]*

PARAMETERS:

s specifies the time interval (in seconds) between each collection.

c specifies the number of collections that you want to invoke. Each collection takes up about one Kilobyte of disk space.

Command Syntax
utils cuic nmon stop
This command stops the nmon capture. The data that is captured in this nmon session is savedin/common/log/installin nmon_output.nmonfile.

utils cuic purge

This command runs a manual purge of the cuic database tables. You might do this if you receive an alert that the database is nearing capacity and you do not want to wait for the daily automatic purge.

The tables purged are:

- CuicDataSetInfo
- CuicDataSet
- CuicReportDefinitionFilter
- CuicReportDefinitionFilterField
- CuicReportDefinitionFilterParameter
- CuicCollection
- CuicCollectionValue

This command prompts for the password of the administration user. When the password is confirmed, the purge runs immediately.

utils cuic restorepub

This command restores security files like keypassfile and cuickeystore files from subscriber to publisher in the same cluster.

Command Syntax
utils cuic restorepub

PARAMETERS:

No optional parameters.

utils cuic cors

Important After you make changes to the CORS status, allowed origins list, exposed header, or allowed header, restart Cisco Intelligence Center Reporting Service for changes to take effect. All CLIs are node-specific and must be run on all nodes in the cluster.

Command Syntax
utils cuic cors enable

This command enables Cross Origin Resource Sharing (CORS) support in Unified Intelligence Center.

Note For Unified Intelligence Centre gadgets (Live Data and Historical) to load in Cisco Finesse, ensure to:

- Enable CORS using the `utils cuic cors enable` command.
- Set the Finesse host URL in the `utils cuic cors allowed_origin add URLs` command.

  Examples:

  - https://<finesse-FQDN>
  - https://<finesse-FQDN>:port

For Live Data gadgets, in addition to the above settings, ensure to enable CORS using the **utils live-data cors enable** command and set the Finesse host URL in the **utils live-data cors allowed_origin add URLs** command. For more information, see *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Command Syntax
utils cuic cors disable

This command disables CORS support in Unified Intelligence Center.

Command Syntax
utils cuic cors status

This command displays the current CORS status in Unified Intelligence Center.

Command Syntax
utils cuic cors allowed_origin list

This command displays the list of allowed URLs that can make CORS requests to Unified Intelligence Center.

Command Syntax
utils cuic cors allowed_origin add <URL1,URL2,URL3>

Parameter: Comma-separated list of URLs (without spaces) that has to be added to the allowed origins list.

The URL format: *http[s]://<hostname>[:port]*

This command adds the given set of comma-separated URLs to the allowed origins list.

Command Syntax
utils cuic cors allowed_origin delete

This command prompts for a choice to delete a particular allowed origin URL or all the allowed origin URLs.

utils cuic cors allowed_origin delete

1. http://google.com

2. http://www.cisco.com

a: all

q: quit

Select the index of origin to be deleted [1-2 or a,q]

Command Syntax
utils cuic cors allowed_headers list

This command lists all the configured allowed headers for CORS. This list is used to validate incoming requests to CUIC.

Command Syntax
utils cuic cors allowed_headers add <header1,header2,header3>

Parameter: Comma-separated list of headers (without spaces) that have to be added to the allowed headers list.

This command adds one or multiple allowed headers for CORS. You can add multiple headers using a comma-separated string.

Command Syntax
utils cuic cors allowed_headers delete

This command prompts for a choice to delete a particular custom allowed header or all the custom allowed headers.

utils cuic cors allowed_headers delete

1: header1

2: header2

a: all

q: quit

Select the index of allowed header to be deleted [1-2 or a, q]: 1

Command Syntax
utils cuic cors exposed_headers list

This command lists the response headers available for a client.

Command Syntax
utils cuic cors exposed_headers add <header1,header2,header3>

Parameter: Comma-separated list of headers (without spaces) that have to be added to the exposed headers list.

This command adds one or multiple exposed headers for CORS. You can add multiple headers using a comma-separated string.

Command Syntax
utils cuic cors exposed_headers delete

This command prompts for a choice to delete a particular custom exposed header or all the custom exposed headers.

utils cuic cors exposed_headers delete

1: header1

2: header2

a: all

q: quit

Select the index of exposed header to be deleted [1-2 or a, q]: 1

utils cuic session

utils cuic session list

This command lists the current Cisco Unified Intelligence Center sessions.

Command Syntax
utils cuic session list

Options

No parameters

Example

```
admin:utils cuic session list
Command run successfully
Session ID details saved to file.
To view file, type "file view activelog cuic-session.out"
To SFTP file, type "file get activelog cuic-session.out"
```

utils cuic session delete

This command deletes the Cisco Unified Intelligence Center sessions based on the username that you pass to this command.

Command Syntax
utils cuic session delete <username 1,username 2>

Parameter

Usernames are names of the currently logged in users of the current Cisco Unified Intelligence Center sessions.

To get the current usernames, you must first run the `utils cuic session list` command and then run `file view activelog cuic-session.out` command.

Example

```
admin:utils cuic session delete CUIC\administrator
Session Deleted successfully
```

utils cuic cluster show

This command shows the current cluster mode enabled on this node and the other member details.

Note The member details are available only in the TCP/IP mode. The member details displayed are of the configured members and does not represent the cluster in real-time.

Command Syntax
utils cuic cluster show

utils cuic cluster mode

This command is used to switch the CUIC cluster join configuration from Multicast to TCP/IP and vice versa.

Note After changing the cluster mode in all the nodes, restart “Intelligence Center Reporting Service ” in all the nodes starting from the publisher sequentially.

Command Syntax
utils cuic cluster mode

utils cuic cluster refresh

This command refreshes the cluster node information only when run in the TCP/IP mode and must be run when there is an addition or deletion of nodes to the CUIC cluster.

Command Syntax
utils cuic cluster refresh

utils cuic logging

The **utils cuic logging** commands update or display the configuration only on the nodes on which the commands are run. To change the logging configuration on each node in the cluster, you must run the command separately on each node.

utils cuic logging config set

This command sets the value for log file configuration.

Command Syntax
utils cuic logging config set [config-name] [config-value]

Options

- [config-name] - mandatory log file configuration name

  Valid configuration names are `max-file-size`, `max-file-count`, `syslog-primary-host` and `syslog-secondary-host`. The maximum limit of `max-file-size` and `max-file-count` is 50 MB and 50 respectively.

  Only one [config-name] option can be set at a time.

- [config-value] - mandatory log file configuration value. For `syslog-primary-host` and `syslog-secondary-host` configuration names, the configuration values are the primary syslog server hostname and the secondary syslog server hostname, respectively.

utils cuic logging config show

This command prints the current log configuration for the given configuration name.

Command Syntax
utils cuic logging config show [config-name]

Options

[config-name] - mandatory log file configuration name

Valid configuration names are `max-file-size`, `max-file-count`, `syslog-primary-host` and `syslog-secondary-host`.

Only one [config-name] option can be printed at a time.

utils cuic logging config clear

This command clears the log file configuration for the primary and secondary syslog servers.

Command Syntax
utils cuic logging config clear [config-name]

Options

[config-name] - mandatory log file configuration name

Valid configuration names are `syslog-primary-host` and `syslog-secondary-host`.

Only one [config-name] option can be cleared at a time.

utils cuic logging list

This command lists the module and the logging level for the specified module. If a module name is specified, the logging level is displayed only for that module.

Command Syntax
utils cuic logging list [module-name]

Options

[module-name] - optional

Possible module names for which, the log levels can be printed are as follows:

```
REPORT, REPORTENGINE, REPORTDEFINITION, SCHEDULER, DASHBOARD, AUTHORIZATION, AUTHENTICATION,
VALUELISTCOLLECTION, SECURITY, CUICUI, DATASOURCE, CUICCONFIG
```

utils cuic logging reset

This command resets any modifications done to the logging configuration to the default value. For all the modules, the default value is `Info`.

Command Syntax
utils cuic logging reset

Options

No parameters

utils cuic logging update

This command updates the log level for the given module name.

Command Syntax
utils cuic logging update [module-name] [log-level]

Options

- [module-name] - mandatory

  Possible module names are as follows:

  ```
  REPORT, REPORTENGINE, REPORTDEFINITION, SCHEDULER, DASHBOARD, AUTHORIZATION,
  AUTHENTICATION, VALUELISTCOLLECTION, SECURITY, CUICUI, DATASOURCE, CUICCONFIG
  ```

- [log-level] - mandatory

  New log level for the module. Valid log-level values are as follows:

  ```
  ERROR, WARN, INFO, DEBUG
  ```

utils cuic user make-admin

This command provides all the roles to the new user and copies all the permission from the administrator to the user.

Command Syntax
utils cuic user make-admin

PARAMETERS:

domain\username

domain\username should be the complete username, including the prefix, as listed in CUIC User List page.

utils dbreplication

utils dbreplication clusterreset

This command is used to reset replication on an entire cluster.

Caution Before executing this command, run the command `utils dbreplication stop` on all Member nodes and then on the publisher (the Controller node).

Command Syntax
utils dbreplication clusterreset

utils dbreplication dropadmindb

This command is used to drop the Informix syscdr database on any server in the cluster.

Caution Run this command only if the command `utils dbreplication reset` or `utils dbreplication clusterreset` fails and replication cannot be restarted.

Command Syntax
utils dbreplication dropadmindb

utils dbreplication rebuild

This command is used to set up database replication across the cluster. This command can only be run from the publisher. This command will run the following commands on the specified nodes:

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

Command Syntax
utils dbreplication rebuild *{ [nodename] | | all }*

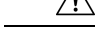
utils dbreplication repair

This command repairs mismatched data on a named node or between nodes. It does not repair replication setup.

Command Syntax
utils dbreplication repair nodename
utils dbreplication repair all

utils dbreplication reset

This command is used to reset replication.



Caution Run this command only when replication setup has failed after an install or upgrade.

Before running this command, you must run `utils dbreplication stop`. If resetting all, stop replication on all nodes first. If resetting <nodename>, stop replication on that node first.

Command Syntax
utils dbreplication reset all
utils dbreplication reset nodename

utils dbreplication runtimestate

This command is used to monitor progress of the database replication process and provides replication state in the cluster.

Command Syntax
utils dbreplication runtimestate *nodename*

OPTION: [nodename} limits the status to that of the node indicated.

utils dbreplication setrepltimeout

Use this command to increase the default timeout for replication setup on large clusters.

The default timeout is 5 minutes, thus all subscribers requesting replication within 5 minutes will be on the broadcast list and will be replicated.

Command Syntax
utils dbreplication setrepltimeout *nteger value of new timeout in seconds*

PARAMETER: *integer value of new timeout in seconds* must be between 300 and 3600 seconds.

utils dbreplication status

Use this command to view status of database replication after setup is complete. To monitor status during setup, use RTMT.

Command Syntax
utils dbreplication status

utils dbreplication stop

This command is used to stop the automatic setup of database replication and to stop the ongoing setup of replication.

Run this command on each node where replication needs to be stopped.

Run on all Member nodes first and then on the publisher (the Controller node).

Run this command with no parameters to run the stop operation on the local node only.

On the publisher, run this command as `stop all` or `stop nodename` to run the stop operation on all nodes or on a named node.

Command Syntax
utils dbreplication stop all
utils dbreplication stop nodename

utils diagnose

Use these commands for various diagnostic functions.

Command Syntax
utils diagnose fix
This command runs diagnostic tests, displays the results, and if possible, attempts to repair the system.

Command Syntax
utils diagnose list
This command lists all available diagnostic commands.

Command Syntax
utils diagnose module *module name*
This command runs a test on a named module test and attempts to fix the problem if possible.

Command Syntax
utils diagnose test
This command runs diagnostic tests and displays the results.

Command Syntax
utils diagnose version
This command displays the version of the diagnostics system.

utils disaster_recovery

utils disaster_recovery backup

This command invokes a backup and makes the tar file on the network drive or the tape.

Command Syntax
utils disaster_recovery backup network *<featurelist> <path> <servername> <userid >*

PARAMETERS:

featurelist indicates the comma-separated feature list to back up. Use the command **utils disaster_recovery show_registration** to display the list of registered features.

path indicates the path to save back up files.

servername is the server ip/hostname where the backup file is to be stored.

userid is the user id used to connect to the remote machine.

utils disaster_recovery backup tape *<featurelist><tapeid>*

PARAMETERS:

featurelist indicates a comma-separated feature list to back up.

tapeid indicates the tape ID to back up the files. Use the command utils **disaster_recovery show_tapeid** to display the list of tape IDs.

utils disaster_recovery cancel_backup

This command cancels an ongoing backup.

Command Syntax
utils disaster_recovery cancel_backup *confirm*

confirm is mandatory and prompts you to enter Yes/Y to continue or any other key to stop.

utils disaster_recovery device

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

This command adds the backup network device.

PARAMETERS :

devicename: Specifies the name of the backup device to be added (mandatory).

path : Specifies the path to retrieve the backup device (mandatory).

server_namei/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 location.

Number_of_backups : Specifies the number of backups to store on the Network Directory (default 2). This parameter is optional.

Command Syntax
utils disaster_recovery device delete *device_name* *

This command deletes the specified device.

PARAMETERS :

device_name: Name of the device to be deleted .

* : Deletes all existing devices except for the ones associated to a schedule

Command Syntax
utils disaster_recovery device list

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

utils disaster_recovery estimate_tar_size

Command Syntax
utils disaster_recovery estimate_tar_size *featurelist*

PARAMETERS:

featurelist indicates the comma separated feature list to backup. Use **utils disaster_recovery show_registration <servername>** to display the list of registered features.

utils disaster_recovery history

This command displays the history of previous backups and restores.

Command Syntax
utils disaster_recovery history *[operation]*

operation specifies backup and restore.

utils disaster_recovery jschLogs

Command Syntax
utils disaster_recovery jschLogs *operation*

PARAMETERS:

operation name of operation like Enable\Disable.

utils disaster_recovery prepare

This command prepares for backup and restore from publisher and subscriber.

Command Syntax
utils disaster_recovery prepare restore

Command Syntax
utils disaster_recovery prepare restore pub_from_sub

utils disaster_recovery restore

These commands invoke a restore.

Command Syntax
utils disaster_recovery restore network *<restore_server> <tarfilename> <path> <servername> <userid>*

PARAMETERS:

restore_server is the hostname of the server to be restored.

tarfilename is the tar file name to be restored.

path is the mandatory path that retrieves the backup tar file from this location.

servername is the server ip\hostname from which to retrieve backup tar file.

userid is the user id used to connect to the remote machine.

Command Syntax
utils disaster_recovery restore tape *<server><tarfilename> <tapeid>*

PARAMETERS

server is the hostname of the server to be restored.

tarfilename is the tar file name to be restored.

tapeid is the tape ID used to restore files from the tape device. Use the command **utils disaster_recovery show_tapeid** to display the list of tape IDs.

utils disaster_recovery show_backupfiles

These commands retrieve information about backup files.

Command Syntax
utils disaster_recovery show_backupfiles network *<path> <servername> <userid>*

PARAMETERS:

path indicates the location of the backup file.

servername is the server ip/hostname where the backup file has been stored.

userid is the user id used to connect to the remote machine.

Command Syntax
utils disaster_recovery show_backupfiles tape *tapeid*

PARAMETER: *tapeid* is the ID of the tape device.

utils disaster_recovery show_registration

This command shows all the registered features and components on a given server.

Command Syntax
utils disaster_recovery show_registration

utils disaster_recovery show_tapeid

This command shows the list of tape IDs.

Command Syntax
utils disaster_recovery show_tapeid

utils disaster_recovery status

This command shows the status of the ongoing backup or restore operation.

Command Syntax
utils disaster_recovery status *operation*

PARAMETER *operation* is the name of the operation: backup or restore.

utils firewall

These commands perform various actions pertaining to the firewall.

Command Syntax
utils firewall disable [*time*]
utils firewall enable

utils firewall list
utils firewall status

OPTION: [time} is the duration in seconds for which the firewall is to be disabled.

utils firewall ipv4

These commands perform various actions pertaining to the firewall ipv4.

Command Syntax
utils firewall debug [*off* \\ *time*]

PARAMETERS:

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.

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 Syntax
utils firewall disable [*time*]

disable Turns off the IPv4 firewall. If you do not enter the time parameter, this command disables the firewall for 5 minutes.

Command Syntax
utils firewall enable [*time*]

enable Turns on the IPv4 firewall.

Command Syntax
utils firewall list

This commands displays the current configuration of the IPv4 firewall.

Command Syntax
utils firewall status

This command displays the current status of the IPv4 firewall.

utils firewall ipv6

These commands perform various actions pertaining to the firewall ipv6.

Command Syntax
utils firewall debug [*off* \\ *time*]

PARAMETERS:

This command turns IPv6 firewall debugging on or off. If you do not enter a time parameter, this command turns on debugging for 5 minutes.

off Turns off the IPv6 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 Syntax
utils firewall disable [*time*]

disable Turns off the IPv6 firewall. If you do not enter the time parameter, this command disables the firewall for 5 minutes.

Command Syntax
utils firewall enable [*time*]

enable Turns on the IPv6 firewall.

Command Syntax
utils firewall list

This commands displays the current configuration of the IPv6 firewall.

Command Syntax
utils firewall status

This command displays the current status of the IPv6 firewall.

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 will reboot after the command successfully completes.

Command Syntax
utils import config

PARAMETERS: None

REQUIREMENTS:

Command privilege level: 1

Allowed during upgrade: Yes

USAGE GUIDELINES

To run this command on a VMware deployment that has been cloned (copied) from a template:

1. Power on the VM.
2. Use the Answer File Generator (AFG) tool. For more information, see https://www.cisco.com/c/en/us/applicat/content/cuc-afg/index.html.

3. Insert the Config.xml file into a virtual floppy instance. For more information, see https://kb.vmware.com/s/article/1739.
4. Mount the .flp file in the floppy drive of the new VM.
5. Log in to the CLI of the VM (using console or SSH) and run the utils importconfig 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.

Note If the platformConfig.xml file contains a new IP address for the publisher, refer to the section *Change Cluster IP Address for Publisher Server Defined by IP Address* in Chapter 3 and perform Step1 on all subscriber nodes before running this CLI from the publisher node.

Note If the platformConfig.xml file contains a new IP address for the subscriber, refer to the section *Change Cluster IP Address for Subscriber Servers Defined by IP Address* in Chapter 3 and perform Step 1 to Step 4 on the publisher node before running this CLI from the subscriber nodes.

utils iostat

This command provides the iostat output for the given number of iterations and interval.

Command Syntax
utils iostat [*options*]

OPTIONS:

[interval] indicates the interval in seconds. Mandatory if iterations is also used.

[iterations] indicates the number of iostat iterations to be performed. Mandatory if interval is also used.

[filename] redirects the output to a file.

utils iothrottle

These commands enable, disable, or show status of I/O throttling enhancements.

Command Syntax
utils iothrottle disable
utils iothrottle enable
utils iothrottle status

utils netdump

This command enables, disable and displays status of the netdump.

Command Syntax
utils netdump enable

Command Syntax
utils netdump disable

Command Syntax
utils netdump status

utils netdump client

These commands configure the netdump client.

Command Syntax
utils netdump start *ip-address-of-netdump-server*
This command starts the netdump client.

PARAMETER *ip-address-of-netdump-server* specifies the IP address of the netdump server to which the client will send diagnostic information.

Command Syntax
utils netdump status
This command starts the netdump client.

Command Syntax
utils netdump status
This command displays the status of the netdump client.

utils network

utils network arp

This command lists, sets, or deletes Address Resolution Protocol (ARP) table entries.

Command Syntax
utils network arp delete *host*
This command deletes an entry in the address resolution table.

host represents the host name or IP address of the host to delete from the table.

Command Syntax
utils network arp list [*options*]
This command lists the contents of the address resolution protocol table.

OPTIONS:

[host host] is the host and host name to list.

[page] displays the output one page at a time.

[numeric] displays hosts as dotted IP addresses.

Command Syntax
utils network arp set <*host*> <*address*>
This command sets an entry in the address resolution protocol table.

<*host*> is the name or dotted IP address of the host to add to the table.

<*address*> is the hardware address (MAC) of the host to be added.

utils network capture

This command captures IP packets on the ethernet interface.

Command Syntax
utils network capture [*options*]

OPTIONS:

[page] pauses output.

[numeric] show hosts as dotted IP addresses.

[file fname] outputs the information to a file saved in platform/cli/fname.cap.

[count num] indicates a count of the number of packets to capture.

[size bytes] indicates a count of the number of packets to capture. Note: The maximum count for the screen is 1000; for a file it is 100000.

[src addr] indicates the source address of the packet as a host name or IPV4 address.

[dest addr] indicate the destination address of the packet as a host name or IPV4 address.

[port num] indicates the port number of the packet (either src or dest).

[host protocol] indicates the host address of the packet as a host name or IPV4 address. This option will display all packets to and from that address. Note: If "host" is provided, do not provide "src" or "dest".

utils network connectivity

This command is valid only on a subscriber (Member) node. It tests the network connectivity from this system to the publisher node (the Controller node).

Command Syntax
utils network connectivity

utils network host

This command resolves a hostname to an address, or an address to a hostname. This command looks for the host locally first. If it cannot resolve it locally, and DNS is configured, then it does a DNS lookup.

Command Syntax
utils network host *name*

PARAMETER *name* is the name of the host or address to resolve.

utils network ping

This command sends one or more ping packets to a remote destination.

Command Syntax
utils network ping *dest* [*count*]

PARAMETER *dest* is the dotted IP or host name of the destination.

OPTION [count] is the optional count value (default is 4).

utils network tracert

This command traces IP packets to a remote destination.

Command Syntax
utils network tracert *dest*

PARAMETER *dest* is the dotted IP or host name of the destination.

utils network ipv6

Command Syntax
utils network ipv6 host *{host_name \ ipv6_address}*

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

host_name Specifies the name of the server.

ipv6_address Specifies the IPv6 address of the server.

Command Syntax
utils network ipv6 traceroute *{ ipv6-address \ address}*

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

hostname Specifies the host name that you want to trace.

ipv6-address Specifies IPv6 address that you want to trace.

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

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

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.

utils ntp

This command displays the NTP status or configuration.

Command Syntax
utils ntp status
utils ntp config

Command Syntax
utils ntp restart

Command Syntax
utils ntp server add*s1 [s1| s2| s3| s4| s5] [norestart]*

The command adds a maximum of five specified NTP servers.

PARAMETERS:

s1... Specifies the NTP servers.

norestart Causes the NTP service to not restart after you add the servers.

Command Syntax
utils ntp server delete

This command deletes NTP servers that are configured.

Note The following warning message, `changing this setting will invalidate the software licence` is not applicable to Cisco Unified Intelligence Center and can be ignored.

Command Syntax
utils ntp server list

This command lists all NTP servers.

Command Syntax
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 raid disk maintenance

Use these commands to maintain the RAID disk. They are needed only on servers using RAID software.

Command Syntax
utils raid disk maintenance disable
This command stops the scheduled RAID service.

Command Syntax
utils raid disk maintenance enable
This command verifies the RAID scheduling.

Command Syntax
utils raid disk maintenance status
This command gives the status for the weekly scheduled RAID software disk verify service.

utils remote_account

These commands create, enable, disable, and show the status of a remote account.

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

Command Syntax
utils remote_account create <*account*> <*life*>

account is the account name.

life indicates the life of the account in days.

utils remote_account disable
utils remote_account enable
utils remote_account status

utils_reset

These commands reset user names and passwords.

Command Syntax
utils reset_application_ui_administrator_name
Use this command to reset the application user name. The application user is the initial Super User who can sign in to the Administration console.

This command prompts for the new name.

Make sure to do the following while running this command:

1. Run this command only when replication is running.
2. Wait for 10 to 15 minutes to ensure that the user name is reset across all nodes.
3. Restart the Cisco Unified Intelligence Center application on all nodes to complete the process.

Warning If you log in to the Cisco Unified Intelligence Center application without completing these steps you will lose all administrator privileges.

Command Syntax
utils reset_application_ui_administrator_password
Use this command to reset the password for the application user. The application user is configured during installation and is the initial Super User who can sign in to the Administration console.

utils restore_application_ui_administrator_account

This command restores the administrator account information in the application.

Command Syntax
utils restore_application_ui_administrator_account

utils service

utils service list

This command retrieves status for all services.

Command Syntax
utils service list [*page*]

OPTION [page] pauses after each page.

utils service restart

This command restarts a service.

Command Syntax
utils service restart *serv*

PARAMETER *serv* is the name of the service to restart.

utils service start

This command starts a service.

Command Syntax
utils service start *serv*

PARAMETER *serv* is the name of the service to start.

utils service stop

This command stops a service.

Command Syntax
utils service stop *serv*

PARAMETER *serv* is the name of the service to stop.

utils snmp

utils snmp get

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

Command Syntax
utils snmp get <*version*>

PARAMETERS:

version is 1 or 2c.

Enter the community string:<Community string>

Enter the ip address of the Server :<IP address of the server>

The Object ID (OID) <Object ID>

Enter parameter as "file" to log the output to a file. [nofile] < name of the text file>

Press Enter to display the results on screen without saving any text files.

utils snmp test

This snmp test sends sample alarms to local syslog, remote syslog and snmp trap.

Command Syntax
utils snmp test

utils snmp walk

This command is used to walk the SNMP MIB starting with the specified OID.

Command Syntax
utils snmp walk <*version*>

PARAMETERS:

version is 1 or 2c.

Enter the community string: <Community string>

Enter the ip address of the Server :<IP address of the server>

The Object ID (OID) :<Object ID>

Enter parameter as "file" to log the output to a file. [nofile]<name of the text file>

Press Enter to display the results on screen without saving any text files.

utils snmp configure

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**}

PARAMETERS:

add Adds a new community string.

delete Deletes a community string.

list Lists all community strings.

update Updates a community string.

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**}

PARAMETERS:

add Adds a notification destination.

delete Deletes a notification destination.

Lists Lists all notification destination.

Update Updates all notification destination.

utils snmp config 1/2c trap

This interactive command affects trap notifications.

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

PARAMETERS:

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

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.

utils snmp config 3 inform

This interactive command affects the v3 inform notification.

utils snmp config 3 inform {**add** | **delete** | **list** | **update**}

PARAMETERS:

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.

utils snmp config mib2

This interactive command affects the Mib2 configuration information.

utils snmp config mib2 {**add** | **delete** | **list** | **update**}

PARAMETERS:

add Adds the Mib2 configuration information.

delete Deletes the Mib2 configuration information.

list Lists the Mib2 configuration information.

update Updates the Mib2 configuration information.

utils snmp config 3 trap

This interactive command affects trap notifications.

utils snmp config 3 trap {**add** | **delete** | **list** | **update**}

PARAMETERS:

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.

utils snmp config 3 user

This interactive command affects v3 user configuration.

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

PARAMETERS:

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.

utils soap realtimeservice test

This soap test runs a number of test cases on the remote server as specified by a parameter of remote-ip, remote-https-user, or remote-https-password.

Command Syntax
utils soap realtimeservice test <*remote-ip*> <*remote-https-user*> <*remote-https-password*>

PARAMETERS: (At least one parameter is required.)

remote-ip = remote ip address of the machine under test

remote-https-user= remote http user who has role to access soap api

remote-https-password = remote http users password

utils system

These commands perform system operations.

utils system restart

This command restarts the server after presenting a confirmation (yes | no) message.

Command Syntax
utils system restart

utils system shutdown

This command shuts the server down after presenting a confirmation (yes | no) message.

Note It is important to shut down using this CLI command. Do not shut down by pressing the power button on the server.

Command Syntax
utils system shutdown

utils system switch-version

This command switches to the other installed version on the server after presenting a confirmation (yes | no) message. Note that if you switch back to an earlier version, any services or functionality available only in the later version are removed.

Command Syntax
utils system switch-version

utils system upgrade

This command allows you to upgrade the server.

Command Syntax
utils system upgrade <*cancel*> <*status*> <*initiate*>

PARAMETERS:

cancel cancels the active upgrade.

status gets the status of the upgrade.

initiate starts an upgrade. Specify the required inputs as the upgrade proceeds.

utils vmtools

utils vmtools refresh

This command refreshes the version of the currently installed VMware tools on the virtual machine to the same version as that of the ESXi host.

Command Syntax
utils vmtools refresh

```
The VMware Tools ISO is not mounted in the CD/DVD drive.

Please ensure that you have selected Guest -> Install/Upgrade VMware Tools
-> Interactive Tools Upgrade by right-clicking on the VM from your VI
client.
```

After you perform the above step, run the command again **utils vmtools refresh**

```
VMware Tools are out-of-date. Proceeding with tools upgrade.

*** 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.Continue (y/n)?
Y Starting VMware Tools upgrade ...

Uninstalling VMware Tools 8.6.0-425873..... Done

Restarting system to complete tools upgrade...

*** W A R N I N G ***

Restart could take up to 5 minutes... Stopping Service Manager
```

Show Commands

show account

This command lists all accounts except the primary admin account.

Command Syntax
show account

show accountlocking

This command shows the current account locking settings.

Command Syntax
show accountlocking

show cert

These commands show certificate information about the selected certificate type.

Command Syntax
show cert list *type*

PARAMETER *type* is mandatory and can be *own* or *trust*.

show cert own*name*

show cert trust*name*

PARAMETER *name* must be a valid certificate name.

show cli

Run this command to show if pagination of the current CLI session is on or off.

Command Syntax
show cli pagination

Run this command to show the CLI session timeout. The CLI session timeout is set to 30 minutes for new CLI sessions.

Command Syntax
show cli session timeout

show cuic-properties

These commands show information about Unified Intelligence Center properties.

Command Syntax
show cuic properties allow-external-links

This command shows the value *on* or *off*, depending on the current value set for the allow-external-links property.

Command Syntax
show cuic properties dashboard-customwidget-enabled
This command shows the value *on* or *off*, depending on the current value set for the dashboard-customwidget-enabled property. This value can be set using **set cuic properties dashboard-customwidget-enabled**.

Command Syntax
show cuic properties host-to-ip
This command shows the current host-to-ip translation for Unified Intelligence Center databases in the cluster.

Command Syntax
show cuic properties http-cache
This command shows the value *on* or *off*, depending on the current value that is set for the http-cache property.

Command Syntax
show cuic properties max-large-schedule
This command shows the number of large schedules set for the Unified Intelligence Center web application.

Command Syntax
show cuic properties purge-retention
This command shows the number of days that data in the Unified Intelligence Center database is retained before it gets purged.

Command Syntax
show cuic properties purge-time
This command shows the time of the day when the data in the Unified Intelligence Center database will be purged and the interval (in minutes) after which the purge operation should be rerun.

Command Syntax
show cuic properties session-timeout
This command shows the Session Timeout for the Unified Intelligence Center web application.

Command Syntax
show cuic properties user-audit-logging

This command shows the value *on* or *off*, depending on the current value that is set for the user-audit-logging property.

Command Syntax
show cuic properties report-query-timeout

This command shows the time limit, in seconds, that is set for a report query execution to timeout.

show cuic component-status

These commands show the status of the Unified Intelligence Center components.

Command Syntax
show cuic component-status subsystem [*options*]

PARAMETER *subsystem* is mandatory.

OPTIONS:

```
[CuicStatus] shows the status of cuic web engine and the DB replication.

[DBReplStatus] shows the status of database replication on this node.

[DBStatus] shows the database status.
```

[SchedulerStatus] shows status of the report scheduler.

The following subsystem options are not supported for Unified Intelligence Center 11.0(1):

[ICMUserStatus] shows the status of Unified ICM user integration.

[EmailStatus] shows status of the emailer component.

[DataSourceConnectionStatus] shows data source connection status.

show diskusage

These commands show disk usage of the given directory as well as the usage of the disk partition the directory exists on.

Command Syntax
show diskusage activelog [*options*]
show diskusage common [*options*]
show diskusage inactivelog [*options*]
show diskusage install [*options*]
show diskusage tftp [*options*]
show diskusage tmp [*options*]

OPTIONS:

[file fname] outputs the information to a file saved in platform/cli/fname.

[directory] show only directory sizes.

[sort] sorts output by sizes in 1024 byte blocks.

show environment

These commands retrieve the current reading of the various fan, power-supply, or temperature sensors.

Command Syntax
show environment fans
show environment power-supply
show environment temperatures

show hardware

This command retrieves some basic platform hardware information.

Command Syntax
show hardware

show ipsec

Use these commands to display ipsec policies.

Command Syntax
show ipsec information [**policy_group**] [**policy-name**]
Use to display detailed information about the specified ipsec policy.

Command Syntax
show ipsec policy_group
Use to display the list of ipsec policy names with specified policy group.

Command Syntax
show ipsec policy_name
Use to view a policy with a given policy name and group. Example:set ipsec policy_name group1 name1.

Command Syntax
show ipsec status
Use to display the status of all ipsec tunnels defined in the system.

show logins

This command shows the last number of platform admin logins. The default is to show 20 logins.

Command Syntax
show logins *last n*

OPTION:

[last n] specifies a number of logins to show. Entering the command with no option shows 20 logins. Specifying a value of 0 will display all previously saved logins.

show memory

These commands displays information about the server memory.

Command Syntax
show memory count
show memory module module number
show memory module ALL
show memory size

show myself

This command shows information about the current account: machine name, account name, admin privilege level, output setting and logging setting. Use the commands set commandcount and set logging to modify current account settings.

Command Syntax
show myself

show network

show network all

This command retrieves all basic platform network information.

Command Syntax
show network all [*options*]

OPTIONS:

[detail] displays more detail.

[page] pauses the output .

[search srchtxt] looks for srchtxt in the output. This is a case-insensitive search.

show network cluster

This command shows the nodes that are part of the network cluster.

Command Syntax
show network cluster

show network dhcp eth0 status

This command displays the DHCP status on eth0.

Command Syntax
show network dhcp eth0 status [*options*]

show network failover

This command shows network fault tolerance information.

Command Syntax
show network failover [*options*]

OPTIONS:

[detail] displays more detail.

[page] pauses the output.

show network ip_conntrack

This command retrieves the current utilization of ip_conntrack.

Command Syntax
show network ip_conntrack [*options*]

show network ipprefs

These commands display the network ports and their status.

Command Syntax
show network all
show network enabled
show network public

show network ipv6

This command shows the IPv6 network settings.

Command Syntax
show network ipv6 settings

Command Syntax
show network ipv6 route [*options*]

OPTIONS:

optional.

detail.

show network max_ip_conntrack

This command retrieves ip_conntrack_max information.

Command Syntax
show network all

show network ntp

This command displays security option configured on /etc/ntp.conf file.

Command Syntax
show network ntp option

show network route

This command retrieves some basic platform network route information.

Command Syntax
show network route [*options*]

OPTIONS:

[detail] displays more detail.

[search srchtxt] looks for srchtxt in the output. This is a case-insensitive search.

show network status

This command retrieves some basic platform network status information.

Command Syntax
show network status [*options*]

OPTIONS:

[detail] displays additional information.

[listen] displays only listening sockets.

[process] displays the process ID and name of the program to which each socket belongs.

[all] displays both listening and non-listening sockets.

[nodes] displays numerical addresses without any DNS information.

[search sext] searches for the "sext" in the output. This is a case-insensitive search.

show open

show open files

These commands show open files.

Command Syntax
show open files all
This command displays all the open files on the machine.

Command Syntax
show open files process *ProcessID1, ProcessID2*
This command displays all the open files on the machine belonging to given process(es).

PARAMETER *Processid* must be a valid process id. You can enter a comma-delimited list of processes.

Command Syntax
show open files regex *"regex"*
This command displays all the open files on the machine that match the regular expression.

PARAMETER *"regex"* is the regular expression to match and must be enclosed in quotation marks.

show open ports

These two commands show open ports.

Command Syntax
show open ports all
This command shows all open ports.

Command Syntax
show open ports regex *"string"*
This command shows all the open ports on the machine that match the regular expression. It takes the parameter *"string"*.

show packages

These commands retrieve the version number of one or more packages on the active or inactive side.

Command Syntax
show packages active *pkg* [*page*]
show packages inactive *pkg* [*page*]

PARAMETER *pkg* must be a valid package name.

OPTION:

[page] pauses the display.

show password

Use these commands to configure password rules.

Command Syntax
show password age *maximum* | *days* *minimum* | *days*
show password complexity *character* *minimum-length*
These commands display the status of the password complexity as enabled or disabled and the minimum length that the password must be.

Command Syntax
show password expiry *maximum-age* *minimum-age* *user*
These commands display the status of the password expiration; the maximum and minimum expiration parameters and the expiration parameter for a specific user.

Command Syntax
show password history *number*
This command displays the number of passwords that will be maintained in the history.

show perf

show perf counterhelp

This command lists the explaining text for a particular perfmon counter.

Command Syntax
show perf counterhelp <*class-name*> <*counter-name*>

PARAMETERS:

class-name is the perf class name that contains the perf counter.

counter-name is the perf counter name to view.

Note If either parameters contain white space, then both should be in quotation marks. For example, **show perf counterhelp** "Cisco Phones" "CallsAttempted".

show perf list

These four commands show various perfmon information.

Command Syntax
show perf list categories
This command lists all categories in the perfmon system.

Command Syntax
show perf list classes [*options*]
This command lists perfmon classes.

Command Syntax
show perf list counters *class-name* [*options*]
This command lists perfmon counters in a particular perfmon class.

Command Syntax
show perf list instances *class-name* [*options*]
This command lists perfmon instances of a particular perfmon class.

PARAMETER *class-name* is the name of the perfmon class.

OPTIONS:

[cat category] shows perfmon classes for a particular category.

[detail] shows detailed information.

show perf query

These four commands show various perfmon queries.

Command Syntax
show perf query class *class-name*

This command queries the perfmon class to show all instances and counter values of each instance.

Most Unified Intelligence Center counters display with this command. For example *show perf query class SchedulerInfo* shows the *SchedulerIntervalLength*, *SchedulerJobsCompletedCount*, *SchedulerJobsFailedCount*, *SchedulerJobsRunningCount*, and *SchedulerState*.

Command Syntax
show perf query counter *class-name* <*counter-name, counter-name...*>
This command queries a counter to show the counter value of all instances.

Command Syntax
show perf query instance <*class-name*> <*instance-name, instance-name...*>
This command queries an instance to show its all counter values.

Command Syntax
show perf query path *path-spec, path-spec*

class-name is the name of the perfmon class. Accepts a comma-delimited list of up to five class-names. If class-name contains white space, enclose it in double quotes.

counter-name is the counter name to view. You can query a maximum of five comma-delimited counter-names. If the name contains white space, enclose it in double quotes.

instance-name is the instance name to view. You can query a maximum of five comma-delimited instance-names. If the name contains white space, enclose it in double quotes.

path-spec is the perfmon query path to view. You can query a maximum of five, comma-delimited path-specs.

show process

These commands show process information.

show process list

This command is used to get the list of all the processes, and critical information about each one of them. This command also displays visually the child-parent relationship between these processes.

Command Syntax
show process list [*options*]

OPTIONS:

[file] - optional file-name for the output.

[detail] - optional detailed output.

show process load

This command shows the current load on the system including the number "num" of processes using the most cpu or memory or time.

Command Syntax
show process load [*options*]

OPTIONS:

[cont] - the command will repeat continuously.

[clear] - the screen will clear before displaying output.

[noidle] - the command will ignore the idle/zombie processes.

[num XX] - configure the number of processes to be displayed (using most cpu) XX is the number of processes: default is 10 processes; minimum value is 1; use 'all' for all processes.

[thread] - show threads.

[cpu]- sort output by CPU usage.

[memory] - sort output by memory.

[usage time] - sort output by time usage.

Note Only one of cpu, memory or time may be specified.

[page] - pause output.

show process name

This command is used get the details of processes that share the same name. This also displays parent-child relationship.

Command Syntax
show process name *process-name* [*file-filename*]

PARAMETER *process-name* must be a valid process name.

OPTION [file file-name] is the file-name for the output.

show process open-fd

This command is used to list the open file descriptors for a comma separated list of process Ids.

Command Syntax
show process open-fd *p1, p2, p3* [*file*]

PARAMETER *p1* is the process ID. You can enter a comma-separated string of process IDs.

OPTION [file] is the file-name for the output.

show process search

This command lets you search some particular patterns in the output of the operating system specific process listing.

Command Syntax
show process search *regexp* [*file*]

PARAMETER *regexp* specifies the regular expression.

OPTION [file] is the file-name for the output.

show process user

This command displays the user and more details on the process used, including the virtual memory used and others.

Command Syntax
show process user *user-name* [*options*]

user-name is mandatory.

OPTION :

[file] is the file-name for the output.

[vm] is the virtual memory of the process.

[detail] show process's page fault, virtual memory, start time and others.

[cont] to repeat the command continuously.

show process using-most

These commands show the processes using the most cpu or the most memory.

Command Syntax
show process using-most cpu [*options*]
show process using-most memory [*options*]

OPTIONS:

[file] - the file-name for the output.

[number] - The number of processes. The default is 5.

show registry

This command displays the contents of the registry.

Command Syntax
show registry <*system*> <*component name*> `page`

PARAMETERS:

system represents the registry system name.

component represents the registry component name.

OPTION: [page] displays one page at a time.

show smtp

This command shows the SMTP server.

Command Syntax
show smtp

show stats io

This command shows system input/output statistics of the machine.

Command Syntax
show stats io [*options*]

OPTIONS:

[kilo] display statistics in kilobytes.

[detail] displays detailed statistics of every available device on the system. This option overrides the [kilo] option.

[page] pauses the output.

[file fname] outputs to a file. The file is saved in platform/cli/fname.txt. The fname must not contain the " character.

show status

This command retrieves basic platform status.

Command Syntax
show status

show tech

show tech activesql

This command shows the active queries to the database taken in the last one minute.

Command Syntax
show tech activesql

show tech all

This command displays all of the different show tech xxx commands and may produce a large output of data.

Command Syntax
show tech all [*options*]

OPTIONS:

[page] displays one line at a time.

[file fname] outputs to a file saved in platform/cli/fname.txt.

show cuic tech

These commands display information about the Unified Intelligence Center database.

Command Syntax
show cuic tech procedures

This command shows the procedures in use for the Unified Intelligence Center database.

Command Syntax
show cuic tech systables

This command displays the name of all tables in the Unified Intelligence Center database.

Command Syntax
show cuic tech table <*tablename*>

This command shows the contents of a table on the Unified Intelligence Center database.

PARAMETER *tablename* is mandatory and must be the name of a table in the Unified Intelligence Center database.

Command Syntax
show cuic tech triggers

This command displays Unified Intelligence Center table names and the triggers associated with those tables.

show tech database

These commands show database information.

Command Syntax
show tech database dump [*options*]

This command dumps the database so that you can send it for debugging.

OPTIONS:

[ccm] - operating system database. This is the default. If you do not include the *cuic* option, this command shows the operating system database.

[cuic] - Unified Intelligence Center database.

Command Syntax
show tech database sessions

This command redirects the session and SQL information of present session IDs to a CSV file.

show tech dberrorcode

This command shows the explanation for a particular database errorcode.

Command Syntax
show tech dberrorcode *errorcode*

PARAMETER *errorcode* is mandatory. Enter the code for the error you are investigating.

show tech dbintegrity

This command checks database server specified disk structures for inconsistencies and displays output in a file.

Command Syntax
show tech dbintegrity

show tech dbinuse

This command displays the database in use.

Command Syntax
show tech dbinuse

show cuic tech dbschema

This command displays the database schema in a CSV file.

Command Syntax
show cuic tech dbschema [*options*]

OPTIONS:

[ccm] - operating system database. This is the default. If you do not include the *cuic* option, this command shows the operating system schema.

[cuic] - Unified Intelligence Center database.

show tech dbstateinfo

This command shows the database state information and outputs it to a file.

Command Syntax
show tech dbstateinfo

show tech dumpCSVandXML

This command collects csv and xml files into a single tar file.

Command Syntax
show tech dumpCSVandXML

show tech network

These commands shows network aspects of the system.

Command Syntax
show tech network all [*options*]
show tech network hosts [*options*]
show tech network interfaces [*options*]
show tech network resolv [*options*]
show tech network routes [*options*]
show tech network sockets [*options*]

OPTIONS:

[page] displays one line at a time.

[search txt] searches the output for txt *. Case insensitive search.

[file fname] outputs to a file saved in platform/cli/fname.txt.

[numeric] displays ports in numeric format.

show tech notify

This command displays the database change notify monitor.

Command Syntax
show tech notify [*search pattern*]

OPTION [search pattern] is a string that needs to be searched in the command output.

show tech params

These commands display the database parameters.

Command Syntax
show tech params all
Shows all parameters.

Command Syntax
show tech params enterprise
Shows enterprise parameters.

Command Syntax
show tech params service
Shows service parameters.

show cuic tech procedures

This command displays the stored procedures in use for the database.

Command Syntax
show cuic tech procedures [*options*]

OPTIONS:

[ccm] - operating system database. This is the default. If you do not include the *cuic* option, this command shows the procedures in use for the operating system database.

[cuic] - Unified Intelligence Center database.

show tech repltimeout

This command shows the replication timeout setting.

Command Syntax
show tech repltimeout

show tech sqlhistory

This command collects sqlhistory statements into a single file (*.out) and directs you to the location of that file.

Command Syntax
show tech sqlhistory

show cuic tech systables

This command displays the name of all tables in the database.

Command Syntax
show cuic tech systables [*options*]

OPTIONS:

[ccm] - operating system database. This is the default. If you do not include the *cuic* option, this command shows the tables in the operating system database.

[cuic] - Unified Intelligence Center database.

show tech system

These commands show various aspects of the system.

Command Syntax
show tech system all [*options*]
show tech system bus [*options*]
show tech system hardware [*options*]
show tech system host [*options*]
show tech system kernel
show tech system software
show tech system tools

OPTIONS:

[page] displays one line at a time.

[file fname] outputs to a file are saved in platform/cli/fname.txt.

show cuic tech table

This command redirects the contents of the specified database table into a file.

Command Syntax
show cuic tech table [*options*]

This command shows the contents of a table on the operating system database.

PARAMETER *tablename* must be the name of a table in the database.

OPTIONS:

[ccm] - operating system database. This is the default. If you do not include the *cuic* option, this command shows only tables in the operating system database.

[cuic] - Unified Intelligence Center database.

This example shows the cuicversion table from the cuic database: *show cuic tech table cuicversion cuic*.

show cuic tech triggers

This command displays table names and triggers associated with those tables.

Command Syntax
show cuic tech triggers [*options*]

OPTIONS:

[ccm] - operating system database. This is the default. If you do not include the *cuic* option, this command shows the table name and triggers associated with the operating system database.

[cuic] - Unified Intelligence Center database.

show tech version

This command displays the version of all RPMs (RedHat Package Manager) installed on the system.

Command Syntax
show tech version

show timezone

These commands display the currently-configured timezone or list of all zones.

Command Syntax
show timezone config
Shows the timezone currently set for the server.

Command Syntax
show timezone list
Displays a list of all timezones. See also *set timezone*.

Related Topics

set timezone, on page 158

show tls server cert_type

This command displays the configured certificate type used by the server for TLS connections.

Command syntax

show tls server cert_type

```
admin:show tls server cert_type
The server certificate type is set to ECDSA

Command successful
```

show ups status

This command communicates with an attached Uninterruptible Power Supply and displays status.

Command Syntax
show ups status

show version

This command displays the software version on the active or inactive side.

Command Syntax
show version [{*activeinactive*}]

The indicator to the **active** or **inactive** partition is required.

show web-security

This command displays web security information.

Command Syntax
show web-security

show workingdir

This command displays the current working directories for the activelog and inactivelog.

Command Syntax
show workingdir

Set Commands

set account

Command Syntax
set account *name*
This command sets up a new account and prompts for privilege level and password.

PARAMETER *name* specifies the name of the admin account.

Command Syntax
set account *enable*
Use this command to enable the user account if the account is disabled due to password inactivity.

set accountlocking

Use these commands to control the administrator accounts.

Command Syntax
set accountlocking {*enabledisableunlocktime*}

PARAMETER *enable* enables account locking.

PARAMETER *disable* disables account locking.

PARAMETER *unlocktime* used to configure the unlock time for admin accounts in seconds. Acceptable values are equal to or greater than 300 seconds but less than 3600 seconds (60 mins).

set cert

This command regenerates the certificate for the unit name. See also *show cert*.

Command Syntax
set cert bulk {*unitall*}
This command consolidates all the certificates available for this unit in the pre-configured sftp location and exports the consolidated file to the same sftp location.

Command Syntax
set cert import {*unitall*}
This command consolidates all the certificates available for this unit in the pre-configured sftp location and imports the consolidated file to the same sftp location.

Command Syntax
set cert regen *unit name*
This command regenerates the certificate for the unit name and prompts for a restart to activate the regenerated certificate.

PARAMETERS:

unit and *unit name* specifies the name of the unit.

Related Topics

show cert, on page 129

set cli

Run this command to set the pagination of the current CLI session.

Command Syntax
set cli pagination *name*

PARAMETER *on* or *off*

Run this command to set the CLI session timeout minutes. Minutes are mandatory. The number of minutes after which sessions are declared to be invalid; range is 5 to 99999.

Command Syntax
set cli session timeout minutes

set commandcount

These commands change the CLI command prompt, so it displays or hides the number of CLI commands run in the current session.

Command Syntax
set commandcount enable
set commandcount disable

set cuic properties

Use these commands to set values for the Unified Intelligence Center properties.

Command Syntax
set cuic properties *allow-external-links*

PARAMETER <*on*|*off*>

This command sets the allow-external-links property to *on* or *off*. By setting the value to *on* or *off*, you can enable or disable the external links in Unified Intelligence Center dashboard respectively. By default, the value is set to *off*.

Note After the upgrade, the external links in the Unified Intelligence Center dashboard will be disabled.

If enabled, the contents from external links are rendered within the HTML iFrame in the dashboard. This will include the `frame-src*` directive in the Content Security Policy of the Unified Intelligence Center web pages.

Command Syntax
set cuic properties *dashboard-customwidget-enabled*

PARAMETER <*on*|*off*>

This command sets the dashboard-customwidget-enabled property to *on* or *off*. By setting the value to *on* or *off*, you can enable or disable the Custom Widget feature in Dashboards respectively. By default, the value is set to *off*.

Note Enabling the custom widget configuration can lead to injection vulnerabilities.

Command Syntax
set cuic properties *host-to-ip*

PARAMETER <*host*> <*ip-address*>

This command sets the IP to be used for the data source host name that is specified while configuring the Unified Intelligence Center data source. This command allows for scalability and overrides the default Historical or Real-time database server that is defined in the **Data Sources** interface.

For <*host*>, enter the value for the host DNS name for the server, as displayed on the **Data Sources** interface.

Note The hostname is case-sensitive. Enter the hostname exactly as entered on the **Data Sources** interface.

For <*ip-address*>, enter the IP address of the server for the Historical or Real-time database.

Note You must restart the Unified Intelligence Center Reporting Services for the change to take effect.

Command Syntax
set cuic properties *max-large-schedule*

PARAMETER *# of large schedules*

This command sets the limit for maximum number of large schedules that you can create. The valid range is 1-6 large schedules. The default value is 1.

Note You must restart the Unified Intelligence Center Reporting Services for the change to take effect

Command Syntax
set cuic properties *purge-time*

PARAMETER 1<*HH:MM* > <*AM/PM*>

PARAMETER 2 <*Interval (in minutes)*>

This command sets the time of day when the Unified Intelligence Center database will be purged and the duration (in minutes) after which the purge operation should be rerun. The default purge time is 12:00 AM and the default purge interval is 60 minutes.

For <*HH:MM*> and <*AM/PM*> specify the time of the day when you want the purge job to run for the first time.

For <*Interval (in minutes)*>, specify the interval in minutes after which you want the purge job to rerun.

After you run this command with the correct parameters, the system displays a message as follows:

```
Next purge is scheduled to run after <x> hours <y> minutes.
Value has been successfully set.
```

Following are the various categories of data that the system purges when you use these CLI commands:

1. **Cached report data** - Data in this category is purged based on the time specified using the `set cuic properties purge-time` command. Note that the purge time is calculated based on the time when the filter used to run the report was last used or refreshed.
2. **Audit trail** - All audit trail data that is older than a month are purged during the last purge operation of the day.
3. **Cached scheduled report data** - The `set cuic properties purge-retention` CLI command applies only to this category.

Each rerun that the system performs using this command, results in the purging of the cached report data. Other categories are purged only during the last purge run of the day.

If you restart the Unified Intelligence Center server after the purge start time, the system discontinues the current purge cycle until the same purge start time on the next day.

For example, if you have set to run the purge job at 11.45 AM on a day with a rerun interval of 1 hour and the Unified Intelligence Center server was restarted at 2 PM, the following happens with respect to the purge runs and reruns:

- Purge job runs typically at 11.45 AM, 12.45 PM., and 1.45 PM.
- After the restart at 2 PM, the system checks for the purge start time and since the purge start time is set as 11.45 AM, the next purge run happens only at 11.45 AM on the next day.

To have continuous rerun even after the system restarts, you must set the purge start time and interval again using the `set cuic properties purge-time` CLI command.

Command Syntax
set cuic properties *purge-retention*

PARAMETER *#number of days*

This command sets the number of days that data in the Unified Intelligence Center database is retained before it gets purged. The default is one day and the maximum permissible value is 31 days.

Note Cached scheduled report data - The `set cuic properties purge-retention` CLI command applies only to this category.

Command Syntax
set cuic properties *session-timeout*

PARAMETER *#numberofSeconds*

This command sets the Session Timeout for the Unified Intelligence Center Reporting web application. The valid range is 1,800-14,400 seconds. The default is 14,400 seconds (4 hours).

Note You must restart the Unified Intelligence Center Reporting Services for the change to take effect.

Command Syntax
set cuic properties *http-cache*

PARAMETER <*on*|*off*>

This command sets the http-cache property to *on* or *off*. By setting the value to *on* or *off*, you can enable and disable the HTTP cache control. By default, the value is set to *on.*

Command Syntax
set cuic properties *user-audit-logging*

PARAMETER <*on*|*off*>

This command sets the user-audit-logging property to *on* or *off*. By setting the value to *on* or *off*, you can enable or disable the user audit logging. By default, the value is set to *off*.

Command Syntax
set cuic properties *report-query-timeout*

PARAMETER *number of seconds*

Range: 180-3600 seconds

This command sets the report query execution timeout value. The command is applicable when you run the report using the interface and does not apply to scheduled reports.

Example

```
set cuic properties report-query-timeout 250
WARNING : Do not change it to a higher value, as it may cause performance issue.

cuic.query.timeout has been updated
This command requires a restart of Intelligence Center service.
Ensure that this command is run on all nodes in the cluster.
```

set ipsec

Use these commands to enable ipsec policies.

Command Syntax
set ipsec policy_group {*groupall*}
Use to enable all policies within a group or all groups.

Command Syntax
set ipsec policy_name [*policy_group*] [*policy_name*]
Use to enable a policy with a given policy name and group. Example: `set ipsec policy_name group1 name1`

set logging

These commands allow you to enable or disable logging.

Command Syntax
set logging enable
set logging disable

set network

set network cluster publisher

Caution These commands are not supported for Unified Intelligence Center.

Command Syntax
set network cluster publisher hostname
This command configures the cluster publisher hostname and causes a temporary loss of network connectivity while the network is restarted with the new configuration.

Command Syntax
set network cluster publisher ip
This command configures the cluster publisher ip address and causes a temporary loss of network connectivity while the network is restarted with the new configuration.

set network dhcp eth0

These commands set the ethernet interface to disable dhcp (if enabled) or to use dhcp (if not already enabled). Entering this command prompts for verification and, if run, causes the system to restart.

Command Syntax
set network dhcp eth0 enable
set network dhcp eth0 disable

set network dns options

This command allows you to set the dns options.

Command Syntax
set network dns options [*options*]

OPTIONS:

[timeout xx] sets the DNS request timeout in seconds.

[attempts xx] sets the number of times to attempt a DNS request before quitting.

[rotate] causes the system to rotate among the configured DNS servers, distributing the load.

set network dns {primary | secondary}

These commands set the IP address for the primary or secondary DNS server. Entering this command prompts for verification and, if run, causes a loss of network connectivity.

Command Syntax
set network dns primary *addr*
set network dns secondary *addr*

PARAMETER *addr* specifies the address of the server.

set network domain

This command sets the domain name for the system. Entering this command prompts for verification and, if run, causes a loss of network connectivity.

Command Syntax
set network domain *name*

PARAMETER *name* specifies the name of the domain.

set network failover

These commands enable and disable Network Fault Tolerance on the Media Convergence Server network interface card. Entering the command prompts for verification and, if run, causes the system to restart.

Command Syntax
set network failover ena *op*
set network failover dis *op*

PARAMETER *op* indicates the operation.

set network gateway

This command enables you to configure the IP address of the network gateway. Entering this command prompts for verification and, if run, causes the system to restart.

Command Syntax
set network gateway *addr*

PARAMETER *addr* specifies the address of the gateway.

set network hostname

This command sets the network hostname and then causes a restart of the system The hostname must follow the rules for ARPANET host names. The hostname must start with an alphabet, end with an alphanumeric, and may contain any alphanumeric characters or hyphens in between. The hostname must be 63 characters or less.

Command Syntax
set network hostname [**name**] *addr*

PARAMETER *name* specifies the network hostname.

set network IP eth0

This command sets the IP address for Ethernet interface 0.

The system asks whether you want to continue to run this command. If you continue, this command causes the system to restart.

Command Syntax
set network ip eth0 <*ipaddr*> <*mask*> <*gateway*>

PARAMETERS:

ipaddr is the IP address.

mask is the mask.

gateway is the gateway.

set network ipv6

These commands are used for configuring the IPv6 feature on the machine.

Command Syntax
set network ip dhcp *action reboot*
This command is used for enabling or disabling the DHCPv6 client.

Command Syntax
set network ip service *action reboot reboot*
This command is used for enabling or disabling the IPv6 feature client.

Command Syntax
set network ipv6 static_address *addr mask*
This command is used for setting the static IPv6 address on the server.

PARAMETERS:

Action is mandatory can have either of these values: *{enable | disable}*

mask is the mask.

Reboot. Reboot after making these changes.

addr is the IP address.

mask is the mask.

set network max_ip_conntrack

This command sets the maximum value for ip_conntract_max.

Command Syntax
set network max_ip_conntrack *ip_conntrack_max*

PARAMETER *ip_conntrack_max* indicates the maximum value.

set network mtu

This command sets the maximum MTU value. The valid range is 500-1500.

Command Syntax
set network mtu *size*

PARAMETER *size* must be 1500 for all servers in the cluster.

set network nic eth0

This command sets the properties of the Ethernet Interface 0. It asks if you want to continue. If you continue, this command causes a temporary loss of network connections while the NIC is reset.

Command Syntax
set network nic eth0 *auto* [{*endis*}] *speed* [{*10100*}] *duplex* [{*halffull*}]

PARAMETERS: At least one is mandatory. Each parameter takes options indicated.

auto specifies whether auto negotiation gets enabled or disabled.

speed specifies the speed of the Ethernet connection: 10 or 100 Mbps.

duplex specifies half-duplex or full-duplex.

set network pmtud

This command enables or disables Path MTU Discovery.

The system asks whether you want to continue to run this command. If you continue, the system temporarily loses network connectivity.

Command Syntax
set network pmtud *state* {*enabledisable*}

PARAMETER *state {enable | disable}*

set network restore

This command restarts the networking on this host. If confirmed, this command causes a temporary loss of network connectivity.

Caution Only use this command when all other CLI 'set network ...' commands have failed to restore network connectivity to an Ethernet port. This command removes all previous Ethernet and Network Fault Tolerance settings. The specified Ethernet port is configured with a minimal static IP address configuration. It is imperative that the original Ethernet port settings be reconfigured AFTER this command using other CLI 'set network ...' commands.

Command Syntax
set network restore <*ethernet port*> <*ip-address*> <*network-mask*> <*gateway*>

PARAMETERS:

ethernet-port is the Ethernet port (for example, eth0).

ip-address is the IP address of the host.

network-mask is the network mask.

gateway is the Gateway IP address.

set network status eth0

This command sets the state of the ethernet interface eth0 to up or down.

Caution Only use this command when all other CLI 'set network ...' commands have failed to restore network connectivity to an Ethernet port. This command erases all previous Ethernet and Network Fault Tolerance settings. The specified Ethernet port is configured with a minimal static IP address configuration. It's imperative that the original Ethernet port settings be reconfigured AFTER this command using other CLI 'set network ...' commands.

Command Syntax
set network status eth0 *state* {*updown*}

PARAMETER *state {up | down}* to set the status up or down is required.

set password

Use these commands to configure password rules.

Command Syntax
set password age *maximum | days minimum | days*
set password complexity *character minimum-length*
set password system bootloader encryptHash
set password change-at-login *enable\disable*

Use this commands to enable or disable password complexity rules.

Command Syntax
set password expiry *maximum-age minimum-age*
set password history *number*
set password inactivity {*enabledisableperiod (days)*}

Use these commands to enable the operating system password inactivity to the default value of 10 days, to disable password inactivity, or set the number of days.

Command Syntax
set password user *admin security*

These commands allow you to change the system administrator and security passwords.

The system prompts you for the old and new passwords and checks the password for strength.

PARAMETERS:

character takes *{enable | disable}*

When enabled, passwords need to meet these guidelines:

- Have at least one lower-case character.
- Have at least one uppercase, one digit and one special character.
- Contain no characters that are adjacent on the keyboard.
- Have not been used as any of the previous ten passwords. The admin user password can be changed only once in 24 hours.
- Cannot have been changed in the past 24 hours.

minimum-length

When enabled, modify the value of minimum password length for Unified CM OS accounts. Acceptable values should be equal to or greater than 6. Use this command only after enabling the character complexity of passwords.

maximum days - Sets the value of the maximum age for the admin accounts in days. Acceptable values should be equal to or greater than 10 days but less than 3650 days (10 years).

minimum days - Sets the minimum password age for the admin accounts in days.

maximum-age - Takes *{enable | disable)* .

Enabling the maximum age sets the value of maximum password age to 3650 days (10 yrs) for CUCM OS admin accounts.

minimum-age - Takes *{enable | disable)*.

number - The number of passwords to maintain in history. Default is 10. Maximum is 20. Enter 0 to disable.

admin - Sets the admin password.

security - Sets the security password.

set smtp

This command sets the SMTP server hostname.

Command Syntax
set smtp *host*

PARAMETER *host* indicates the hostname for the smtp server.

set cuic syslog

This command sets the syslog as enabled or disabled.

Command Syntax
set cuic syslog {*enabledisable*}

set timezone

This command changes or sets the timezone. You must restart the system after you change the timezone.

Command Syntax
set timezone *zone*

PARAMETER *zone* indicates the timezone.

Enter the appropriate string or zone index id to uniquely identify the timezone.

To see a list of valid timezones, use the *show timezone* command.

Be aware that the timezone name is case-sensitive.

Related Topics

show timezone, on page 146

set tls server cert_type

Use this command to set the server certificate type to either RSA or ECDSA ciphers for TLS connections. The certificate set to the specified type is then presented for the cipher negotiations on all incoming TLS communications.

Command syntax

set tls server cert_type [option]

Option

ecdsa—Sets the certificate type to ECDSA.

rsa—Sets the certificate type to RSA.

Example

```
admin:set tls server cert_type rsa

Configuring the server to use RSA certificates for all inbound connections.

Do you want to continue (y/n) ? y
Yes entered
Configuring the server to use RSA ciphers for inbound connections.

Successfully configured the server to use RSA certificate for all inbound
connections.

******************************************************
A system reboot will occur for the changes to take effect.
It is highly recommended that you perform a system backup
after the system reboot.
```

```
Ensure all the nodes in the cluster are running on the same
certificate type by running the 'set' command
******************************************************

Broadcast message from root@uccxfirstnode (Mon Jul 5 10:31:04 2021):

The system is going down for reboot in 1 Minute

Broadcast message from root@uccxfirstnode (Mon 2021-07-05 10:31:05 IST):

The system is going down for reboot at Mon 2021-07-05 10:32:04 IST!
```

set tls min-version

This command allows you to set the minimum TLS version in the server or client that can be used for inbound or outbound SSL connections respectively. You must restart the system for the changes to take effect.

Note

- When you upgrade the TLS minimum version from TLSv1.0 to TLSv1.1 or TLSv1.2, reinstall the Cisco Unified Real-Time Monitoring Tool.
- In a multi-node CUIC deployment, run this CLI command on all the nodes of the cluster starting from the publisher. Restart all the nodes after executing the CLI command.

Command Syntax
set tls *[server | client]***min-version***<1.0|1.1|1.2>*

set web-security

This command sets the web security certificate information for the operating system.

Command Syntax
set web-security *<orgunit> <orgname> <locality> <state> < country>[hostname]*

PARAMETERS: (First five parameters are mandatory.)

orgunit is the organizational unit.

orgname is the organizational name.

locality is the location of the organization.

state is the state of the organization.

country is the country of the organization.

hostname is the alternate hostname. This parameter is optional.

For more information about setting the alternative host name, see https://supportforums.cisco.com/docs/DOC-6119.

set workingdir

These commands set the CLI working directory for activelog or inactivelog.

Command Syntax
set workingdir activelog *directory*
set workingdir inactivelog *directory*

PARAMETER *directory* must be a valid sub-directory of the activelog or inactivelog.

Run Commands

run loadxml

This command can be run on the publisher (the Controller node) as a workaround when service parameters or product specific information does not appear on the administration screen.

Running this command might necessitate a restart of some services.

Command Syntax
run loadxml

run cuic sql

This runs a SQL command to query and select from the database and table.

Command Syntax
run cuic sql *sql statement* [*options*]

PARAMETER *sql statement* specifies the SQL command to run. For example, select * from tablename.

OPTIONS:

[ccm] - operating system database. This is the default. If you do not include the *cuic* option, this command runs a sql statement from the system database.

[cuic] - Unified Intelligence Center database. For example, *select * from cuic:tablename*

You can run only one sql_statement at a time. But in the sql_statement you can use multiple tables. For example: *Select * from cuic:cuicreport, cuic_data:cuicreportdefinition*.

run loadcsv

This command runs on the publisher, to install product csv's on the server. It is necessary to run this command on the publisher only.

Running this command might necessitate a restart of some services.

Command Syntax
run loadcsv

file commands

Note File commands that include **activelog** list a **livedata** directory. For Packaged CCE deployments only, this directory contains logs for the Live Data reporting components.

file check

This command checks whether any files or directories have been added, removed, or changed in size since the last fresh installation or upgrade. The results display after the check.

Note This command is system-intensive. Run it at off-hours.

Command Syntax
file check [*detection-size-kb*]

OPTION: [detection-size-kb] specifies the minimum file size change that is required for the command to display the file as changed. The default is 100Kb.

file delete

These commands delete one or more specified files.

Command Syntax
file delete activelog *file-spec* [*options*]
file delete inactivelog *file-spec* [*options*]
file delete install *file-spec* [*options*]

PARAMETERS:

file-spec specifies the path and filename of the file(s) to delete.

OPTIONS:

[detail] displays a listing of deleted files with the date and time.

[noconfirm] deletes files without asking you to confirm each deletion.

Caution You cannot recover a deleted file, except possibly by using the Disaster Recovery System.

file dump

These commands dump the contents of the indicated files to the screen, one page at a time.

Command Syntax
file dump activelog *file-spec* [*options*]
file dump inactivelog *file-spec* [*options*]
file dump install *file-spec* [*options*]
file dump sftpdetails *file-spec* [*options*]

PARAMETER *file-spec* specifies the path and filename of the file(s) to dump.

OPTIONS:

[detail] displays listing with the date and time.

[hex] displays output in hexadecimal.

file get

These commands get (transfer) the specified file to another system by using SFTP. After the command identifies the specified files, you are prompted to enter an SFTP host, username, and password.

Command Syntax
file get activelog *file-spec* [*options*]
file get inactivelog *file-spec* [*options*]
file get install *file-spec* [*options*]
file get partBsalog *file-spec* [*options*]
file get salog *file-spec* [*options*]

PARAMETER *file-spec* specifies the path and filename of the file(s) to transfer.

OPTIONS:

[abstime] is absolute time period, specified as hh:mm:MM/DD/YY.

[reltime] is relative time period, specified as minutes | hours | days | weeks | months value.

[match] matches a particular string in the filename, specified as string value.

[recurs] gets all files, including subdirectories.

file list

These commands list the log files in an available log directory.

Command Syntax
file list activelog *file-spec* [*options*]
file list inactivelog *file-spec* [*options*]
file list install *file-spec* [*options*]
file list partBsalog *file-spec* [*options*]
file list salog *file-spec* [*options*]

PARAMETER *file-spec* specifies the path to the directory to list.

OPTIONS:

[page] displays the output one screen at a time.

[reverse] reverses sort direction.

[detail] displays a long listing with date and time.

[date] sorts by date.

[size] sorts by file size.

file search

These commands search the content of a log and display the matching lines one page at a time.

Command Syntax
file search activelog *file-spec* [*options*]
file search inactivelog *file-spec* [*options*]
file search install *file-spec* [*options*]

PARAMETERS:

file-spec represents the path to the file(s) to search.

reg-exp represents a regular expression.

OPTIONS:

[reltime] only search files that were modified within relative time.

[abstime] only search files that were modified within specific time range.

[ignorecase] ignores case distinctions.

[recurs] searches for the pattern recursively through subdirectories.

file tail

These commands tail (print the last few lines) of a log file.

Command Syntax
file tail activelog *file-spec* [*options*]
file tail inactivelog *file-spec* [*options*]
file tail install *file-spec* [*options*]

PARAMETER *file-spec* specifies the path to the file to tail.

OPTIONS:

[detail] displays a long listing with date and time.

[hex] displays hexadecimal listing.

[lines] specifies number of lines to display.

file view

These commands display the contents of the logging files specified.

Command Syntax
file view activelog *file-spec*
file view inactivelog *file-spec*

file view install *file-spec*
file view system-management-log

PARAMETER *file-spec* specifies the path to the file to view.

Delete Commands

delete account

This command allows you to delete an administrator account.

Command Syntax
delete account *name*

PARAMETER *name* specifies the name of the admin account.

delete dns

This command deletes the specified DNS server from the system and results in loss of network connectivity.

Command Syntax
delete dns *addr*

PARAMETER *addr* specifies the IP address name of the domain name server.

delete ipsec

These commands allow you to delete IPSec policies. You can delete a pokcy with a given policy name and group.

Command Syntax
delete ipsec policy_group [{*groupall*}]
Use to delete all policies within a group or to delete all groups.

Command Syntax
delete ipsec policy_name [*policy_group*] [*policy_name*]
Use to delete a policy with a given policy name and group. Example: `delete ipsec policy_name group1 name1`

PARAMETERS:

policy_group

policy_name

delete process

This command allows you to delete a particular process.

Command Syntax
delete process *pid* [{**options**}]

PARAMETER *pid* specifies the process ID number.

OPTIONS:

[force] stops the process.

[terminate] terminates the process.

[crash] crashes the process with a crash dump.

delete smtp

This command deletes the SMTP host.

Command Syntax
delete smtp

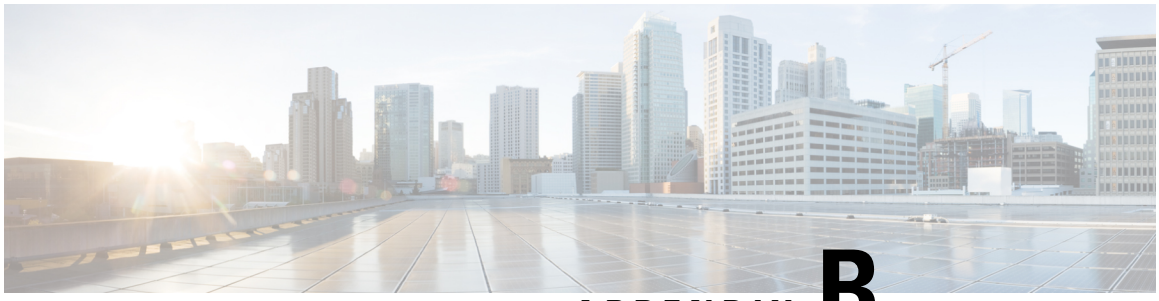
Use CLI

Note If you choose to configure Unified Intelligence Center with Live Data using CLI commands, refer chapter 4 on *Live Data Installation* in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Certain CLI commands are useful for specific inquiries.

- utils system restart
- utils system shutdown
- utils system switch-version
- utils system upgrade
- set network (dns / dhcp / hostname / mtu / cluster)
- show status
- utils disaster_recovery backup
- utils raid disk maintenance
- show diskusage
- show hardware
- show memory
- show ups status
- show environment
- utils create report

- show tech system
- show status
- show process using-most
- show stats io
- utils iostat
- show perf
- utils service start
- show process list
- show open files
- show open ports
- show timezone
- utils core
- utils create report
- show version
- set network
- utils network ping
- utils firewall
- show tech network
- set account
- show logins
- show web-security
- show cert
- utils auditd
- utils firewall
- show packages
- show cuic-properties
- set cuic properties
- show perf
- run cuic sql
- show tech
- utils dbreplication



APPENDIX B

Load Balance

• Load Balance , on page 167

Load Balance

In cases where a Unified Intelligence Center multi-node deployment experiences a heavy reporting workload, system administrators have the option to deploy server load balancing (SLB).

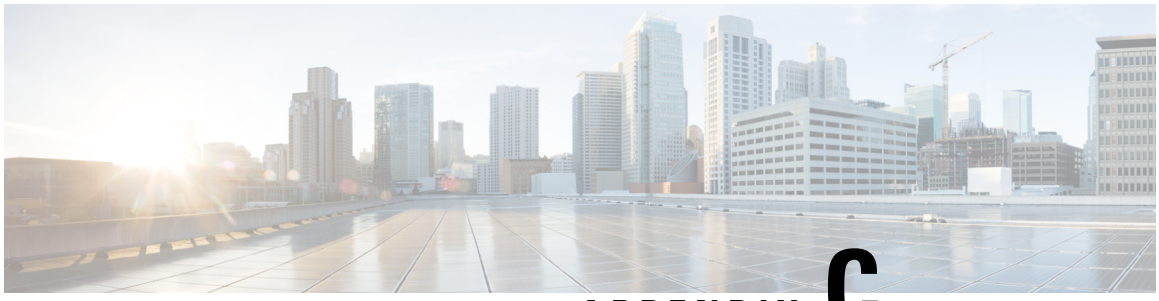
Note SSO access to the Unified Contact Center Enterprise web applications through the load balancer is not qualified.

SLB is a technique to distribute client requests among the nodes in a cluster or to select the server that can successfully fulfill a client request in the shortest time without overloading that server or the cluster as a whole.

Note In a Unified Intelligence Center deployment with SLB, if one of Unified Intelligence Center is down, the report viewer pointing to that server displays this error **Report execution Failed. Please check browser console logs for more info**. When you refresh your browser, a new Unified Intelligence Center log in page will display.

Note Load balancing for Live Data reports in Unified Intelligence Center is not supported in any deployments.

Load Balance



APPENDIX C

Unrestricted Resource Access

• Unrestricted Resource Access, on page 169

Unrestricted Resource Access

Cisco Unified Intelligence Center allows unrestricted access to the following resources and API endpoints:

Table 14: Resources with Unrestricted Access

Resource	Path
JavaScript Files	/cuicui/scripts/*", "/cuicui/js/*", "/gadgets/report/js/*
Style sheets	/cuicui/css/*", "/cuicui/gadgets/report/css/*
Images	/cuicui/images/*
API endpoints to get the information regarding locales supported by Cisco Unified Intelligence Center	/cuicui/api/i18n/* /cuicui/api/locales/ /cuic/rest/locales/*
API endpoints to check if Cisco Unified Intelligence Center server is online	/cuicui/api/status/* /cuic/rest/status/*
CORS pre-flight request for all REST API endpoints	/cuic/*"[OPTIONS (http method)]"
API endpoint to retrieve the list of sessions that are active in Cisco Unified Intelligence Center	/cuic/rest/usersessiondetail/*
API endpoint to retrieve the list of drf schedules	/cuic/rest/genericservices/drf/*

Unrestricted Resource Access