# Table of Contents

Preface .................................................................................................................. 1
Purpose .................................................................................................................... 1
Audience ............................................................................................................... 1
Organization ......................................................................................................... 1
Related Documentation ....................................................................................... 2
Conventions ......................................................................................................... 2
Obtaining Documentation and Submitting a Service Request............................. 3
Documentation Feedback .................................................................................... 4

1. The Administration Console.............................................................................. 5
   About the Administration Console.................................................................... 5
   Who can Sign In to Unified IC Administration?.............................................. 6
   The Welcome Page........................................................................................... 6
   About the Unified IC Cluster.......................................................................... 7
      Nodes in the Unified IC Cluster.................................................................. 7

2. Admin User Management Drawer .................................................................. 9
   Admin Users.................................................................................................... 9
      Multiple Super Users and Security............................................................. 10
   Configure User............................................................................................... 11

3. Device Management Drawer.......................................................................... 15
   Device Configuration....................................................................................... 15
      Defining the Member Node in the Administration Console...................... 17
   Device Configuration Detail......................................................................... 18
   Log and Trace Settings.................................................................................. 19
      About Logging and Tracing....................................................................... 19
   Edit Serviceability Settings......................................................................... 20
   Infrastructure Trace Definitions.................................................................... 22
  Subsystem Trace Definitions - OAMPServer................................................. 23
   Subsystem Trace Definitions - CUICServer.................................................. 24

4. Control Center Drawer.................................................................................... 27

5. Cluster Configuration Drawer.......................................................................... 29
   Reporting Configuration.................................................................................. 29
      Active Directory Tab.................................................................................. 29
      Report Scheduler Email Settings Tab......................................................... 31
   Unified CCE User Integration Configuration................................................. 32
      About Unified CCE User Integration.......................................................... 33
   License File Management.............................................................................. 34

6. Network Management Drawer....................................................................... 37
   SNMP (Simple Network Management Protocol)............................................ 37
   Unified IC SNMP MIBs.................................................................................. 38
      MIB Objects............................................................................................... 38
      MIB Notifications (CUIC TRAPs)............................................................... 43

7. Tools Drawer.................................................................................................. 47
   RTMT.............................................................................................................. 47
      Download and Launch RTMT..................................................................... 48
      RTMT Integration with Unified IC............................................................. 49
# Appendix A. Command Line Interface

- **Using CLI** .............................................. 94
- **Delete Commands** .................................. 96
- delete account ....................................... 96
- delete dns .............................................. 97
- delete ipsec ............................................. 97
- delete process ......................................... 97
- delete smtp ............................................. 97
- **File Commands** .................................... 98
- file check .............................................. 98
- file delete ............................................ 98
- file dump .............................................. 99
- file get .................................................. 99
- file list .................................................. 100
- file search .......................................... 100
- file tail .................................................. 101
- file view ............................................... 101
- **Run Commands** .................................. 102
- run loadxml .......................................... 102
- run sql .................................................. 102
- **Set Commands** .................................... 102
- set account .......................................... 103
- set accountlocking ................................. 103
- set cert ................................................. 104
set cli................................................................. 104
set commandcount................................. 104
set cuic-properties............................... 105
set ipsec.................................................. 105
set logging............................................ 106
set network............................................ 106
set password...................................... 110
set smtp.................................................. 112
set syslog.............................................. 112
set timezone........................................ 112
set trace............................................ 112
set web-security................................. 114
set workingdir....................................... 114
Show Commands................................. 114
  show account....................................... 115
  show accountlocking............................ 116
  show cert........................................... 116
  show cli.......................................... 116
  show cuic-properties......................... 116
  show cuis-component-status.................. 117
  show cuis-license-info......................... 117
  show diskusage................................... 118
  show environment............................... 118
  show hardware................................... 118
  show ipsec......................................... 119
  show logins...................................... 119
  show memory..................................... 119
  show myself.................................... 119
  show network.................................... 120
  show open........................................ 121
  show packages.................................. 122
  show password................................... 123
  show perf......................................... 123
  show process.................................... 125
  show registry.................................... 127
  show smtp......................................... 127
  show stats io.................................... 127
  show status...................................... 127
  show subsys...................................... 128
  show tech......................................... 128
  show timezone................................. 133
  show trace...................................... 133
  show ups status............................... 134
  show version.................................... 134
  show web-security.............................. 134
  show workingdir................................. 134
Unset Command................................. 134
  unset cuic-properties.......................... 135
  unset ipsec.................................... 135
  unset network dns............................. 135
  unset_host-to-ip................................ 135
<table>
<thead>
<tr>
<th>Commands</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>utils auditd</td>
<td>136</td>
</tr>
<tr>
<td>utils core</td>
<td>136</td>
</tr>
<tr>
<td>utils create report</td>
<td>137</td>
</tr>
<tr>
<td>utils csa</td>
<td>137</td>
</tr>
<tr>
<td>utils dbreplication</td>
<td>138</td>
</tr>
<tr>
<td>utils diagnose</td>
<td>140</td>
</tr>
<tr>
<td>utils disaster_recovery</td>
<td>140</td>
</tr>
<tr>
<td>utils firewall</td>
<td>142</td>
</tr>
<tr>
<td>utils iostat</td>
<td>143</td>
</tr>
<tr>
<td>utils iothrottle</td>
<td>143</td>
</tr>
<tr>
<td>utils netdump</td>
<td>143</td>
</tr>
<tr>
<td>utils network</td>
<td>144</td>
</tr>
<tr>
<td>utils ntp</td>
<td>146</td>
</tr>
<tr>
<td>utils purge</td>
<td>146</td>
</tr>
<tr>
<td>utils raid</td>
<td>147</td>
</tr>
<tr>
<td>utils remote_account</td>
<td>147</td>
</tr>
<tr>
<td>utils reset</td>
<td>147</td>
</tr>
<tr>
<td>utils service</td>
<td>148</td>
</tr>
<tr>
<td>utils snmp</td>
<td>149</td>
</tr>
<tr>
<td>utils soap realtime service test</td>
<td>150</td>
</tr>
<tr>
<td>utils system</td>
<td>150</td>
</tr>
</tbody>
</table>

**Appendix B. Load Balancing** .......................................................... 153

Example of ACE Load Balancing Configuration ........................................ 153

**Index** ................................................................................................. 157
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure User</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>Device Configuration</td>
<td>17</td>
</tr>
<tr>
<td>3</td>
<td>Member Configured</td>
<td>18</td>
</tr>
<tr>
<td>4</td>
<td>Log and Trace Settings</td>
<td>19</td>
</tr>
<tr>
<td>5</td>
<td>Edit Serviceability Settings</td>
<td>20</td>
</tr>
<tr>
<td>6</td>
<td>SubSystem Settings</td>
<td>21</td>
</tr>
<tr>
<td>7</td>
<td>Select Detailed to edit Trace Definitions</td>
<td>22</td>
</tr>
<tr>
<td>8</td>
<td>RTMT Desktop Icon</td>
<td>48</td>
</tr>
<tr>
<td>9</td>
<td>RTMTTraceLog</td>
<td>49</td>
</tr>
<tr>
<td>10</td>
<td>RTMT Critical Services</td>
<td>50</td>
</tr>
<tr>
<td>11</td>
<td>RTMT Alerts</td>
<td>50</td>
</tr>
<tr>
<td>12</td>
<td>RTMT Performance Interface</td>
<td>51</td>
</tr>
<tr>
<td>13</td>
<td>Report Execution</td>
<td>54</td>
</tr>
<tr>
<td>14</td>
<td>RTMT Counter Help</td>
<td>55</td>
</tr>
<tr>
<td>15</td>
<td>Navigation dropdown</td>
<td>79</td>
</tr>
<tr>
<td>16</td>
<td>Database Replication</td>
<td>83</td>
</tr>
<tr>
<td>17</td>
<td>Drawers in the Administration Console</td>
<td>87</td>
</tr>
<tr>
<td>18</td>
<td>Online Help Navigation Icon</td>
<td>88</td>
</tr>
<tr>
<td>19</td>
<td>Online Help</td>
<td>88</td>
</tr>
<tr>
<td>20</td>
<td>Using ACE</td>
<td>154</td>
</tr>
</tbody>
</table>
Preface

Purpose

This document explains the Cisco Unified Intelligence Center Administration console.

The Administration console, available on 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 IC. The other is the Unified IC Reporting application.

Audience

This guide is prepared for "Super Users (page 91)" who sign in to the Administration interface to administer, provision, monitor, and troubleshoot Cisco Unified Intelligence Center.

Organization

In addition to this Preface, this guide is organized as follows:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1 (page 5)</td>
<td>Explains the Administration console and the Unified IC cluster.</td>
</tr>
<tr>
<td>Chapters 2 through 7</td>
<td>Explain the six drawers on the left panel of the Administration Console page:</td>
</tr>
<tr>
<td></td>
<td>• Admin User Management (page 9)</td>
</tr>
</tbody>
</table>
### Chapter 1: Device Management
- Device Management (page 15)
- Control Center (page 27)
- Cluster Configuration (page 32) (Reporting, Unified CCE User Integration, and License File Management)
- Network Management (page 37) (SNMP and MIBs)
- Tools (page 47) (RTMT)

### Chapter 8 (page 79)
Explains the Cisco System Applications you can open from the Navigation menu:
- Cisco Unified Serviceability (page 80)
- Cisco Unified OS Administration (page 81)
- Disaster Recovery System (page 81)

### Chapter 9 (page 87)
Explains the Administration Console interface.

### Appendix A (page 93)
Documents the Command Line Interface.

**Note**: You cannot access the CLI directly from the Administration interface.

### Appendix B (page 153)
Includes a configuration example for Load Balancing

---

**Related Documentation**

- **Troubleshooting tips for the Cisco Unified Intelligence Center** (http://docwiki.cisco.com/wiki/Troubleshooting_Unified_Intelligence_Suite)
- **The Developers' Forum for the Cisco Unified Intelligence Center** (http://developer.cisco.com/web/ccr)

---

**Conventions**

This manual uses the following conventions:
<table>
<thead>
<tr>
<th><strong>Convention</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>boldface font</td>
<td>Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example:</td>
</tr>
<tr>
<td></td>
<td>• Choose <strong>Edit &gt; Find</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Finish</strong>.</td>
</tr>
<tr>
<td>italic font</td>
<td>Italic font is used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• To introduce a new term. Example: A <em>skill group</em> is a collection of agents who share similar skills.</td>
</tr>
<tr>
<td></td>
<td>• For emphasis. Example: <strong>Do not</strong> use the numerical naming convention.</td>
</tr>
<tr>
<td></td>
<td>• A syntax value that the user must replace. Example: IF <em>(condition, true-value, false-value)</em></td>
</tr>
<tr>
<td></td>
<td>• A book title. Example: See the <em>Cisco CRS Installation Guide</em>.</td>
</tr>
<tr>
<td>window font</td>
<td>Window font, such as Courier, is used for the following:</td>
</tr>
<tr>
<td></td>
<td>• Text as it appears in code or that the window displays. Example: <code>&lt;html&gt;&lt;title&gt;Cisco Systems, Inc. &lt;/title&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Angle brackets are used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• For arguments where the context does not allow italic, such as ASCII output.</td>
</tr>
<tr>
<td></td>
<td>• A character string that the user enters but that does not appear on the window such as a password.</td>
</tr>
</tbody>
</table>

**Obtaining Documentation and Submitting a Service Request**

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
Documentation Feedback

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

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.
Chapter 1

The Administration Console

This chapter contains the following topics:

• About the Administration Console, page 5
• Who can Sign In to Unified IC Administration?, page 6
• The Welcome Page, page 6
• About the Unified IC Cluster, page 7

About the Administration Console

Unified IC 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 IC Reporting web applications. As cluster can consist of the Controller node only.

Member nodes are optional and have the Unified IC Reporting application only. (Unified IC 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 (page 80) and SNMP (page 37)
• Cisco Unified OS Administration (page 81)
• Disaster Recovery System (page 81)
• Real Time Monitoring Tool (RTMT) (page 47)
Who can Sign In to Unified IC Administration?

The System Application User (page 91) 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 9) page.

To access the Administration console:

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

2. Sign in, using your Super User (system application user) ID and password.

   A successful sign in launches the Welcome Page (page 6).

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

See also: Users in the Administration Console (page 91).

The Welcome Page

The Welcome page appears by default after a successful sign in.

The left panel of the Welcome page contains drawers (page 87).

Drawers are similar to menus in that they group logically-related functional elements. Clicking a drawer in the left panel opens a panel on the right where you can define or display parameters for a function.

Table 1: Actions from this page

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the values for a function.</td>
<td>Click a drawer in the left panel.</td>
</tr>
<tr>
<td>Open the cisco.com website.</td>
<td>Click the Cisco logo at the top left.</td>
</tr>
<tr>
<td>Select from the Navigation dropdown at the top right.</td>
<td>Options are:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Serviceability (page 80)</td>
</tr>
<tr>
<td></td>
<td>Use to view and configure operating system serviceability parameters (such as Alarm, Trace, and SNMP).</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified OS Administration (page 81)</td>
</tr>
</tbody>
</table>
To | Do this
---|---
Use to configure and manage operating system parameters (such as IP settings and remote support accounts).
- Disaster Recovery System (page 81)
Use to manage backup and restore procedures.

Open the Unified IC reporting interface on a member node.
There are two ways to do this:
- Click Control Center > Device Control to open the Control Center page. Click the name of a member node to display the sign in page for that node.
- Open a new browser window and enter this URL: `http://<HOST ADDRESS>/cuic` 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:

Log out.
Click Log Out in the menubar.

Return to this Welcome page once you have navigated off of it.
Click the About link in the menubar.

About the Unified IC Cluster

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

Nodes in the Unified IC Cluster

The first node in the Unified IC 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 CUIC 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 CUIC databases are replicated synchronously among the Controller/publisher and all Member/subscribers by means of an "update anywhere" model. See Database Replication (page 83).
Database maintenance is performed by the Disaster Recovery System (page 81).
Admin User Management Drawer

Select Admin User Management drawer > Admin User Management to access the Admin 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 IC Reporting.

This chapter contains the following topics:

- Admin Users, page 9
- Configure User, page 11

Admin Users

The Admin Users page is a list of the names and roles 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 IC. See Users in the Administration Console (page 91).

To navigate to this page, click the Admin User Management drawer > Admin User Management.

The rows on the Users page contain two columns. There is a checkbox to the left of each row for selecting that user. Click the checkbox in the heading row to select all users. Use the Filter (page 88) feature narrow the list of names.
Table 2: Rows on this page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The User ID used to log in to the operations console.</td>
</tr>
<tr>
<td>Role</td>
<td>The role is Super User for all user names.</td>
</tr>
</tbody>
</table>

Table 3: Actions from this page

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a new Super User</td>
<td>Click Add New to open a blank Configure User (page 11) page.</td>
</tr>
<tr>
<td></td>
<td>You can add as many Super Users as you need.</td>
</tr>
<tr>
<td>Delete a Super User</td>
<td>Check the box next to the User Name and click Delete.</td>
</tr>
<tr>
<td></td>
<td>You cannot delete:</td>
</tr>
<tr>
<td></td>
<td>• the Super User defined in the installation.</td>
</tr>
<tr>
<td></td>
<td>• the Super User who is currently signed in.</td>
</tr>
<tr>
<td>Edit an existing Super User</td>
<td>The User Name is a link. Click the User Name to open that user’s Configure User (page 11) page.</td>
</tr>
<tr>
<td>Search for a Super User</td>
<td>Enter values in the filter fields.</td>
</tr>
<tr>
<td>Select a User Name</td>
<td>Check the checkbox in the left column of the row for that user.</td>
</tr>
<tr>
<td>Select all Users Names</td>
<td>Check the checkbox in the top (header) row of the list.</td>
</tr>
</tbody>
</table>

See also: Troubleshooting Admin User Management (http://docwiki.cisco.com/wiki/Troubleshooting_Tips_for_Unified_IC_8.0)

Multiple Super Users and Security

In this release, 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 IC Reporting\(^1\), 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.

As a best practice, the initial Super User might limit the number of additional Super Users and advise them to exercise caution in deleting or changing the credentials of other Super Users.

---

\(^1\) Additional Super Users have log in permission only for Unified IC Reporting.
Configure User

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

To navigate to this page, click Admin User Management drawer > Admin User Management to open the Users page. Then click Add New to add and configure a new user or click an existing User Name to edit the configuration for that user.

This page has three tabs - General, Credentials, and Policy.

**Figure 1: Configure User**

![Configuration User Page](image)

If a field is grayed-out, then that field it not editable. An asterisk indicates that the field is required.

Actions on this page are Save and Cancel.

**Table 4: General Tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The user Id for the user.</td>
</tr>
<tr>
<td>Password</td>
<td>Password. To require a secure password, enable Check for Trivial Passwords on the Policy tab.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The same password as above to confirm spelling.</td>
</tr>
<tr>
<td>Role</td>
<td>The only role is Super User.</td>
</tr>
</tbody>
</table>

The values on the General tab apply to the specific Super User being added or edited.
### Table 5: Credentials Tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locked by Administrator</td>
<td>If checked, this Super User is locked out.</td>
</tr>
<tr>
<td>User Cannot Change/Must Change</td>
<td>This pertains to the user password. Select either <strong>User Cannot Change</strong> or <strong>User Must Change at Next Login</strong>. You cannot select both.</td>
</tr>
<tr>
<td>Does Not Expire</td>
<td>This pertains to the user password. If the Credentials Expire After (days) field on the Policy tab is checked, then this field is disabled. If the Credentials Expire After (days) field on the Policy tab is clear, check Does Not Expire to enable a persistent password for the Super User.</td>
</tr>
<tr>
<td>Note:</td>
<td>DO NOT check the <strong>Does Not Expire</strong> box if you have checked <strong>User Must Change at Next Login</strong>, as the user will not be prompted to change the password at the next login.</td>
</tr>
<tr>
<td>Reset Hack Count</td>
<td>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.</td>
</tr>
<tr>
<td>Note:</td>
<td>If the user is locked out of the account due to failed logins exceeding the number set for Failed Login (on the policy tab), then you can unlock the account by checking this box and clicking Save.</td>
</tr>
<tr>
<td>Failed Login Attempts</td>
<td>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 login attempts time has expired.</td>
</tr>
<tr>
<td>Time Last Changed</td>
<td>Displays the last time this user's credentials were changed.</td>
</tr>
<tr>
<td>Time of Last Failed Login Attempt</td>
<td>Displays the date and time of the last login attempt by the user.</td>
</tr>
<tr>
<td>Time Locked by Administrator</td>
<td>Displays the date and time that this user account was locked.</td>
</tr>
<tr>
<td>Time Locked Due to Failed Logon Attempts</td>
<td>Displays the date and time that the system last locked this user account due to failed logon attempts.</td>
</tr>
</tbody>
</table>

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

**Note:** The credentials for Administration Super Users are encrypted into the local database. Super Users are not authenticated through Active Directory.
### Table 6: Policy Tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Logon</td>
<td>Specify the number of allowed failed logon attempts. When this threshold is reached, the system locks the account. Allowed range is 0 to 10.</td>
</tr>
<tr>
<td></td>
<td>To allow unlimited logon attempts, enter a value of 0 or check the <strong>No Limit for Failed Logons</strong> box.</td>
</tr>
<tr>
<td>Reset Failed Logon Attemps every (minutes)</td>
<td>Specify the number of minutes before the counter is reset for failed logon attempts. After the counter resets, the user can try logging in again. Allowed range is 0 to 120; default is 30.</td>
</tr>
<tr>
<td>Locked Duration (minutes)</td>
<td>Specify the number of minutes an account remains locked when the number of failed logon attempts exceeds the specified threshold. Allowed range is 0 to 120; default is 30. Checking the <strong>Administrator Must Unlock</strong> check box means that the account must be unlocked manually.</td>
</tr>
<tr>
<td>Minimum Duration Between Credential Changes (minutes)</td>
<td>Specify the number of minutes that are required before a user can change credentials again. Allowed range is 0 to 120; default is 0.</td>
</tr>
<tr>
<td>Credentials Expire After (days)</td>
<td>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 login. Optionally you can check <strong>Never Expires</strong> to have the credentials never expire.</td>
</tr>
<tr>
<td>Minimum Credential Length</td>
<td>Minimum number of characters for the password.</td>
</tr>
<tr>
<td>Stored Number of Previous Credentials</td>
<td>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.</td>
</tr>
<tr>
<td>Inactive Days Allowed</td>
<td>Specify the number of days that a password can remain inactive before the account gets locked. Allowed range is 0 to 5000; default is 0.</td>
</tr>
<tr>
<td>Expiry Warning Days</td>
<td>Specify the number of days before a user password expires to start warning notifications. Allowed range is 0 to 90; default is 0.</td>
</tr>
<tr>
<td>Check for Trivial Passwords</td>
<td>Check this check box to require the system to disallow credentials that are easily hacked, such as common words, repeated character patterns, and so on.</td>
</tr>
</tbody>
</table>

The values on the Policy tab apply to all Super Users.
Device Management Drawer

Open the Device Management drawer to view and maintain the devices in the cluster and to view log and trace settings for those devices.

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

See also: Troubleshooting Device Management (http://docwiki.cisco.com/wiki/Troubleshooting_Tips_for_Unified_IC_8.0)

This chapter contains the following topics:

- Device Configuration, page 15
- Log and Trace Settings, page 19

Device Configuration

This pages lists all currently-configured devices (nodes) in the cluster that contain the Unified IC reporting process.

A cluster can contain a maximum of eight such devices: one Controller (which runs both Administration and Unified IC reporting) and seven Members (which run Unified IC).

Note:

- The license type determines the number of devices (nodes) that you can install and configure. See License Types (page 90).
- You cannot add a member node until you have uploaded the license.

To navigate to this page, click Device Management > Device Configuration.
This list always contains at least one row for the Controller, which is added by the installation. You cannot delete the Controller from this page. To delete the Controller, you must uninstall it.

**Note:** Before you can install a new Member node, you must define the Member in this interface.

The rows on the Device Summary page contain four columns. There is a checkbox to the left of each row for selecting that device for deletion. Click the checkbox in the heading row to select all devices.

### Table 7: Rows on this page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the device is a link. Click a name to edit the configuration for that device. The software assigns default alias names - for the Controller, <em>CUIC1</em>; for the members, <em>Member1</em>, <em>Member2</em>, and so forth. You can edit the default aliases to names that are more meaningful for you.</td>
</tr>
<tr>
<td>Host Address</td>
<td>The IP address for the device.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the device.</td>
</tr>
</tbody>
</table>
| Type       | The type of device: Controller or Member.  
|            | • There is one Controller. It runs both the Administration console and Unified IC Reporting.  
|            | • There can be a maximum of seven Members. Members run the Unified IC Reporting. |

### Table 8: Actions from this page

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add Member</strong></td>
<td>Click <strong>Add Member</strong> to open a blank Device Configuration Detail (page 18) page for a new member. This button is disabled if you have not applied a license or when you have the maximum number of members allowed by your license.</td>
</tr>
</tbody>
</table>
| **Delete** a device | Check the box at the left of the device row and click **Delete**.  
|             | 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 | Each device name is a link. Click the name link to open its Device Configuration Detail (page 18) page. |
Defining the Member Node in the Administration Console

If you intend to add a Member node, you must define the Member in the Administration console before you run the installation for the member.

**Step 1**
To access the Administration console, direct a browser to the URL `http://<HOST ADDRESS>/oamp` where HOST ADDRESS is the IP Address or Hostname of your server.

**Step 2**
Sign in using the system application user ID and password that you defined during installation.

**Step 3**
From the panel in the left, select the **Device Management** drawer. Then select **Device Configuration**.

*Figure 2: Device Configuration*

The Device Configuration page shows the Controller that you have installed. Note that the hostname defaults to the alias CUIC1. (You can change it.)

**Step 4**
On the Device Configuration page, click **Add Member**.

**Step 5**
On the Device Configuration fields for the new member, enter a name by which you can identify the member, the hostname or IP address, and a description for the device.

**Step 6**
Click **Save**.

The Member appears on the Device Configuration list.
Now that the Member is defined in Device Configuration, you can begin to configure and install as documented in the *Installation Guide for Cisco Unified Intelligence Center*.

**Device Configuration Detail**

Use the device configuration detail page to define information about a new device or to edit information about an existing device.

To navigate to this page, click **Device Management > Device Configuration**. Then click **Add Controller** or Add Member to add and configure a new device or click an existing device name to edit the detail configuration for that device.

Text at the top of the page shows the type of server you are adding or editing.

**Table 9: Rows on this page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the device. (Required)</td>
</tr>
<tr>
<td>Host Address</td>
<td>The IP address or hostname of the device. (Required)</td>
</tr>
</tbody>
</table>

You cannot edit the IP address of the Controller on this page.

**Note:** There is a CLI command to change the IP address of the Controller, but that command is unsupported for Unified IC.

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.

**Note:** There is a CLI command to change the IP address of the Member, but that command is unsupported for Unified IC. The only way to change the IP address of a member node is to reinstall the member node.
Log and Trace Settings

Use the Log and Trace Settings page to see the list of Host Addresses for all configured devices and to configure log and trace settings for those devices.

This page is accessed from Device Management > Logging and Tracing.

Click the arrow icon at the left of each host address to expand the row and display the list of server processes running on that device. The server processes are identified by name, and each name is a link.

*Figure 4: Log and Trace Settings*

The host address for the Controller expands to show two processes - OAMPServer and the name for the Unified IC reporting server processes running on the Controller. These names are links.

Click the link to open the Edit Serviceability Settings (page 20) page for that server process.

See also: Troubleshooting Log and Trace Settings ([http://docwiki.cisco.com/wiki/Troubleshooting_Tips_for_Unified_IC_8.0](http://docwiki.cisco.com/wiki/Troubleshooting_Tips_for_Unified_IC_8.0)).

### About Logging and Tracing

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 normal 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.
Log and Trace Settings

There are two ways to review log and tracing information:

- **The Command Line Interface (page 93)**. Using the show trace command.
- **The RTMT (page 47)**

**Edit Serviceability Settings**

This page opens when you click the link for the OAMPServer or CUIC server process on the Log and Trace Settings (page 19) page.

Use the Edit Serviceability Settings page to provide syslog server connection settings and to change the type of logging the servers provide.

*Figure 5: Edit Serviceability Settings*

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

**Log Settings**

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

*Table 10: Log setting rows*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Log Directory Size</td>
<td>Enter a numeric value between 50 and 50,000. The default is 5,000.</td>
</tr>
<tr>
<td>Maximum Log File Size</td>
<td>Enter a numeric value between 1 and 50. The default is 50.</td>
</tr>
</tbody>
</table>

When the directory size exceeds 50,000, the oldest log files are deleted.
When a log size exceeds 50, a new log file is created.

**Syslog Settings**

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

*Table 11: Log file storage rows*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Host</td>
<td>The host address of the primary syslog server that stores the log files.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The port is fixed at 514.</td>
</tr>
<tr>
<td>Backup Host</td>
<td>The host address of the backup syslog server that stores the log files.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The port is fixed at 514.</td>
</tr>
</tbody>
</table>

**Subsystem Settings**

Navigate in this expandable list of subsystems to set the log levels and trace definitions (page 21) for each subsystem.

*Figure 6: SubSystem Settings*

**Actions on this page**

- **Save** - Saves the changes you have made.
- **Cancel** - Undoes all changes you have made since the last save.
- **Refresh** - Undoes all changes and revert fields back to the default values.
- **Reset** - restores the original settings and does not keep your changes.

See also: Log Levels and Trace Level Definitions: Basic and Detailed (page 21)

**Log Levels and Trace Level Definitions: Basic and Detailed**

There are two log levels for all subsystems:

**Basic**

This is the default log level. With this setting, messages and warnings are displayed (INFO, ERROR, and WARN).
When the log level is basic, the trace definitions are not editable.

**Detailed**

If you check the detailed log level, the trace check boxes for Subsystem Specific Trace Definitions and Infrastructure Trace Definitions become editable. You can check the boxes to turn on specific trace code paths to output to the log file.

*Figure 7: Select Detailed to edit Trace Definitions*

Trace Definitions are documented in the *Administration Console User Guide for Cisco Unified Intelligence Center*. They are not documented in the Online help.

There are two ways to review log and trace information:

- The Command Line Interface (show trace).
- **RTMT** (page 47)

**Infrastructure Trace Definitions**

Infrastructure Trace Definitions are the same for CUIC and for Operation Administration Maintenance and Provisioning (OAMP) Infrastructure and OAMP-BO. There are no Infrastructure Trace Definitions for OAMP WSM_BO.

<table>
<thead>
<tr>
<th>Trace</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACEHandledException</td>
<td>Description of the exception and how it was handled</td>
</tr>
<tr>
<td>TRACE_JMX</td>
<td>JMX and management interface related traces.</td>
</tr>
<tr>
<td>TRACE_JMS</td>
<td>JMS and message bus related traces.</td>
</tr>
<tr>
<td>TRACE_HEARTBEAT</td>
<td>Related to heartbeats, heartbeat thread, or heartbeat send/received</td>
</tr>
<tr>
<td>TRACE_PARAM</td>
<td>For any parameters (not just method arguments)</td>
</tr>
<tr>
<td>TRACE_CALL</td>
<td>For traces related to a call / call processing</td>
</tr>
<tr>
<td>TRACE_MESSAGE</td>
<td>For general debug details of incoming/outgoing messages</td>
</tr>
<tr>
<td>TRACE_NOTIFICATION</td>
<td>Trace for notification API</td>
</tr>
<tr>
<td>TRACE_GENERAL_CFG</td>
<td>General traces for config API</td>
</tr>
<tr>
<td>TRACE_OOOQUEUE</td>
<td>Set this bit to enable OoOQueue tracing</td>
</tr>
<tr>
<td>TRACE_METHOD</td>
<td>When entering/exiting a method</td>
</tr>
<tr>
<td>Trace</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>TRACE_LOW_LEVEL</td>
<td>Bits and Bytes, etc</td>
</tr>
</tbody>
</table>

Subsystem Trace Definitions - OAMPServer

**OAMP**

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

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

**Infrastructure**

**Infrastructure Subsystem Specific Trace Definitions**

<table>
<thead>
<tr>
<th>Trace</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACE_STATS</td>
<td>Operations of the Stats Manager</td>
</tr>
<tr>
<td>TRACE_SERVICEABILITY</td>
<td>Traces to do serviceability, the act of logging and tracing</td>
</tr>
<tr>
<td>TRACE_THREAD</td>
<td>All Infrastructure thread operations</td>
</tr>
<tr>
<td>TRACE_SNMP</td>
<td>TRACE_SNMP SNMP Forwarder/logging/stats</td>
</tr>
<tr>
<td>TRACE_SHUTDOWN</td>
<td>Log detailed shutdown info</td>
</tr>
<tr>
<td>TRACE_LICENSING</td>
<td>Log any/all licensing operations</td>
</tr>
<tr>
<td>TRACE_STARTUP</td>
<td>Log detailed startup info</td>
</tr>
<tr>
<td>LOAD_SUBSYSTEM</td>
<td>When loading subsystems</td>
</tr>
<tr>
<td>TRACE_TIMER</td>
<td>Logs when a Timer expires</td>
</tr>
</tbody>
</table>

**OAMP-BO**

**OAMP-BO Subsystem Specific Trace Definitions**

<table>
<thead>
<tr>
<th>Trace</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACE_BULK</td>
<td>To control logging for looping/bulk operations</td>
</tr>
</tbody>
</table>
### Log and Trace Settings

<table>
<thead>
<tr>
<th>Trace</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACE_EXCEPTION</td>
<td>For tracing Exceptions</td>
</tr>
<tr>
<td>TRACEGENERAL_BO</td>
<td>General Traces for OAMP back-end</td>
</tr>
<tr>
<td>TRACE_PARAM</td>
<td>For tracing Parameters</td>
</tr>
<tr>
<td>TRACE_DBACCESS</td>
<td>Trace DB Access for db fetch and modify such as Save, Update, Delete</td>
</tr>
<tr>
<td>TRACE_METHOD</td>
<td>For tracing of Entry/Exit of Methods</td>
</tr>
</tbody>
</table>

#### WSM-BO

**WSM-BO Subsystem Specific Trace Definitions**

<table>
<thead>
<tr>
<th>Trace</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACE_EXCEPTION</td>
<td>For tracing Exceptions</td>
</tr>
<tr>
<td>TRACEGENERAL_BO</td>
<td>General Traces for OAMP back-end</td>
</tr>
<tr>
<td>TRACE_PARAM</td>
<td>For tracing Parameters</td>
</tr>
<tr>
<td>TRACE_DBACCESS</td>
<td>Trace DB Access for db fetch and modify such as Save, Update, Delete</td>
</tr>
<tr>
<td>TRACE_METHOD</td>
<td>For tracing of Entry/Exit of Methods</td>
</tr>
</tbody>
</table>

#### Subsystem Trace Definitions - CUICServer

**CUIC Subsystem Specific Trace Definitions**

CUIC Subsystem, Cache, Thread, Schedule, Util, Statistics, JMX, I18N, L10N, Message, Help

<table>
<thead>
<tr>
<th>Trace</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUIC_SUBSYS_SETUP</td>
<td>Trace for CuicSubsystem setup</td>
</tr>
<tr>
<td>CUIC_SUBSYS_OBJECT</td>
<td>Trace for CuicSubsystem object dump</td>
</tr>
</tbody>
</table>

#### Infrastructure

**Infrastructure Subsystem Specific Trace Definitions**

<table>
<thead>
<tr>
<th>Trace</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACE_STATS</td>
<td>Operations of the Stats Manager</td>
</tr>
<tr>
<td>TRACE_SERVICEABILITY</td>
<td>Traces to do serviceability, the act of logging and tracing</td>
</tr>
<tr>
<td>TRACE_THREAD</td>
<td>All Infrastructure thread operations</td>
</tr>
<tr>
<td>TRACE_SNMP</td>
<td>TRACE_SNMP SNMP Forwarder/logging/stats</td>
</tr>
</tbody>
</table>
CUIC MODEL OBJECTS

**CUIC Model Objects Specific Trace Definitions** for Reports, ReportDefinitions, Templates, Dashboards, Categories, Value Lists, Collections

<table>
<thead>
<tr>
<th>Trace</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MODEL_DASHBOARD</td>
<td>Trace dashboard objects</td>
</tr>
<tr>
<td>MODEL_DATA_SOURCE</td>
<td>Trace data source objects</td>
</tr>
<tr>
<td>MODEL_REPORT_DEFINITION</td>
<td>Trace report definition objects</td>
</tr>
<tr>
<td>MODEL_COLLECTION</td>
<td>Trace collection objects</td>
</tr>
<tr>
<td>MODEL_REPORT</td>
<td>Trace report objects</td>
</tr>
<tr>
<td>MODEL_VALUE_LIST</td>
<td>Trace value list objects</td>
</tr>
</tbody>
</table>

CUIC DATA PROCESSING

**CUIC Data Processing Subsystem Specific Trace Definitions** for DataSource, DataProcessing, Hibernate

<table>
<thead>
<tr>
<th>Trace</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCP</td>
<td>Trace for DCP other than worker threads</td>
</tr>
<tr>
<td>DCP_WORKER</td>
<td>Trace for DCP worker threads</td>
</tr>
</tbody>
</table>

CUIC SECURITY

**CUIC Data Processing Subsystem Specific Trace Definitions** for Encryption, Permission, User, Group, ICM User Synchronization

<table>
<thead>
<tr>
<th>Trace</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERMISSION_OPERATION</td>
<td>Trace for security operation details</td>
</tr>
<tr>
<td>PERMISSION_OBJECT</td>
<td>Trace for security object details</td>
</tr>
</tbody>
</table>
Control Center Drawer

Click Control Center > Device Control to open the Control Center page, where you can check the status of each device, and start, stop, or restart devices. The status is displayed within five seconds of loading the page.

The rows on this page contain five columns, and there is a radio button to the left of each row.

This page always contains at least one row for the Controller.

As soon as you add a device on the Device Configuration (page 15) page, this Control Center page also shows a row for that Cisco Unified Intelligence Center Reporting Server device. Use the Filter (page 88) feature narrow the list of names.

Table 12: Rows on this page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the device.</td>
</tr>
<tr>
<td></td>
<td>For the Controller, this field is populated by default.</td>
</tr>
<tr>
<td></td>
<td>For each member, this field shows the name of the device from the Device Management page. Each name is a link; click the name to open the sign in page for that node.</td>
</tr>
<tr>
<td></td>
<td>Changing the name on this page also changes in on the Device Configuration page.</td>
</tr>
<tr>
<td>Host Address</td>
<td>The IP address for the device.</td>
</tr>
<tr>
<td>Device Type</td>
<td>A description of the device (Controller or Member).</td>
</tr>
<tr>
<td>Server Type</td>
<td>The server type is always CUIC.</td>
</tr>
<tr>
<td>Status</td>
<td>The current state of the device. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Starting - the server is in the process of starting up.</td>
</tr>
</tbody>
</table>
### Field and Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Unknown</td>
<td>- the server or subsystem that communicates with the Administration Console could not be reached.</td>
</tr>
<tr>
<td>• Stopped</td>
<td>- the server is not running.</td>
</tr>
<tr>
<td>• Running (in service)</td>
<td>- the server is running and active.</td>
</tr>
<tr>
<td>• Running (partial service)</td>
<td>- the server is running, but is not ready to work. The server may be starting up, or there may be one or more issues, for instance, the connection to Unified ICM is down.</td>
</tr>
<tr>
<td>• Stopping</td>
<td>- the server is in the process of stopping.</td>
</tr>
</tbody>
</table>

### Actions from this page

You can access and sign in to a member node.

You can start, shutdown, or restart a device by selecting the radio box for the device and clicking the appropriate button. Buttons are dimmed for operations not supported on the device at that time.

The status of the operation is displayed at the bottom of the page. When starting, stopping, or restarting, a confirmation dialog is displayed to confirm the current action you are performing.

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

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Start the device.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Shut down the device. Respond OK or Cancel to the confirmation message.</td>
</tr>
<tr>
<td>Restart</td>
<td>Restart the device.</td>
</tr>
<tr>
<td>Sign in to the Reporting</td>
<td>Click the name of the member node to open a sign in page where you can</td>
</tr>
<tr>
<td>application on a member</td>
<td>enter your user name and password.</td>
</tr>
<tr>
<td>node</td>
<td></td>
</tr>
<tr>
<td>Refresh dropdown</td>
<td>You can refresh the status at any time. For example, if the status is</td>
</tr>
<tr>
<td></td>
<td>unknown, you can change the Refresh for status polling by using the</td>
</tr>
<tr>
<td></td>
<td>drop down menu on the upper-right of the page and click <strong>Go</strong>.</td>
</tr>
<tr>
<td></td>
<td>Refresh options are: No refresh</td>
</tr>
</tbody>
</table>

See also: [Troubleshooting Control Center](http://docwiki.cisco.com/wiki/Troubleshooting_Tips_for_Unified_IC_8.0)
Chapter 5

Cluster Configuration Drawer

This chapter contains the following topics:

- Reporting Configuration, page 29
- Unified CCE User Integration Configuration, page 32
- License File Management, page 34

Reporting Configuration

To navigate to this page, click Cluster Configuration > Reporting Configuration.

This page has these tabs for entering reporting configuration:

- Active Directory Tab (page 29)
- Report Scheduler Email Settings Tab (page 31)

See also: Troubleshooting Reporting Configuration (http://docwiki.cisco.com/wiki/Troubleshooting_Tips_for_Unified_IC_8.0)

Active Directory Tab

Fields on the active directory tab configure the Active Directory server to authenticate reporting users as they log in to the Unified IC web application.

You must configure Active Directory for the Unified ICM/CC supervisors so that they can sign in as Unified IC reporting 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 Admin User Management (page 9) interface, and their credentials are encrypted into the local database.
To navigate to this page, click **Cluster Configuration > Reporting Configuration** and select the Active Directory tab.

**Table 13: Fields on this tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Address and Port for Primary Active Directory Server</td>
<td>Provide the Host name or IP address and the port of the Primary Active Directory server. The port defaults to 389.</td>
</tr>
<tr>
<td>Host Name and Port for Redundant Active Directory Server</td>
<td>Provide the Host name or IP address and the port of the Redundant Active Directory server. The port defaults to 389.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>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.</td>
</tr>
<tr>
<td>Manager Distinguished Name</td>
<td>Enter the Manager Distinguished Name used to login to the Active Directory server, for example, on a default installation of Microsoft AD: <strong>CN=Administrator, CN=users, DC=MYSERVER, DC=COM</strong>. Replace MYSERVER and COM with your respective hostname.</td>
</tr>
<tr>
<td>Manager Password</td>
<td>Enter the Active Directory manager password.</td>
</tr>
<tr>
<td>Confirm Manager Password</td>
<td>Confirm the Active Directory manager password.</td>
</tr>
<tr>
<td>User Search Base</td>
<td>Specify the user search base. For example on a default installation of Microsoft AD, <strong>CN=users, DC=MYSERVER, DC=COM</strong> Replace MYSERVER and COM with your respective hostname.</td>
</tr>
<tr>
<td>Note:</td>
<td>This example assumes 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: <strong>OU=MYUSERS, DC=MYSERVER, DC=COM</strong>. Note that it is &quot;OU=MYUSERS&quot; instead of &quot;CN=MYUSERS&quot;.</td>
</tr>
<tr>
<td>Attribute for User ID</td>
<td>The attribute for the User ID. Generally <strong>sAMAccountName</strong> is the default attribute used by Microsoft AD server.</td>
</tr>
<tr>
<td>Note:</td>
<td>The default is sAMAccountName, indicating the short name (jlopez)</td>
</tr>
<tr>
<td></td>
<td>Using userPrincipalName indicates that the user id entered will be in email format (<a href="mailto:jlopez@company.com">jlopez@company.com</a>).</td>
</tr>
<tr>
<td></td>
<td>Contact your Active Directory Administrator for the correct attribute to use.</td>
</tr>
<tr>
<td>Test Connection button</td>
<td>Click to test the connection to display the test connection status.</td>
</tr>
</tbody>
</table>

**Actions on this tab:**

**Cluster Configuration Drawer**

Administration Console User Guide for Cisco Unified Intelligence Center Release 8.9(3)

30
• **Save** saves the configuration information you entered above for active directory. Note that clicking **Save does not validate the configuration**. Use the **Test Connection** button to test the connection.

• **Refresh** undoes all changes since the last save and reloads the values set at the last save.

Report Scheduler Email Settings Tab

Use the Report Scheduler Email Settings tab 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 IC web application. The report scheduler emails scheduled reports at the exact time they are scheduled.

To navigate to this page, click **Cluster Configuration** > **Reporting Configuration** and select the Report Scheduler Email Settings tab.

**Table 14: Fields on this tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP hostname/IP address</td>
<td>Enter the Hostname or IP address of the SMTP Server. Leave this field blank if you do not have an SMTP server.</td>
</tr>
<tr>
<td>From email address</td>
<td>Enter the email address that is to appear in the From field of emails sent by the Scheduler.</td>
</tr>
<tr>
<td>Use email proxy</td>
<td>Check this if you use a proxy server to reach your SMTP server. The only supported proxy type is http.</td>
</tr>
<tr>
<td>Email proxy hostname</td>
<td>Enter the Hostname or IP address of the proxy server used to reach the SMTP server.</td>
</tr>
<tr>
<td>Email proxy port</td>
<td>Enter the port the Unified IC will use to connect to the SMTP proxy server. This defaults to 80.</td>
</tr>
<tr>
<td>Use SMTP authentication</td>
<td>Check this if your SMTP server expects to receive username/password credentials.</td>
</tr>
<tr>
<td>SMTP Username</td>
<td>If you check the Authenticate checkbox, enter the username that is to be authenticated.</td>
</tr>
<tr>
<td>SMTP Password</td>
<td>If you check the Authenticate checkbox, enter the password that is to be authenticated.</td>
</tr>
<tr>
<td>Test Connection button</td>
<td>Click to test the connection. Unified IC attempts to send an email to check for open connections. The connection status displays next to the button.</td>
</tr>
</tbody>
</table>

**Actions on this tab:**

• **Save** saves the configuration information you entered above for active directory. Note that clicking **Save does not validate the configuration**. Use the **Test Configured Connection** button to test the connection.
Unified CCE User Integration Configuration

- **Refresh** undoes all changes since the last save and reloads the values set at the last save.

### Unified CCE User Integration Configuration

To navigate to this page, click **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 cuicdatabase and can sign in Unified IC with their User ID and Password. They are created as users in Unified IC 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 UCCE User Integration runs, data is retrieved from the UCCE Data Source and two stock Value Lists (Agents and Agent Teams) are updated.

**Note:** You cannot run User Integration until you upload the license.

See also: [Troubleshooting Unified ICM User Integration](http://docwiki.cisco.com/wiki/Troubleshooting_Tips_for_Unified_IC_8.0)

**Warning:** Schedule UCCE 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 UCCE User Integration runs at the same time as the purge, the user integration will fail.

#### Table 15: Fields on this tab:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable UCCE User Integration at...check box</td>
<td>Check this to:</td>
</tr>
<tr>
<td></td>
<td>• Enable UCCE User Integration and to</td>
</tr>
<tr>
<td></td>
<td>• Set the time and the day of week when it is to occur.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Leave this field blank if you do not want to run Unified CCE User Integration. See About Unified CCE User Integration (page 33).</td>
</tr>
<tr>
<td>Hour</td>
<td>Minute</td>
</tr>
<tr>
<td>Day of the week fields</td>
<td>Select one, several, or all days that you want the Unified CCE User Integration synchronization to occur.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Run Status</td>
<td>Shows the status of the last synchronization. Shows PENDING if the synchronization is still in progress.</td>
</tr>
<tr>
<td>Duration</td>
<td>Shows how long the synchronization process took.</td>
</tr>
<tr>
<td>UCCE Supervisors imported</td>
<td>Shows the number of new supervisors imported since the last import. You can view supervisors on the User List in the Unified IC Reporting Interface (Security drawer). Supervisors are imported with their Active Directory credentials and can sign in to Unified IC Reporting with those credentials.</td>
</tr>
<tr>
<td>Team Collections Updated</td>
<td>Shows a count of all teams updated. Teams are resynchronized on each run. Supervisors can view their Agents and Agent Teams collections in the Value List drawer in the Unified IC Reporting interface.</td>
</tr>
</tbody>
</table>

**Actions on this tab:**

- **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.

  This button is disabled if you have not yet applied a license.

- **Save** - Click to save your time and date settings.

- **Refresh** - Click to refresh the page to see changes that others might have made.

See also: About Unified CCE User Integration (page 33).

**About Unified CCE User Integration**

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 IC.

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

**Note:**  
- You cannot run User Integration until you upload the license.
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 UCCE User Integration.

**The tasks are to:**

- Enable Unified CCE User Integration in the Administration interface.
- Complete the configuration of the UCCE Historical Data Source in the Data Sources drawer 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.

**Results of Unified CCE User Integration:**

- Integrated Supervisors can sign in to Unified IC Reporting (provided their Active Directory authentication has been configured.
- Integrated Supervisors are added to the Unified IC Reporting User List with the User Roles of Report Designer and Dashboard Designer.
- The Unified IC Value Lists page is updated with *Agents* and *Agent Teams* collections.
- Integrated Supervisors can view their *Agents* and *Agent Teams* collections ([Unified IC Reporting > Value Lists](#) drawer).
- Integrated Supervisors are granted permissions to *Agents* and *Agent Teams* collections only ([Unified IC Reporting > Security](#) drawer).

Once Unified CCE User Integration schedule is set up, Unified IC is updated with changes to supervisors and their teams every time the synchronisation updates.

**License File Management**

To navigate to this page, click **Cluster Configuration > License Management**.

Use the License Management tab to upload and retrieve your Unified IC license. Once a license is uploaded, this tab displays information about the current license.

Unified IC uses a centralized licensing model, where the license file is uploaded to the Controller through this interface and, based on License Type, is distributed to nodes in the cluster using database replication.

The license file is saved to the operating system, with its properties encrypted, as *Cuic.lic*. 

If the member node is not online when the license file is replicated, Unified IC passes the license information when the member starts up.

**Table 16: Fields on this page:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current License Type</td>
<td>The type of license - Standard, Premium, Lab, or Trial/Demo. See License Types (page 90).</td>
</tr>
<tr>
<td>Maximum number of devices in this cluster Servers</td>
<td>The number of servers the license allows. For most License Types, this shows 8.</td>
</tr>
<tr>
<td>Start Date</td>
<td>For Demo License Types only, shows the date the license became active.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The date the license will expire. For most License Types, this shows <em>Never expires</em>. For Demo licenses, this shows the date 90 days later than the Start date.</td>
</tr>
<tr>
<td>User Count</td>
<td>For Lab License Types only, shows the maximum number of logged in users per device (5).</td>
</tr>
</tbody>
</table>

**Actions on this tab:**

- **Upload license file (Browse)** - If you have no license, click **Browse** and navigate to the local directory where your license (*.lic file) is stored.

- **Apply License** - Click this to apply the license to all devices.

  A message displays indicating that the license file was uploaded successfully and will be distributed in the cluster in approximately one minute.

  **Note:** The databases are polled once a minute for changes. The license replication is not immediate but will occur within a minute.

- **Retrieve** - Click this to open a dialog box where you can choose to open the license file to review it or to save it to your local drive. You might save if, for example, to have a backup copy in the event that your original license is lost or corrupted.

See also:

- **Troubleshooting License Management** (http://docwiki.cisco.com/wiki/Troubleshooting_Tips_for_Unified_IC_8.0)

- How to Obtain Your License (page 89)

- License Types (page 90)
Network Management Drawer

Open this drawer to access the SNMP page.

This chapter contains the following topics:

- SNMP (Simple Network Management Protocol), page 37
- Unified IC SNMP MIBs, page 38

SNMP (Simple Network Management Protocol)

To navigate to this page, click the Network Management drawer.

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 dropdown at the top right of the screen. Then click Go.

The Unified IC SNMP MIBs are documented in the Administration Console User Guide for Cisco Unified Intelligence Center. They are not documented in the Online help.
Unified IC SNMP MIBs

The Unified IC SNMP sub-agent captures the following in a Management Information Base. All are scalar objects.

See also: Troubleshooting SNMP (http://docwiki.cisco.com/wiki/Troubleshooting_Tips_for_Unified_IC_8.0)

Unified IC MIB Structure

- MIBObjects (page 38)
  - CuicGeneralInfo (page 38)
  - CuicLicenseInfo (page 39)
  - CuicReporting (page 40)
  - CuicReportScheduler (page 41)
  - CuicDbInfo (page 41)
  - CuicClusterInfo (page 42)
  - CuicSecurity (page 42)
- MIB Notifications (page 43)

MIB Objects

The Cisco Unified IC MIB Objects are:

- CuicGeneralInfo (page 38)
- CuicLicenseInfo (page 39)
- CuicReporting (page 40)
- CuicReportScheduler (page 41)
- CuicDbInfo (page 41)
- CuicClusterInfo (page 42)
- CuicSecurity (page 42)
- CuicDataSourceInfo (page 42)
This table contains a list of CUIC servers. An entry in this table represents a CUIC 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.

<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cuicGeneralInfoServerName</td>
<td>Host name for the Unified IC server as entered during installation.</td>
</tr>
<tr>
<td>cuicGeneralInfoServerDescription</td>
<td>The description of the Unified IC application installed on this server, as entered for the application during installation</td>
</tr>
<tr>
<td>cuicGeneralInfoVersion</td>
<td>The version number of the Unified IC software installed on the server displayed in the format CUIC_&lt;major&gt;<em>&lt;minor&gt;</em>&lt;buildnumber&gt;.</td>
</tr>
<tr>
<td>cuicGeneralInfoStartTime</td>
<td>This object indicates the starting time for the Unified IC application server.</td>
</tr>
<tr>
<td>cuicGeneralInfoTimeZoneName</td>
<td>The time zone where the Unified IC server is physically located.</td>
</tr>
<tr>
<td>cuicGeneralInfoSystemStatus</td>
<td>The last known status of the application</td>
</tr>
<tr>
<td></td>
<td>Status of the reporting service:</td>
</tr>
<tr>
<td></td>
<td>• 'inService' = The service is up and running optimally, accepting connections.</td>
</tr>
<tr>
<td></td>
<td>• 'partialService' = Some of the components comprising the application are not running; the service is in warning state.</td>
</tr>
<tr>
<td></td>
<td>• 'notresponding' = The service is either shut down or not responding.</td>
</tr>
<tr>
<td></td>
<td>• 'unknown' = The service status is unknown.</td>
</tr>
<tr>
<td>cuicGeneralInfoOpsConsoleURL</td>
<td>The URL for the Unified IC Administration operations console web server.</td>
</tr>
<tr>
<td>cuicGeneralInfoEnableNotifications</td>
<td>This object specifies the notification status to management station, to disable and alternatively enable outbound notifications on this server.</td>
</tr>
</tbody>
</table>
CuicLicenseInfo

An entry in this table describes the Unified IC licensing details. A row is created in this table whenever a Unified license is installed on a server in this cluster.

<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cuicLicenseInfoType</td>
<td>This object specifies the type of license installed.</td>
</tr>
<tr>
<td>cuicLicenseInfoStartTime</td>
<td>The timestamp for when the license was installed and applied.</td>
</tr>
<tr>
<td>cuicLicenseInfoEndTime</td>
<td>The timestamp when the license will expire.</td>
</tr>
<tr>
<td>cuicLicenseInfoHost</td>
<td>The host name of the Controller node where the license is installed. All other nodes in the cluster point to the license on the Controller.</td>
</tr>
</tbody>
</table>

CuicReporting

This table lists statistics of the Unified IC reporting nodes. A row is created in this table when new server is being added to the cluster. A row is deleted when a server is removed from this cluster."

<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cuicReportingDataSourceCount</td>
<td>The number of Data Sources configured in the Unified IC reporting application.</td>
</tr>
<tr>
<td>cuicReportingEngineStatus</td>
<td>The last known status of the reporting engine:</td>
</tr>
<tr>
<td></td>
<td>• 'running' = Service is running and can fetch data from data source</td>
</tr>
<tr>
<td></td>
<td>• 'stopped' = Service is shutdown.</td>
</tr>
<tr>
<td></td>
<td>• 'unknown' = The status is unknown.</td>
</tr>
<tr>
<td>cuicReportingHistoricalReportDefinitionCount</td>
<td>The number of historical report definitions installed on the CUIC application.</td>
</tr>
<tr>
<td></td>
<td>A report definition is template for a report. Each report has an association with a report definition.</td>
</tr>
<tr>
<td>cuicReportingRealTimeReportDefinitionCount</td>
<td>The number of real time report definitions installed on the CUIC application.</td>
</tr>
<tr>
<td>cuicReportingHistoricalReportRunning</td>
<td>The number of historical reports that are currently running.</td>
</tr>
<tr>
<td>cuicReportingHistoricalReportWaiting</td>
<td>The number of historical reports that are currently waiting to execute.</td>
</tr>
<tr>
<td>cuicReportingTotalKickedOffHistoricalReports</td>
<td>The total number of historical reports that have been launched since the server last started.</td>
</tr>
</tbody>
</table>
### CuicReportScheduler

This table lists Report Scheduler health and statistics. A row is created in this table whenever the Scheduler Component is enabled on a server in this cluster.

<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cuicSchedulerStatus</td>
<td>The status of the reporting scheduler engine:</td>
</tr>
<tr>
<td></td>
<td>• 'running' = Service is running and can generate a report on execution</td>
</tr>
<tr>
<td></td>
<td>• 'stopped' = Service is shutdown.</td>
</tr>
<tr>
<td></td>
<td>• 'unknown' = The status is unknown.</td>
</tr>
<tr>
<td>cuicSchedulerEmailServerStatus</td>
<td>The status of the email server:</td>
</tr>
<tr>
<td></td>
<td>• 'running' = Service is running and can send email</td>
</tr>
<tr>
<td></td>
<td>• 'stopped' = Service is shutdown.</td>
</tr>
<tr>
<td></td>
<td>• 'unknown' = The status is unknown.</td>
</tr>
<tr>
<td>cuicSchedulerJobsCompletedCount</td>
<td>The number of jobs that the scheduler service has completed since the server started.</td>
</tr>
<tr>
<td>cuicSchedulerJobsRunningCount</td>
<td>The number of jobs that the scheduler service is currently running. Note that this counter is not the number of reports scheduled.</td>
</tr>
<tr>
<td>cuicSchedulerJobsFailedCount</td>
<td>The number of jobs that the scheduler service has failed to complete successfully</td>
</tr>
</tbody>
</table>

### CuicDbInfo

This table gives the status of the Unified IC database (cuic_data) and some perfmon counters.

The cuidatabase exists on each node in the cluster and stores reports and configurations. The system replicates each cuidatabase to other servers in a cluster.

A row is created in this table whenever a server is added to the cluster. A row is deleted when a server is removed from the cluster.
### Unified IC SNMP MIBs

#### MIB

<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cuicDbInfoStatus</td>
<td>The status of the database server:</td>
</tr>
<tr>
<td></td>
<td>• 'running' = The database server is up and running</td>
</tr>
<tr>
<td></td>
<td>• 'stopped' = The database server is shutdown.</td>
</tr>
<tr>
<td></td>
<td>• 'unknown' = The database server is unknown.</td>
</tr>
<tr>
<td>cuicDbInfoReplicationStatus</td>
<td>The status of the last replication operation:</td>
</tr>
<tr>
<td></td>
<td>• 'success' = Replication performed successfully.</td>
</tr>
<tr>
<td></td>
<td>• 'fail' = Replication failed.</td>
</tr>
<tr>
<td></td>
<td>• 'unknown' = Failed to get replication status.</td>
</tr>
<tr>
<td>cuicDbInfoTmpSpaceUsed</td>
<td>The number megabytes of disk space used. The value is in MB.</td>
</tr>
<tr>
<td>cuicDbInfoSpaceUsed</td>
<td>The number megabytes of temporary space used. The value is in MB.&quot;</td>
</tr>
</tbody>
</table>

#### CuicClusterInfo

This table describes the Unified IC cluster.

<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cuicClusterName</td>
<td>The unique name of cluster, which helps in associating a device with the cluster.</td>
</tr>
<tr>
<td>cuicClusterServerCount</td>
<td>Number of Unified IC servers in the cluster</td>
</tr>
<tr>
<td>cuicClusterFirstNodeName</td>
<td>The hostname of the first node in the cluster. This is the Controller (publisher) node.</td>
</tr>
</tbody>
</table>

#### CuicSecurity

This table gives information about Users and User Groups.

<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cuicSecurityUsersConfigured</td>
<td>The number of users that have been created to access Unified IC</td>
</tr>
<tr>
<td>cuicSecurityUsersLoggedIn</td>
<td>The number of users currently signed in.</td>
</tr>
<tr>
<td>cuicSecurityLoginFailedAttempts</td>
<td>The number of rejected login attempts.</td>
</tr>
<tr>
<td>cuicSecurityGroupsConfigured</td>
<td>The number of user groups created on this server.</td>
</tr>
</tbody>
</table>
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 IC 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.

Table 17: CuicDataSourceInfo MIB Objects

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

MIB Notifications (CUIC TRAPs)

Trap notifications are sent by Unified IC when unusual conditions occur that can potentially affect the functioning of a Unified IC 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.

Unified IC supports a generic trap and raises SNMP traps on the following events:

- Database service going offline
- DB Replication failure
- Failing to run a scheduled report.
- Report execution failure
Table 18: Unified IC Notification Event attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cuicEventId</td>
<td>The unique notification message identifier assigned by the Unified IC application. This identifier is unique for each different notification but consistent for each instance of the same notification.</td>
</tr>
<tr>
<td>cuicEventHostName</td>
<td>The host name or the fully qualified domain name of the Unified IC server from which this event originated.</td>
</tr>
<tr>
<td>cuicEventAppName</td>
<td>The service-specific name of the functional service that generated this notification.</td>
</tr>
<tr>
<td>cuicEventName</td>
<td>The service-specific name of the Unified IC service notification message, used to group and correlate similar notifications.</td>
</tr>
<tr>
<td>cuicEventState</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• '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.</td>
</tr>
<tr>
<td></td>
<td>• 'clear' = indicates that the condition which generated a previous raise notification has been resolved.</td>
</tr>
</tbody>
</table>
| 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.

<table>
<thead>
<tr>
<th>cuicEventTimestamp</th>
<th>The date and time that the notification was generated on the originating device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cuicEventText</td>
<td>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.</td>
</tr>
</tbody>
</table>

**ThreadPool Events**

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

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThreadsMaxAvailable</td>
<td>The maximum number of threads available to the Unified IC web server thread pool manager.</td>
</tr>
<tr>
<td>ThreadsRunning</td>
<td>The number of threads that are currently running tasks.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Object</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>QueuedTasks</td>
<td>the number of queued tasks. A task is a job, performed by one or more thread</td>
</tr>
<tr>
<td>QueuedTasksMax</td>
<td>The maximum number of queued tasks.</td>
</tr>
</tbody>
</table>

**EnvInfo Events**

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

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WaErrors</td>
<td>The total number of HTTP errors (for example, 401 Unauthorized) encountered by a Unified IC web application</td>
</tr>
<tr>
<td>WaSessionsActive</td>
<td>The number of currently active (in use) sessions for the web application.</td>
</tr>
<tr>
<td>JvmPercentCPUTime</td>
<td>The percentage of CPU utilized by the Tomcat JVM. This object is for the Unified IC Tomcat JVM object</td>
</tr>
<tr>
<td>JvmMemoryFree</td>
<td>The amount of free dynamic memory in the Unified IC Tomcat Java Virtual Machine.</td>
</tr>
<tr>
<td>JvmMemoryTotal</td>
<td>The Tomcat Java Virtual Machine current total dynamic memory, including free and in-use memory.</td>
</tr>
<tr>
<td>JvmMemoryMax</td>
<td>The Unified IC Tomcat Java Virtual Machine maximum dynamic size.</td>
</tr>
<tr>
<td>TomcatThreadsBusy</td>
<td>The Unified IC Tomcat Connector’s current number of busy/in-use request processing threads.</td>
</tr>
<tr>
<td>TomcatThreadsTotal</td>
<td>The Unified IC tomcat connector’s current total number of request processing threads, including available and in-use threads</td>
</tr>
<tr>
<td>TomcatThreadsMax</td>
<td>This object indicates the Connector maximum number of request processing threads. Each incoming request on a Unified IC 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</td>
</tr>
</tbody>
</table>
The RTMP Plugin Download page includes a link to download the Real Time Monitoring Tool (RTMT).

RTMT runs as a client-side application and can be installed on a Windows workstation. It is cluster-aware and provides critical service and performance monitoring (perfmon), trace/log collection and viewing, and Alert Management on the node for the IP address you request when you launch the RTMT. It 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, and
- Monitor performance counters.

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

See also: Download and Launch RTMT (page 48).

Troubleshooting RTMT (http://docwiki.cisco.com/wiki/Troubleshooting_Tips_for_Unified_IC_8.0)
Download and Launch RTMT

**On the download page:**

1. Select the Windows platform.

2. Click **Download**.

3. Run the file or save the CuicServRtmtPlugin executable file and then run it from the saved location.

4. Follow the prompts and click the buttons on the installation screens.

**To launch:**

1. Launch RTMT from the desktop icon.

2. In the Host IP Address field, enter the IP address for the node you want to monitor.

3. Enter the User Name and Password for a Super User. (Only a Super User can install RTMT.)

4. Accept the default port (8443).

5. Check **Secure Connection**.

   You see an error if the Host IP Address is not found or there is no network connection.

6. Click **Yes** to accept the certificate.

7. Click **OK** to accept the default configuration.

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

**Note:** *The performance counters are documented in the Administration Console User Guide for Cisco Unified Intelligence Center. They are not documented in the Online help.*

**Required Services for Supporting the RTMT Client**

RTMT users the following services/servlets:
• Cisco AMC service
• Cisco Unified 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
• Cisco Serviceability Reporter

Manage these services from the Cisco Unified Serviceability (page 80) application.

RTMT Integration with Unified IC

Tracing and Logging

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

Figure 9: RTMTTraceLog

Critical Services.

Unified IC exposes service information through the RTMT Critical Services interface.
Figure 10: RTMT Critical Services

Uniﬁed IC exposes perfmon information and statistics through the RTMT Tools > Alert Central interface.

Figure 11: RTMT Alerts

Perfmon and Statistics.

Uniﬁed IC exposes perfmon information and statistics through the RTMT Performance interface.
The RTMT Interface

The RTMT system monitoring objects on the left panel of the RTMT page are:

- **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 CPU usage and Virtual memory usage for the server.
  
  - Process - Displays information on the processes running on the server.
  
  - Disk Usage - Displays information on 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).

To view the CUIC Services, click the tab for an Intelligence Center node. See Unified IC Counters (page 55).

• **Performance**

Performance monitoring allows you to:

– Monitor performance counters related to the system and to the Unified IC application.

– Continuously monitor a set of preconfigured objects and receive notification in the form of an email message.

– Associate counter threshold settings to alert notification.

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

– Display up to six perfmon counters in one chart for performance comparisons.

– Use performance queries to add a counter to monitor.

Performance objects are:

– CPU and Memory - Displays information on CPU usage and Virtual memory usage for the server.

– Process - Displays information on the processes running on the server.

– Disk Usage - Displays information on 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).

To view the CUIC Services, click the tab for an Intelligence Center node. See Unified IC Counters (page 55).

• **Performance Log Viewer**

The 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 current status of every alert in the system. Click the Intelligence Center tab to see Unified IC alerts.

Trace & Log Central
– Allows you to configure on-demand trace collections for a specific date range or absolute time.

Job Status
– Shows the status of trace collection events.

Syslog Viewer
– Use to view, by node, the system, application, and security logs.

Unified IC Performance Objects and Counters

Unified IC performance objects are named for system components that generate data. Each performance object provides performance counters that represent data for specific to that object. For example, the CUIC Licensing performance object has counters for License Start and License Expiration dates. The CUIC 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.
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 IC and explains the counters for each.

**Note:** Online help is available for each counter. Right-click the counter and select Counter Description.
For information on the objects and counters that are kept for the operating system, refer to the RTMT online help.

Unified IC Counters

Counters:

- CUIC Tomcat Connector (page 56)
- CUIC Tomcat JVM (page 57)
- CUIC Tomcat Web Application (page 57)
- DB Change Notification Client (page 57)
- DB Change Notification Server (page 58)
- DB Local DSN (page 59)
- DB User Host Information Counters (page 59)
- DB Performance Info (page 59)
- Enterprise Replication DBSpace Monitors (page 59)
- Enterprise Replication Perfmon Counters (page 59)
- Intelligence Center General Information section (page 60)
- Intelligence Center JVM Statistics (page 60)
- Intelligence Center License Information section (page 61)
The Tomcat Connector object provides information about Tomcat non-secure and secure Hypertext Transport Protocol (HTTP) connectors. A Tomcat Connector represents an endpoint that receives requests and sends responses.

The Connector handles HTTP/HTTPS requests and sends HTTP/HTTPS responses that occur when Cisco Unified Intelligence Center web pages are accessed. There are two instances of this object based on the Secure Sockets Layer (SSL) status of the URLs for web applications: **http-8443** for SSL (HTTPS) connections and **http-8081** for non-SSL (HTTP) connections.

<table>
<thead>
<tr>
<th><strong>Counter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors</td>
<td>The total number of HTTP errors (for example, 401 Unauthorized) encountered by the Connector.</td>
</tr>
<tr>
<td>MBytes Received</td>
<td>The total number of data received by the Connector.</td>
</tr>
<tr>
<td>MBytes Sent</td>
<td>The total number of data that the Connector has sent.</td>
</tr>
<tr>
<td>Requests</td>
<td>The total number of requests that have been handled by the Connector.</td>
</tr>
</tbody>
</table>
## 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 IC.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KBytesMemoryFree</td>
<td>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 Cisco 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.</td>
</tr>
<tr>
<td>MemoryMax</td>
<td>The maximum dynamic memory block size for the Unified IC Tomcat Java Virtual Machine.</td>
</tr>
<tr>
<td>MemoryTotal</td>
<td>This current total dynamic memory block size - including free and in-use memory - for the Tomcat Java Virtual Machine.</td>
</tr>
</tbody>
</table>

## 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.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors</td>
<td>The total number of HTTP errors (for example, 401 Unauthorized) encountered by a Cisco Unified Intelligence Center (CUIC)-related web application.</td>
</tr>
<tr>
<td>Requests</td>
<td>The total number of requests handled by the web application. Each time a web application is accessed, its Requests counter increments accordingly.</td>
</tr>
<tr>
<td>Sessions Active</td>
<td>The number of currently active (in use) sessions the web application currently has.</td>
</tr>
</tbody>
</table>
DB Change Notification Client

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MessagesProcessed</td>
<td>The number of database change notifications that have been processed. This counter refreshes every 15 seconds by default.</td>
</tr>
<tr>
<td>MessagesProcessing</td>
<td>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.</td>
</tr>
<tr>
<td>QueueHeadCounter</td>
<td>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.</td>
</tr>
<tr>
<td>QueueMax</td>
<td>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.</td>
</tr>
<tr>
<td>QueueTailPointer</td>
<td>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.</td>
</tr>
<tr>
<td>TablesSubscribed</td>
<td>The number of tables to which this client has subscribed.</td>
</tr>
</tbody>
</table>

DB Change Notification Server

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clients</td>
<td>The total number of change notification clients.</td>
</tr>
<tr>
<td>CNProcessed</td>
<td>The total number of change notification messages processed by server since reboot.</td>
</tr>
<tr>
<td>QueueDelay</td>
<td>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.</td>
</tr>
<tr>
<td>QueuedRequestsInDB</td>
<td>The number of records from DBCNQueue table.</td>
</tr>
<tr>
<td>QueuedRequestsInMemory</td>
<td>The number of change notification requests queued in memory.</td>
</tr>
</tbody>
</table>
DB Change Notification Subscriptions

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SubscribedTable</td>
<td>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.</td>
</tr>
</tbody>
</table>

DB Local DSN

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CcmDbSpace_Used</td>
<td>The amount of ccm dbspace consumed.</td>
</tr>
<tr>
<td>CcmtempDbSpace_Used</td>
<td>The amount of ccment temp dbspace consumed.</td>
</tr>
<tr>
<td>CNDbSpace_Used</td>
<td>The percentage of CN dbspace consumed.</td>
</tr>
<tr>
<td>Local DSN</td>
<td>The data source name (DSN) that is being referenced from the local machine.</td>
</tr>
<tr>
<td>RootDBSpaceUsed</td>
<td>The amount of root dbspace consumed.</td>
</tr>
<tr>
<td>SharedMemory_Free</td>
<td>Total shared memory that is free.</td>
</tr>
<tr>
<td>SharedMemory_Used</td>
<td>Total shared memory that is used.</td>
</tr>
</tbody>
</table>

DB User Host Information Counters

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB:User:Host Instances</td>
<td>The number of connections that are present for each instance of DB:User:Host.</td>
</tr>
</tbody>
</table>

DBPerformance Info

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CuicDbSpace_Used</td>
<td>The amount of CUIC dbspace consumed.</td>
</tr>
<tr>
<td>CuicSbSpace_Used</td>
<td>The amount of CUIC Blob Space consumed.</td>
</tr>
<tr>
<td>CuicTempDbSpace_Used</td>
<td>The amount of CUIC Temp dbspace consumed.</td>
</tr>
<tr>
<td>RootDbSpace_Used</td>
<td>The amount of root dbspace consumed.</td>
</tr>
</tbody>
</table>

Enterprise Replication DBSpace Monitors

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERDbSpace_Used</td>
<td>The amount of enterprise replication DbSpace consumed.</td>
</tr>
<tr>
<td>ERSBDbSpace_Used</td>
<td>The amount of ERDbSpace consumed.</td>
</tr>
</tbody>
</table>
### Enterprise Replication Perfmon Counters

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReplicationQueueDepth</td>
<td>Displays the replication queue depth</td>
</tr>
</tbody>
</table>

### Intelligence Center General Information section

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeviceType</td>
<td>The number id of the device type.</td>
</tr>
<tr>
<td>Global StatisticInterval</td>
<td>Size in milliseconds of the global statistics interval</td>
</tr>
<tr>
<td>InetAddress Type</td>
<td>The type of the ip address of the device, either IPv4 or IPv6</td>
</tr>
<tr>
<td>Time Zone Offset Hours</td>
<td>The hours component of the offset of the default configured timezone</td>
</tr>
<tr>
<td>Time Zone Offset Minutes</td>
<td>The minutes component of the offset of the default configured timezone</td>
</tr>
<tr>
<td>Uptime (sec)</td>
<td>[null]</td>
</tr>
</tbody>
</table>

### Intelligence Center JVM Statistics

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnvMaxThreadsUsed</td>
<td>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 Cisco Intelligence Center standalone and thread pool threads as well as threads created by the web application server running within the same runtime environment</td>
</tr>
<tr>
<td>EnvRtCommitMemUsed</td>
<td>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 Mega bytes</td>
</tr>
<tr>
<td>EnvRtCurrMemAvail</td>
<td>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.</td>
</tr>
<tr>
<td>EnvRtCurrMemUsed</td>
<td>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</td>
</tr>
</tbody>
</table>
### Counter Description

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnvRtCurrThreadsInUse</td>
<td>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 Cisco Intelligence Center standalone and thread pool threads as well as those threads created by the web application server running within the same runtime environment.</td>
</tr>
<tr>
<td>EnvRtMaxMemAvail</td>
<td>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 expressed as a count of Mega bytes.</td>
</tr>
<tr>
<td>EnvRtMaxMemUsed</td>
<td>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 Mega bytes and indicates the high water mark of memory that can be used by the runtime environment.</td>
</tr>
<tr>
<td>EnvRtUpTime</td>
<td>The real-time up time object is a real-time snapshot metric indicating how long the Cisco Intelligence Center application has been running. The object value is expressed as a count of milliseconds that have elapsed since the application began executing.</td>
</tr>
</tbody>
</table>

### Intelligence Center License Information section

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Count</td>
<td>The number of concurrent nodes this license enables</td>
</tr>
<tr>
<td>User Count</td>
<td>The number of concurrent users this license enables</td>
</tr>
</tbody>
</table>

### Intelligence Center System Condition Table

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUIC_DATASOURCE_UNAVAILABLE</td>
<td>This counter is no longer valid with the counter value -1. It has been rendered obsolete by the Await Write Time counter.</td>
</tr>
<tr>
<td>CUIC_DB_REPLICATION_FAILED</td>
<td>Database replication failed</td>
</tr>
<tr>
<td>CUIC_LICENSE_EXPIRED</td>
<td>CUIC Application license has expired</td>
</tr>
<tr>
<td>CUIC_REPORT_EXECUTION_FAILED</td>
<td>Could not run the report. Could be because associated datasource is offline</td>
</tr>
<tr>
<td>CUIC_SERVICE_UNAVAILABLE</td>
<td>Service going down</td>
</tr>
<tr>
<td>Counter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Infrastructure_DEADLOCK_DETECTED</td>
<td>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.</td>
</tr>
<tr>
<td>Infrastructure_LICENSE_EXPIRED</td>
<td>There is an expired feature in the the license file.</td>
</tr>
<tr>
<td>Infrastructure_LICENSE_EXPIRING</td>
<td>There is a feature in the license file that will expire within the next 14 days.</td>
</tr>
<tr>
<td>Infrastructure_LICENSE_NO_LICENSE</td>
<td>No license file was loaded. Using default evaluation license.</td>
</tr>
<tr>
<td>Infrastructure_LICENSE_PROBLEM</td>
<td>There is an error in the license file.</td>
</tr>
<tr>
<td>Infrastructure_LOG_PURGER_ERROR</td>
<td>An error occurred while log files were being purged.</td>
</tr>
<tr>
<td>Infrastructure_PERSISTENT_STORE_SIZE_ALMOST_FULL</td>
<td>The message store that persists reporting data during a connection loss is approaching capacity. If it fills completely, reporting data will be lost.</td>
</tr>
<tr>
<td>Infrastructure_PERSISTENT_STORE_SIZE_FULL</td>
<td>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.</td>
</tr>
<tr>
<td>Infrastructure_PERSISTENT_STORE_SIZE_WARN</td>
<td>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.</td>
</tr>
<tr>
<td>Infrastructure_PORT_SECURITY_MANAGER_ERROR_LOADING</td>
<td>Error manipulating PortSecurityManager firewall rules</td>
</tr>
<tr>
<td>Infrastructure_SC_JMX_CONFIGURATION_ERROR</td>
<td>There is a configuration problem with JMX ports.</td>
</tr>
<tr>
<td>Infrastructure_SERVER_NOT_READY</td>
<td>The Server state is not ready.</td>
</tr>
<tr>
<td>Infrastructure_SNMP_CONNECTION_ERROR</td>
<td>The connection to SNMP Subagent Failed.</td>
</tr>
<tr>
<td>Infrastructure_SOFTWARE_CONFIGURATION_ERROR</td>
<td>There is an error in the files configuring the software on the disk.</td>
</tr>
<tr>
<td>Infrastructure_SUBSYSTEM_HEARTBEAT_FAILED</td>
<td>Heartbeats from one or more subsystems have stopped.</td>
</tr>
<tr>
<td>Infrastructure_SUBSYSTEM_START_FAILURE</td>
<td>One or more subsystems failed to start.</td>
</tr>
<tr>
<td>Infrastructure_SUBSYSTEM_STOP_FAILURE</td>
<td>One or more subsystems failed to stop.</td>
</tr>
<tr>
<td>Infrastructure_SYSTEM_SHUT_DOWN</td>
<td>One or more subsystems failed to stop.</td>
</tr>
<tr>
<td>RS_CONFIG_UNAVAILABLE</td>
<td>System detected critical error accessing configuration</td>
</tr>
</tbody>
</table>
### Counter & Description

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS_DATABASE_UNAVAILABLE</td>
<td>System detected critical error with database</td>
</tr>
<tr>
<td>RS_MAINTENANCE_IN_PROGRESS</td>
<td>System has detected maintenance in progress on Reporting Server</td>
</tr>
<tr>
<td>RS_SYSTEM_THRESHOLD_REACHED</td>
<td>System has detected a critical system threshold reached on Reporting Server</td>
</tr>
<tr>
<td>RS_UNRECOVERABLE_ERROR</td>
<td>System has detected an internal error within Reporting Server which may prevent it from functioning correctly. Restart may be required.</td>
</tr>
</tbody>
</table>

### Intelligence Center Thread Pool Section

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Thread Count</td>
<td>Number of threads currently executing a task.</td>
</tr>
<tr>
<td>Core Pool Size</td>
<td>Minimum number of threads the thread pool is configured to have.</td>
</tr>
<tr>
<td>Largest Pool Size</td>
<td>The largest number of threads that have ever simultaneously been in the pool.</td>
</tr>
<tr>
<td>Maximum Pool Size</td>
<td>Maximum number of threads to which the thread pool can grow.</td>
</tr>
<tr>
<td>Pool Size</td>
<td>Number of currently available threads. Calculated from (total pool size) - (number of active threads)</td>
</tr>
<tr>
<td>Task Queue Size</td>
<td>The number of tasks currently queued for execution waiting for a thread.</td>
</tr>
</tbody>
</table>

### IP

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

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frag Creates</td>
<td>The number of IP datagrams fragments that have been generated at this entity.</td>
</tr>
<tr>
<td>Frag Fails</td>
<td>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.</td>
</tr>
<tr>
<td>Frag OKs</td>
<td>The number of IP datagrams that were successfully fragmented at this entity.</td>
</tr>
<tr>
<td>In Delivers</td>
<td>The number of input datagrams that were delivered to IP user protocols. This includes Internet Control Message Protocol (ICMP).</td>
</tr>
<tr>
<td>In Discards</td>
<td>The number of input IP datagrams where no problems were encountered, but which were discarded. Lack of buffer space</td>
</tr>
<tr>
<td>Counter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>provides one possible reason. This counter does not include any datagrams that were discarded while awaiting reassembly.</td>
<td></td>
</tr>
<tr>
<td>In HdrErrors</td>
<td>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.</td>
</tr>
<tr>
<td>In Receives</td>
<td>The number of input datagrams that were received from all network interfaces. This counter includes datagrams that were received with errors.</td>
</tr>
<tr>
<td>In UnknownProtos</td>
<td>The number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.</td>
</tr>
<tr>
<td>InOut Requests</td>
<td>The number of incoming IP datagrams that were received and the number of outgoing IP datagrams that were sent.</td>
</tr>
<tr>
<td>Out Discards</td>
<td>The number of output IP datagrams that were not transmitted and were discarded. Lack of buffer space provides one possible reason.</td>
</tr>
<tr>
<td>Out Requests</td>
<td>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.</td>
</tr>
<tr>
<td>Reasm Fails</td>
<td>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.</td>
</tr>
<tr>
<td>Reasm OKs</td>
<td>The number of IP datagrams that were successfully reassembled.</td>
</tr>
<tr>
<td>Reasm Reqds</td>
<td>The number of IP fragments that were received that required reassembly at this entity.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frag Creates</td>
<td>The number of IP datagrams fragments that have been generated at this entity.</td>
</tr>
<tr>
<td>Frag Fails</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 7-1: IP Statistics Description

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frag OKs</td>
<td>The number of IP datagrams that were successfully fragmented at this entity</td>
</tr>
<tr>
<td>In Delivers</td>
<td>The number of input datagrams that were delivered to IP user protocols. This includes Internet Control Message Protocol (ICMP).</td>
</tr>
<tr>
<td>In Discards</td>
<td>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.</td>
</tr>
<tr>
<td>In HdrErrors</td>
<td>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.</td>
</tr>
<tr>
<td>In Receives</td>
<td>The number of input datagrams that were received from all network interfaces. This counter includes datagrams that were received with errors.</td>
</tr>
<tr>
<td>In UnknownProtos</td>
<td>The number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.</td>
</tr>
<tr>
<td>InOut Requests</td>
<td>The number of incoming IP datagrams that were received and the number of outgoing IP datagrams that were sent.</td>
</tr>
<tr>
<td>Out Discards</td>
<td>The number of output IP datagrams that were not transmitted and were discarded. Lack of buffer space provides one possible reason.</td>
</tr>
<tr>
<td>Out Requests</td>
<td>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.</td>
</tr>
<tr>
<td>Reasm Fails</td>
<td>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.</td>
</tr>
<tr>
<td>Reasm OKs</td>
<td>The number of IP datagrams that were successfully reassembled.</td>
</tr>
<tr>
<td>Reasm Reqds</td>
<td>The number of IP fragments that were received that required reassembly at this entity.</td>
</tr>
</tbody>
</table>

Memory

The memory object provides information about the usage of physical memory and swap memory on the server.
<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Mem Used</td>
<td>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.</td>
</tr>
<tr>
<td>% Page Usage</td>
<td>The percentage of active pages.</td>
</tr>
<tr>
<td>% VM Used</td>
<td>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.</td>
</tr>
<tr>
<td>Buffers KBytes</td>
<td>The capacity of buffers in your system in kilobytes.</td>
</tr>
<tr>
<td>Cached KBytes</td>
<td>The amount of cached memory in kilobytes.</td>
</tr>
<tr>
<td>Free KBytes</td>
<td>The total amount of memory that is available in your system in kilobytes.</td>
</tr>
<tr>
<td>Free Swap KBytes</td>
<td>The amount of free swap space that is available in your system in kilobytes.</td>
</tr>
<tr>
<td>HighFree</td>
<td>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 certain physical address, and its amount depends on the total memory and the type of kernel on the system.</td>
</tr>
<tr>
<td>HighTotal</td>
<td>The total amount of memory in the high region.</td>
</tr>
<tr>
<td>LowFree</td>
<td>The free low (non-paged) memory for kernel.</td>
</tr>
<tr>
<td>LowTotal</td>
<td>The total low (non-paged) memory for kernel.</td>
</tr>
<tr>
<td>PageFaultsPerSec</td>
<td>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.</td>
</tr>
<tr>
<td>PageMajorFaultsPerSec</td>
<td>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).</td>
</tr>
<tr>
<td>Pages</td>
<td>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.</td>
</tr>
<tr>
<td>Pages Input</td>
<td>The total number of pages that the system paged in from the disk.</td>
</tr>
<tr>
<td>Pages Input Per Sec</td>
<td>The total number of kilobytes the system paged in from disk per second.</td>
</tr>
<tr>
<td>Pages Output</td>
<td>The total number of pages that the system paged out to the disk.</td>
</tr>
<tr>
<td>Pages Output Per Sec</td>
<td>This represents the total number of kilobytes the system paged out to disk per second.</td>
</tr>
<tr>
<td>Counter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Shared KBytes</td>
<td>The amount of shared memory in your system in kilobytes.</td>
</tr>
<tr>
<td>SlabCache</td>
<td>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 slabinfo.</td>
</tr>
<tr>
<td>SwapCached</td>
<td>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.</td>
</tr>
<tr>
<td>Total KBytes</td>
<td>The total amount of memory in your system in kilobytes.</td>
</tr>
<tr>
<td>Total Swap KBytes</td>
<td>The total amount of swap space in your system in kilobytes.</td>
</tr>
<tr>
<td>Total VM KBytes</td>
<td>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.</td>
</tr>
<tr>
<td>Used KBytes</td>
<td>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.</td>
</tr>
<tr>
<td>Used Swap KBytes</td>
<td>The amount of swap space that is in use on your system in kilobytes.</td>
</tr>
<tr>
<td>Used VM KBytes</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Network Interface**

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

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxBytes</td>
<td>The number of bytes, including framing characters, that was received on the interface.</td>
</tr>
<tr>
<td>Rx Dropped</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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
<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interfaces) that contained errors that prevented them from being deliverable to a higher layer protocol</td>
<td></td>
</tr>
<tr>
<td>Rx Multicast</td>
<td>This represents the number of multicast packets that was received on this interface.</td>
</tr>
<tr>
<td>Rx Packets</td>
<td>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.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>This represents the total number of received (Rx) bytes and transmitted (Tx) bytes.</td>
</tr>
<tr>
<td>Total Packets</td>
<td>This represents the total number of received (Rx) packets and transmitted (Tx) packets.</td>
</tr>
<tr>
<td>Tx Bytes</td>
<td>This represents the total number of octets, including framing characters, that was transmitted out of the interface.</td>
</tr>
<tr>
<td>Tx Dropped</td>
<td>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.</td>
</tr>
<tr>
<td>Tx Errors</td>
<td>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.</td>
</tr>
<tr>
<td>Tx Packets</td>
<td>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.</td>
</tr>
<tr>
<td>Tx QueueLen</td>
<td>This represents the length, measured in packets, of the output packet queue.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number or Replicates Created</td>
<td>Displays the number of replicates that were created by Informix for the DB tables. This counter displays information during Replication Setup.</td>
</tr>
<tr>
<td>Replicate_State</td>
<td>This counter represents the state of replication. The following list provides possible values:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Counter</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>• 1 = Replication setup script fired from this node. Cisco recommends that you run utils dbreplication status on the CLI to determine the location and cause of the failure.</td>
<td></td>
</tr>
<tr>
<td>• 2 = Good Replication.</td>
<td></td>
</tr>
<tr>
<td>• 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. Cisco recommends that you run utils dbreplication status on the CLI to determine the location and cause of the failure.</td>
<td></td>
</tr>
<tr>
<td>• 4 = Replication setup did not succeed.</td>
<td></td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>% CPU Time</td>
<td>The percentage of CPU time that is dedicated to handling IO requests that were issued to the disk.</td>
</tr>
<tr>
<td>% Used</td>
<td>The percentage of disk space that is in use on this file system.</td>
</tr>
<tr>
<td>% Wait in Read</td>
<td>Not used. It has been rendered obsolete by the Await Read Time counter.</td>
</tr>
<tr>
<td>% Wait in Write</td>
<td>Not used. It has been rendered obsolete by the Await Write Time counter.</td>
</tr>
<tr>
<td>Await Read Time</td>
<td>The average time, measured in milliseconds, for read requests issued to the device to be served.</td>
</tr>
<tr>
<td>Await Time</td>
<td>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</td>
</tr>
<tr>
<td>Await Write Time</td>
<td>The average time, measured in milliseconds, for write requests that are issued to the device to be served.</td>
</tr>
<tr>
<td>Queue Length</td>
<td>The average queue length for the requests that were issued to the disk.</td>
</tr>
<tr>
<td>Read Bytes Per Sec</td>
<td>The amount of data in bytes per second that was read from the disk.</td>
</tr>
<tr>
<td>Total Mbytes</td>
<td>The amount of total disk space in megabytes that is on this file system.</td>
</tr>
<tr>
<td>Used Mbytes</td>
<td>The amount of disk space in megabytes that is in use on this file system.</td>
</tr>
</tbody>
</table>
### Counter | Description
--- | ---
Write Bytes Per Sec | The amount of data that was written to the disk in bytes per second.

### Process

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>% CPU Time</td>
<td>Expressed as a percentage of total CPU time, represents the task's share of the elapsed CPU time since the last update.</td>
</tr>
<tr>
<td>% Memory Usage</td>
<td>The percentage of physical memory that a task is currently using.</td>
</tr>
<tr>
<td>Data Stack Size</td>
<td>The stack size for task memory status.</td>
</tr>
<tr>
<td>Nice</td>
<td>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.</td>
</tr>
<tr>
<td>Page Fault Count</td>
<td>The number of major page faults that a task encountered that required the data to be loaded into memory.</td>
</tr>
<tr>
<td>PID</td>
<td>The task's unique process ID, which periodically wraps, though never restarting at zero.</td>
</tr>
<tr>
<td>Process Status</td>
<td>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.</td>
</tr>
<tr>
<td>Shared Memory Size</td>
<td>The amount of shared memory, in KB, that a task is using. Other processes could potentially share the same memory.</td>
</tr>
<tr>
<td>STime</td>
<td>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.</td>
</tr>
<tr>
<td>Thread Count</td>
<td>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.</td>
</tr>
<tr>
<td>Total CPU Time Used</td>
<td>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.</td>
</tr>
<tr>
<td>UTime</td>
<td>The amount of time, measured in jiffies, that the task has been scheduled for in user mode. One second is equal to 100 jiffies.</td>
</tr>
<tr>
<td>VmDate</td>
<td>The virtual memory usage of the heap for the task in kilobytes (KB).</td>
</tr>
</tbody>
</table>
### Processor

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VmRSS</td>
<td>The virtual memory (Vm) resident set size (RSS) that is currently in physical memory in kilobytes (KB), including Code, Data, and Stack.</td>
</tr>
<tr>
<td>VmSize</td>
<td>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</td>
</tr>
<tr>
<td>% CPU Time</td>
<td>The processor's share of the elapsed CPU time excluding the idle time since last update, expressed as a percentage of CPU time.</td>
</tr>
<tr>
<td>Idle Percentage</td>
<td>The percentage of time that the CPU or CPUs were idle and the system did not have an outstanding disk I/O request.</td>
</tr>
<tr>
<td>IOwait Percentage</td>
<td>The percentage of time that the CPU or CPUs were idle, during which the system had an outstanding disk I/O request.</td>
</tr>
<tr>
<td>Iq Percentage</td>
<td>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.</td>
</tr>
<tr>
<td>Nice Percentage</td>
<td>The percentage of CPU utilization that occurred while executing at the user level with nice priority.</td>
</tr>
<tr>
<td>Softirq Percentage</td>
<td>The percentage of time that the processor is executing the softirq, which means that task switching is deferred until later to achieve better performance.</td>
</tr>
<tr>
<td>System Percentage</td>
<td>The percentage of CPU utilization that occurred while executing at the system level (kernel).</td>
</tr>
<tr>
<td>User Percentage</td>
<td>The percentage of CPU utilization that occurred while executing at the user level (application).</td>
</tr>
</tbody>
</table>

### Ramfs

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FilesTotal</td>
<td>The total number of files in the ram-based filesystem (ramfs).</td>
</tr>
<tr>
<td>SpaceFree</td>
<td>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.</td>
</tr>
<tr>
<td>SpaceUsed</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Reporting Engine Info

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report (H/RT) CellsRetrieved</td>
<td>Total number of cells (rows times columns) that have been retrieved from all data sources.</td>
</tr>
<tr>
<td>Report (H/RT) Completed</td>
<td>Total number of reports that have been successfully executed.</td>
</tr>
<tr>
<td>Report (H/RT) CompletedInterval</td>
<td>Change of counter Report (H/RT) Completed over the last interval.</td>
</tr>
<tr>
<td>Report (H/RT) Data PreprocessingTimeChart</td>
<td>Total amount of time spent processing report's data to display it in charts.</td>
</tr>
<tr>
<td>Report (H/RT) Data PreprocessingTimeGauge</td>
<td>Total amount of time spent processing report's data to display it in gauges.</td>
</tr>
<tr>
<td>Report (H/RT) Data PreprocessingTimeGrid</td>
<td>Total amount of time spent processing report's data to display it in grids.</td>
</tr>
<tr>
<td>Report (H/RT) DataSetFetch Accepted</td>
<td>The total number of times that a request to fetch a DataSet has been accepted. Not all requests to fetch a DataSet are accepted. If the data for a report is already being fetched, another worker thread is not created to retrieve the same data.</td>
</tr>
<tr>
<td>Report (H/RT) DataSetFetch AcceptedInterval</td>
<td>The interval measure of the above counter.</td>
</tr>
<tr>
<td>Report (H/RT) DataSetFetch Requests</td>
<td>The total number of times that a request to fetch data from a Data Source has been received. This happens every time a report is launched for the first time (in which case, there is also a request to create a new DataSetInfo object), and every time there is a request to refresh a report that has already been launched.</td>
</tr>
<tr>
<td>Report (H/RT) DataSetInfo Created</td>
<td>Out of all the requests for a new DataSetInfo object (Report (H/RT) DataSetInfoRequested),...</td>
</tr>
<tr>
<td>Counter</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Report (H/RT) DataSetInfo CreatedInterval</td>
<td>The interval measure of the Report (H/RT) DataSetInfoCreated counter.</td>
</tr>
<tr>
<td>Report (H/RT) DataSetInfo Requested</td>
<td>The total number of times that a request to create a new DataSetInfo object has been received.</td>
</tr>
<tr>
<td>Report (H/RT) DataSetInfo RequestedInterval</td>
<td>The interval measure of the counter.</td>
</tr>
<tr>
<td>Report (H/RT) DataSetInfo Read</td>
<td>The number of times that a view (grid/gauge/chart) has read the data of a (H/RT) report. This tells how many times the data of reports is being prepared to be displayed to a user (turned into HTML or XML).</td>
</tr>
<tr>
<td>Report (H/RT) DataSetInfo ReadInterval</td>
<td>The interval measurement of the Report (H/RT) DataSetReadTotal counter.</td>
</tr>
<tr>
<td>Report (H/RT) Failed</td>
<td>The total number of reports that have failed. The total number of times that CUIC has tried to fetch data from a Data Source but it has not been able to.</td>
</tr>
<tr>
<td>Counter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Report (H/RT) RenderedChart</td>
<td>Total number of times that the data of a report has been turned into a Chart and sent to a browser (or any other client).</td>
</tr>
<tr>
<td>Report (H/RT) RenderedChart Interval</td>
<td>The interval measurement of the Report (H/RT) RenderedChart counter.</td>
</tr>
<tr>
<td>Report (H/RT) RenderedGauge</td>
<td>Total number of times that the data of a report has been turned into a Gauge and sent to a browser (or any other client).</td>
</tr>
<tr>
<td>Report (H/RT) RenderedGrid</td>
<td>Total number of times that the data of a report has been turned into a Grid and sent to a browser (or any other client).</td>
</tr>
<tr>
<td>Report (H/RT) RenderedRows Retrieved</td>
<td>The total number of rows that have been retrieved by CUIC from data sources.</td>
</tr>
<tr>
<td>Report (H/RT) Running</td>
<td>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.</td>
</tr>
<tr>
<td>Report (H/RT) Runtime</td>
<td>Total amount of seconds spent running running reports.</td>
</tr>
<tr>
<td>Report (H/RT) RuntimeInterval</td>
<td>Change of counter Report (H/RT) Runtime over the last interval.</td>
</tr>
<tr>
<td>Report (H/RT) Runtime DataSourceTime</td>
<td>The number of seconds or milliseconds that CUIC has spent waiting for ICM, or any other database, to return the data of a query. This includes the time from the moment CUIC commits the JDBC query to the moment CUIC gets control back (when the worker thread stops being in an I/O blocked state).</td>
</tr>
<tr>
<td>Subset of Report (H/RT) IRuntime. Amount of time that was spent waiting for data sources to return the report's data.</td>
<td></td>
</tr>
<tr>
<td>Report (H/RT) Runtime DataSourceTimeInterval</td>
<td>The interval measurement of the Report (H/RT) DataSourceTimeTotal counter.</td>
</tr>
</tbody>
</table>
### Counter

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report (H/RT) Waiting</td>
<td>Total number of reports that are currently queued for execution.</td>
</tr>
<tr>
<td>Report (H/RT) Waiting Interval</td>
<td>Change of counter ReportRealtimeWaiting over the last interval.</td>
</tr>
<tr>
<td>ReportsUniqueUsersLoggedinInterval</td>
<td>Total number of unique logged in users over the past interval. Does not count same user who leaves and comes back within the interval.</td>
</tr>
<tr>
<td>ReportsUsersFailedLoginAttempts</td>
<td>Total number of failed login attempts.</td>
</tr>
<tr>
<td>ReportsUsersFailedLoginAttemptsInterval</td>
<td>Change of counter ReportsUsersFailedLoginAttempts over the last interval.</td>
</tr>
<tr>
<td>ReportsUsersLoggedin</td>
<td>Total number of users that are currently logged in</td>
</tr>
</tbody>
</table>

### SchedulerInfo

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SchedulerIntervalLength</td>
<td>How often the scheduler will execute, in seconds.</td>
</tr>
<tr>
<td>SchedulerJobsCompletedCount</td>
<td>The number of jobs that the scheduler service has completed</td>
</tr>
<tr>
<td>SchedulerJobsFailedCount</td>
<td>The number of jobs that the scheduler service has failed to complete successfully.</td>
</tr>
<tr>
<td>SchedulerJobsRunningCount</td>
<td>The number of jobs that the scheduler service is currently running.</td>
</tr>
<tr>
<td>SchedulerState</td>
<td>The current state of the scheduler. The possible values are: 0. - Stopped, 1.- Idle, 2.- Suspended and 3.-Running</td>
</tr>
</tbody>
</table>

### System

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

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocated FDs</td>
<td>Represents the total number of allocated file descriptors.</td>
</tr>
<tr>
<td>Being Used FDs</td>
<td>Represents the number of file descriptors that is currently in use in the system.</td>
</tr>
<tr>
<td>Freed Fds</td>
<td>Represents the total number of allocated file descriptors on the system that is freed.</td>
</tr>
<tr>
<td>IOAwait</td>
<td>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.</td>
</tr>
<tr>
<td>Counter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IOCpuUtil</td>
<td>The percentage of CPU time during which I/O requests were issued to the device</td>
</tr>
<tr>
<td></td>
<td>(bandwidth utilization for the device) on this server.</td>
</tr>
<tr>
<td>IODeviceReqQueueSize</td>
<td>The average queue length of the requests that were issued to all devices on</td>
</tr>
<tr>
<td></td>
<td>this server.</td>
</tr>
<tr>
<td>IODeviceReqSectorSize</td>
<td>The average size in sectors of the requests that were issued to all devices</td>
</tr>
<tr>
<td></td>
<td>on this server.</td>
</tr>
<tr>
<td>IOKBytesReadPerSecond</td>
<td>The total number of KBytes read per second from all devices on this server.</td>
</tr>
<tr>
<td>IOKBytesWrittenPerSecond</td>
<td>The total number of KBytes written per second to all devices on this server.</td>
</tr>
<tr>
<td>IOPerSecond</td>
<td>The total number of input/output operations on all disk partitions per</td>
</tr>
<tr>
<td></td>
<td>second on this server. If you experience a system performance issue, use the</td>
</tr>
<tr>
<td></td>
<td>information in this counter to measure the impact of the aggregate I/O</td>
</tr>
<tr>
<td></td>
<td>operations on this server.</td>
</tr>
<tr>
<td>IOReadReqPerSecond</td>
<td>The total number of read requests per second that were issued to all devices</td>
</tr>
<tr>
<td></td>
<td>on this server.</td>
</tr>
<tr>
<td>IOReadQueueMergedPerSecond</td>
<td>The total number of read requests merged per second that were queued to all</td>
</tr>
<tr>
<td></td>
<td>devices on this server.</td>
</tr>
<tr>
<td>IOSectorsReadPerSecond</td>
<td>The total number of sectors read per second from all devices on this server.</td>
</tr>
<tr>
<td>IOSectorsWrittenPerSecond</td>
<td>The total number of sectors written per second to all devices on this server.</td>
</tr>
<tr>
<td>IOServiceTime</td>
<td>The average service time, in milliseconds, for I/O requests that were issued</td>
</tr>
<tr>
<td></td>
<td>to all devices on this server.</td>
</tr>
<tr>
<td>IOWriteReqPerSecond</td>
<td>The total number of write requests per second that were issued to all devices</td>
</tr>
<tr>
<td></td>
<td>on this server.</td>
</tr>
<tr>
<td>IOWriteReqQueueMergedPerSecond</td>
<td>The total number of write requests merged per second that were queued to</td>
</tr>
<tr>
<td></td>
<td>all devices on this server.</td>
</tr>
<tr>
<td>Max Fds</td>
<td>Represents the maximum number of file descriptors that is allowed on the</td>
</tr>
<tr>
<td></td>
<td>system.</td>
</tr>
<tr>
<td>Total CPU Time</td>
<td>Represents the total time, measured in jiffies, that the system has been</td>
</tr>
<tr>
<td></td>
<td>up and running. A jiffy corresponds to a unit of CPU time and gets used as a</td>
</tr>
<tr>
<td></td>
<td>base of measurement. One second is equal to 100 jiffies.</td>
</tr>
<tr>
<td>Total Processes</td>
<td>Represents the total number of processes on the system.</td>
</tr>
<tr>
<td>Total Threads</td>
<td>Represents the total number of threads on the system.</td>
</tr>
</tbody>
</table>
### TCP

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

### Thread

<table>
<thead>
<tr>
<th><strong>Counter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>% CPU Time</td>
<td>The thread's share of the elapsed CPU time since the last update, expressed as a percentage of total CPU time.</td>
</tr>
<tr>
<td>PID</td>
<td>The thread's leader process ID.</td>
</tr>
</tbody>
</table>
Chapter 8

Accessing Cisco Unified Communications Solutions Tools from Unified IC

The Navigation dropdown menu at the top right of the Unified IC Administration page has three Cisco Unified Communications Solutions tools:

Figure 15: Navigation dropdown

To sign in to these tools, use the user name and password for the Installation Administrator account.

To access these tools from a Member node, where x.x.x.x is the IP address of the member:

- To access Unified Serviceability: http://x.x.x.x/ccmservice/
- To access Unified OS Administration: http://x.x.x.x/cmplatform
- To access Disaster Recovery System: http://x.x.x.x/drf

This chapter contains the following topics:
Cisco Unified Serviceability

Cisco Unified Serviceability is one of three system-level tools that Unified IC shares with Cisco Unified Communications Solutions. The other two are Disaster Recovery System (page 81) and Cisco Unified OS Administration (page 81).

To access Cisco Unified Serviceability, select it from the Navigation dropdown in the upper-right corner and click Go.

Cisco Unified Serviceability is a web-based troubleshooting tool, with four menus (Alarms, Trace, Tools, and SNMP). Unified Serviceability features are supported by and applicable to Unified IC with exceptions noted in Unified IC Notations.

Cisco Unified Serviceability features include the following:

- Provides information on configuring alarms, traces, and SNMP
- Saves alarms and events for troubleshooting and provides alarm message definitions.
- Saves trace information to various log files for troubleshooting.
- Monitors real-time behavior of components through the Cisco Unified Real-Time Monitoring Tool (RTMT).
- Provides feature services that you can activate, deactivate, and view through the Service Activation window.
- Provides an interface for starting and stopping feature and network services.
- Generates and archives daily reports; for example, alert summary or server statistic reports.
- Allows Cisco Unified Communications Manager and Cisco Unity Connection to work as a managed device for SNMP remote management and troubleshooting.
- Monitors the disk usage of the log partition on a server.
- Monitors the number of threads and processes in the system; uses cache to enhance the performance.

All information in the Cisco Unified Serviceability documentation is applicable to Unified Intelligence system.
Cisco Unified OS Administration

Cisco Unified OS Administration is one of three system-level tools that Unified IC shares with Cisco Unified Communications Solutions. The other two are Disaster Recovery System (page 81) and Cisco Unified Serviceability (page 80).

To access Cisco Unified OS Administration select it from the Navigation dropdown in the upper-right corner and click Go.

Use Cisco Unified OS Administration to perform many common system administration functions. Unified OS Administration menus are the following:

- **Show**: How to view information on Cluster Nodes, Hardware Status, Network Configuration, Installed Software, System Status, and IP Preferences.
- **Settings**: How to display and change IP settings, host settings, and Network Time Protocol (NTP) settings.
- **Security**: How to manage certificates and how to set up and manage IPSec policies
- **Software Upgrades**: How to perform an upgrade and how to revert to a previous version.
- **Services**: How to use the Ping and Remote Support features

Disaster Recovery System

The Disaster Recovery System (DRS) is one of three system-level tools that Unified IC shares with Cisco Unified Communications Solutions. The other two are Cisco Unified OS Administration (page 81) and Cisco Unified Serviceability (page 80).

To access Disaster Recovery System, select it from the Navigation dropdown in the upper-right corner and click Go. You can also enter this URL from any node in the cluster: https://x.x.x.x:8443/drf where x.x.x.x is the IP address of the node. Sign in using the System Administrator credentials.

The Disaster Recovery System provides backup and restore capability for all servers in a Unified IC cluster and allows you to perform regularly-scheduled automatic backups as well as user-invoked data backups.

Refer to the DRS online help for topics including:

- Backup and Restore procedures
- Creating and editing backup schedules
- Starting a manual backup
Disaster Recovery System

- Restoring a backup version and viewing restore status
- Restoring a cluster
- Error messages that can occur during a backup or a restore

All information in the DRS online help is applicable to Unified Intelligence system. See the topics below for DRS-related information that pertains to Unified IC.

Databases Installed with Unified IC Cluster

The Informix Dynamic Server (IDS) is installed on all nodes in the cluster. The installation creates two databases on each node:

- The Unified IC database (CUIC).
  
  This database holds tables for reports, report definition, users, and other records integral to the reporting functionality.
  
  This database appears on the Data Sources page in the Unified IC Reporting interface.

- The UCCE database.
  
  This is the database that populates the stock templates.
  
  This database appears on the Data Sources page in the Unified IC Reporting interface. It is partially configured. You need to complete information for the IP address, user name, and password.

- The System database (ccm_data).
  
  This database is the standard Cisco Call Manager database that is modified for the Unified IC.
  
  The system database is not listed on the Data Source tab in the Unified IC Reporting interface.

These databases are not documented and are not directly accessible for review and management in the Cisco Unified Operating System.

From both a platform and application point of view, data is replicated between the nodes using Informix replication services.

You can use the Command Line Interface to perform certain actions and to view database tables and properties. These commands include `run sql`, various `show tech` commands, the `utils dbreplication` and `utils purge` commands.
Database Replication

Replication of the CUIC database (the maintenance and synchronization of multiple copies of the cuicdatabase (CUIC) across servers) is essential for the Unified IC cluster.

Unified IC uses the update-anywhere enterprise replication model based on a topology of Fully Connected Database servers. Each database server has connection to all other database servers. Data can be transferred from any machine to all others.

Data is replicated immediately - as soon as changes are made. Changes that are apparent in the User Interface (such as the addition or deletion of a dashboard or a change to a report definition) are evident across all devices when the page is refreshed, provided that all devices in the cluster have all the required network connections and CPU power to do all processing.

Conflict resolution (for example, when one user is deleting an object that another user is updating) is handled on a last-update-wins basis.

Backup

You can perform a manual or a scheduled backup on a configured backup device using the Backup menu in the Disaster Recovery System application.

A backup device is logical mapping to a tape or a remote (NFS) location. Each backup device can store up to 14 backups.

You can back up all or some nodes in the cluster. The Controller node must be running for any backup to take place. Any Member nodes that are to be backed up must also be running.

Although you can run a backup and continue operations, it is best to back up at off-peak times.
The following are backed up:

- CUIC and System databases
- Unified IC configuration and properties files
- Encryption files
- License files
- Platform config files
- SNMP Syslog component and CDP subagent
- Trace Collection tool
- Cluster Manager (CLM)

**Restore**

You perform a restore using the Restore menu in the Disaster Recovery System application. Select the backup device from which you need to restore, and from that device select the timestamped backup you want.

When you restore, the node must be shut down. After the successful restore, reboot the node or cluster. The database will be online once the restore completes and the node is started. Replication begins automatically.

The Disaster Recovery System supports the following restore scenarios:

- Restoring the entire cluster.
- Restoring the cluster or a node to the last known good configuration
- Restoring the publisher (controller) node only
- Restoring the subscriber (member) nodes only

**Data Purge**

Data is purged automatically once a day on all nodes in the cluster. The purge runs at midnight 12.00 AM and uses the timezone setting of VOS machine. The Daylight Savings time change has no impact on data purge.

The Daylight Savings time change has no impact on data purge.

You can also run a purge manually using the `utils purge` (page 146) command.

The following tables are purged from the cuic database when the Purge utility run:
• CuicDataSetInfo
• CuicDataSet
• CuicReportDefinitionFilter
• CuicReportDefinitionFilterField
• CuicReportDefinitionFilterParameter
• CuicCollection
• CuicCollectionValue

Purging these tables removes:
• Filters as follows:
  – Filters that are not used by active DataSetInfo
  – Filters that are not default filters of any report.
  – Filter that are not Filters of any drilldown

  **Note:** Deleting a filter cascades to the filter fields, filter parameters, collections used by the filter fields/parameters, and collection values used by the collections deleted.

• Any nonactive DataSets

  **Warning:** Database tables are locked during the purge and are unlocked when the purge completes. Any other processes that are running at the same time as the purge will fail.

**Restoring and Rebuilding when the First Node Goes Down**

If the publisher node is down for any reason, and the subscribers are running normally while the publisher is down, the data mismatch is corrected automatically when the publisher is back in operation.

Once the publisher is running, a merge process synchronizes the data so that data that has been *inserted* in the subscribers while the publisher was offline is replicated to the publisher.

If rows were *deleted* in a subscriber while the publisher was down, the publisher will merge those rows back into the subscriber database. You will need to redefine them.
Chapter 9

The Administration Console Interface

This chapter contains the following topics:

- Drawers, page 87
- Filter, page 88
- Online Help, page 88
- Sorting, page 88
- Title Bar, page 89
- Licenses, page 89
- Users in the Administration Console, page 91

Drawers

The left panel of the Administration interface contains *drawers*.

Drawers are similar to menus: they group logically-related functions. Clicking (opening) a drawer in the left panel might immediately open a page in the right panel or it might expand to show a list or tree of nested links.

*Figure 17: Drawers in the Administration Console*
Filter

Many pages let you filter items to limit the number of results that appear in a given list. You can also filter items to find a specific item or a subset of items with similar values.

Note: Quickly clear a filter by clicking the Clear Filter button.

Online Help

There is a Help icon on each page.

Clicking Help opens a new window with a topic relevant to the window you are on.

From a help topic, click the Navigation icon

*Figure 18: Online Help Navigation Icon*

This opens the Table of Contents and exposes the help functions such as Index and Search.

*Figure 19: Online Help*

Sorting

Any page that contains lists of items can be sorted by any field name. To sort a list of items:

**Step 1**  
Click the name of the field on the top of the column that you want to sort.

The listed is sorted in ascending order for that column.

**Step 2**  
Click the name of the field again to sort the list in descending order.
Step 3
Click any other field name at the top of the column to sort on that column.

Title Bar

The title bar is visible from each window and has the following:

• A Cisco Systems logo that links to http://www.cisco.com/.

• A Navigation dropdown, where you can open Disaster Recovery System, Cisco Unified OS Administration, and Cisco Unified Serviceability.

• A Log Out link.

• The About link.

Licenses

Unified IC licenses are "node-locked." This means a license is physically located on the Controller node and is distributed to all members nodes in the cluster through database replication.

There can be only one license installed on a system at any point in time.

Uploading the license file is the first action the Super User must take after installing the Controller node.

After installation, until the Super User obtains and uploads a Standard or Premium license, he or she:

• Can sign in to the Operations Console to view the Controller and to add the alias name.

• Cannot perform other Operations Console functions.

• Cannot sign in to the Unified IC Reporting application.

• Cannot install member nodes.

How To Obtain Your License

To acquire a license:

1. Go to the Cisco Product License Registration website at this URL: https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet

2. If you do not have a PAK, click the available licenses link (https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?DemoKeys=Y).
3. Scroll to Voice Products and click **Cisco Unified Intelligence Center - v8.0**.

4. Enter your MACAddress, accept the agreement, and enter your Registrant Information.

5. Follow prompts to complete the registration pages.

You will receive the license file in an email from Cisco Systems. When you receive it, save it locally in a location where it cannot be deleted by mistake or opened by an unauthorized person. In the event that your system becomes corrupted, you can browse to this location to upload the license file again.

The same license file will be valid if you need to reapply it - unless you apply it to a new server with a new MAC address.

**Caution: License files are human-readable and can be opened. However, changing any text in the license file invalidates the license.**

### License Types

Unified Intelligence Suite has four license types: Demo, Lab/Trial, Standard, and Premium.

<table>
<thead>
<tr>
<th>TYPE</th>
<th>EXPIRATION</th>
<th>NODES</th>
<th>USERS</th>
<th>FEATURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEMO</td>
<td>Valid for 90 days and contains an expiration date. Can be extended for one additional 90-day session with a reinstallaion of Unified IC.</td>
<td>Controller and all Member nodes (a maximum of 8 nodes).</td>
<td>No limit</td>
<td>Premium feature set</td>
</tr>
<tr>
<td>LAB/TRIAL</td>
<td>Has no expiration/timeout.</td>
<td>Controller node only</td>
<td>Five users</td>
<td>Premium feature set</td>
</tr>
<tr>
<td>STANDARD</td>
<td>Has no expiration/timeout.</td>
<td>Controller and all Member nodes (a maximum of 8 nodes).</td>
<td>Unlimited but requires system sizing for optimum performance. See the Sizing Tool for guidelines.</td>
<td>Standard feature set</td>
</tr>
<tr>
<td>PREMIUM</td>
<td>Has no expiration/timeout.</td>
<td>Controller and all Member nodes (a maximum of 8 nodes).</td>
<td>Unlimited but requires system sizing for optimum performance. See the Sizing Tool for guidelines.</td>
<td>Premium feature set</td>
</tr>
</tbody>
</table>
Users in the Administration Console

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

- **Super Users** (page 91)
- **System Application User** (page 91)
- **System Administration User** (page 92)

**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** (page 91) who is configured during installation.

The initial Super User (the System Application User) can sign in to the Unified IC Reporting console and has *all User Roles* and *full permissions* for all drawers in Unified IC 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 IC Reporting and are considered to be IMS users. They have the limited Login User role only until the Unified IC Reporting security administrator gives them additional roles and flags them as Active users.

**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, it is a best practice to 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 IC.

This user has full rights to all functions in the Administration and Unified IC 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 sign in to Unified IC and has full rights to all functions in Unified IC.
- Is the initial Security Administrator user in the Unified IC reporting application
Can create additional Security Administrator users in the Unified IC reporting application.

Cannot have any role taken away from him.

Cannot take any role away from himself.

This user can log in to the Reporting application and is the initial System Administration User.

The System Administrator account User ID and password are configured at installation for each node. It is a best practice to 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 dropdown 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 IC reporting application.

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

Certain CLI commands are useful for specific inquiries.

**Basic system commands:**

- `utils system restart` (page 150)
- `utils system shutdown` (page 150)
- `utils system switch-version` (page 151)
- `utils system upgrade` (page 151)
- `set network` (page 106) (`dns / dhcp / hostname / mtu / cluster`)
- `set password` (page 110)
- `show status` (page 127)

**Disk and Backup:**

- `utils disaster recovery_backup` (page 140)
- `utils disk raid maintenance` (page 147)
- `show diskusage` (page 118)

**Hardware Information:**

- `show hardware` (page 118)
- `show memory` (page 119)
- `show ups status` (page 134)
- `show environment` (page 118)
- `utils create report hardware` (page 137)
- `show tech system` (page 132)

**Performance:**

- `show status` (page 127)
- `show process using-most cpu/memory` (page 126)
- shows stats io (page 127)
- utils iostat (page 143)
- show perf (page 123)
- utils service start (page 148)

**Platform:**
- show process list (page 125)
- show open files (page 121)
- show open ports (page 122)
- show timezone (page 133)
- utils core analyze (page 137)
- utils create report platform (page 137)
- show version (page 134)

**Network Utilities:**
- set network (page 106)
- utils network ping (page 145)
- utils firewall (page 142)
- show tech network (page 130)

**Security**
- set account (page 103)
- show logins (page 119)
- show web-security (page 134)
- show cert list (page 116)
- utils auditd (page 136)
- utils csa (page 137)
- utils firewall (page 142)
Delete Commands

Unified IC:

• show packages active cuic (page 122)
• show cuic properties (page 116)
• set cuic properties (page 105)
• show cuic-license-info (page 117)
• set trace (page 112)
• show trace (page 133)
• show perf (page 123)

Unified IC Database:

• run sql (page 102)
• show tech (page 128)
• utils dbreplication (page 138)

Delete Commands

• delete account (page 96)
• delete dns (page 97)
• delete ipsec (page 97)
• delete process (page 97)
• delete smtp (page 97)

delete account

This command allows you to delete an administrator account.

COMMAND: 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: 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 policy with a given policy name and group.

COMMANDS:

delete ipsec policy_group  {group | all} Use to delete all policies within a group or to delete all groups.

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: 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.
File Commands

- file check (page 98)
- file delete (page 98)
- file dump (page 99)
- file get (page 99)
- file list (page 100)
- file search (page 100)
- file tail (page 101)
- file view (page 101)

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: **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.

COMMANDS:

- **file delete activelog** file-spec [options]
- **file delete inactivelog** file-spec [options]
- **file delete install** file-spec [options]
- **file delete license** file-name [options]

PARAMETERS:
File Commands

file-spec specifies the path and filename of the file(s) to delete.

file-name specifies the name of the license file 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.

COMMANDS:

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.

COMMANDS:

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.

COMMANDS:

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]

file list sftpdetails 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.

COMMANDS:
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.

COMMANDS:

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.

COMMANDS:

file view activelog  file-spec
Run Commands

- **run loadxml (page 102)**
- **run sql (page 102)**

**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:** `run loadxml`

**run sql**

This runs a SQL command to query and select from the database and table.

**COMMAND:** `run 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 IC 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`.

Set Commands

- **set account (page 103)**
• set accountlocking (page 103)
• set cert (page 104)
• set cli (page 104)
• set commandcount (page 104)
• set cuic-properties (page 105)
• set ipsec (page 105)
• set logging (page 106)
• set network (page 106)
• set password (page 110)
• set smtp (page 112)
• set syslog (page 112)
• set timezone (page 112)
• set trace (page 112)
• set web-security (page 114)
• set workingdir (page 114)

set account

COMMANDS:

```plaintext
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.

```plaintext
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: `set accountlocking enable | disable | unlocktime`
PARAMETER *enable* enables account locking.

PARAMETER *disable* disables account locking.

PARAMETER *unlocktime* Use this command 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 (page 116).*

**COMMANDS:**

*set cert bulk  unit | all* 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.

*set cert export  unit | all* 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.

*set cert import  unit | all* 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.

*set cert regen  unit name* This command regenerates the certificate for the unit name and prompt for a restart to activate the regenerated certificate.

*set cert sftp* This command prompts for the SFTP IP address, server port, User ID, password, and remote directory information to be used for Bulk operations.

**PARAMETERS:**

*unit* and *unit name* specifies the name of the unit.

**set cli**

Run this command to set the pagination of the current CLI session.

**COMMAND:** *set cli pagination name*

PARAMETER *on or off*

**set commandcount**

These commands change the CLI command prompt, so it displays or hides the number of CLI commands executed in the current session.

**COMMANDS:**

*set commandcount enable*
set commandcount disable

set cuic-properties

Use these commands to set values for the cuic database and session timeout.

COMMANDS:

set cuic-properties host-to-ip

PARAMETER <host> <ip-address>

This command sets the host-to-ip translation and is used when there is a need to configure and IP address for one of the UCCE Databases that is unique to the member node from which you are running the command. This command allows for scalability and overrides the default Historical or Realtime 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.

For <ip-address>, enter the IP address of the server for the Historical or Realtime database.

set cuic-properties purge-time

PARAMETER HH:MM AM or PM

This command sets the time of day when the cuic database will be purged. The default is 12:00 AM.

set cuic-properties purge-retention

PARAMETER #number of days

This command sets the number of day(s) that data in the cuic database is retained before it gets purged. The default is one day.

set cuic-properties session-timeout

PARAMETER #numberofSeconds

This command sets the Session Timeout for the Unified IC Reporting web application. The default is 14,400 seconds (4 hours).

set ipsec

Use these commands to enable ipsec policies.

COMMAND: set ipsec policy_group [group | all] Use to enable all policies within a group or all groups.
COMMAND: `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.

**COMMANDS:**

- `set logging enable`
- `set logging disable`

**set network**

**set network cluster publisher**

*Caution: These commands are not supported for Unified IC.*

- `set network cluster publisher hostname` This command configures the cluster publisher hostname and cause a temporary loss of network connectivity while the network is restarted with the new configuration.
- `set network cluster publisher ip` This command configures the cluster publisher ip address and cause 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 executed, causes the system to restart.

**COMMANDS:**

- `set network dhcp eth0 enable`
- `set network dhcp eth0 disable`

**set network dns options**

This command allows you to set the dns options.

**COMMAND: 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 executed, causes a loss of network connectivity.

**COMMANDS:**

```
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 executed, causes a loss of network connectivity.

**COMMAND:** `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 executed, causes the system to restart.

**COMMANDS:**

```
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 executed, causes the system to restart.

**COMMAND:** `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 hyphen in between. The hostname must be 63 characters or less.

COMMAND: `set network hostname [name] addr`

PARAMETER `name` specifies the network hostname.

set network ip eth0

**Caution: This command is not supported for Unified IC.**

This command sets the IP address for Ethernet interface 0.

The system asks whether you want to continue to execute this command. If you continue, this command causes the system to restart.

COMMAND: `set network ip eth0 <addr> <mask>`

PARAMETERS:

- `addr` is the IP address.
- `mask` is the mask.

set network ipv6

These commands are used for configuring the IPv6 feature on the machine.

COMMANDS:

- `set network ip dhcp action reboot` This command is used for enabling or disabling the DHCPv6 client.
- `set network ip service action reboot reboot` This command is used for enabling or disabling the IPv6 feature client.
- `set network ipv6 static_address addr mask` This command is used for setting the static IPv6 address on the server.

PARAMETERS:

- `Action` is mandatory and 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_connntrack_max.

COMMAND: set network max_ip_conntrack ip_connntrack_max

PARAMETER ip_connntrack_max indicates the maximum value

set network mtu

This command sets the maximum MTU value. The valid range is 500-1500.

COMMAND: 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: set network nic eth0 auto [en | dis] speed [10 | 100] duplex [half | full]

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 execute this command. If you continue, the system temporarily loses network connectivity.

COMMAND: set network pmtud state {enable | disable}

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: 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: set network status eth0 state {up | down}

PARAMETER state {up | down} to set the status up or down is required.

set password

Use these commands to configure password rules.

COMMANDS:

set password age maximum | days minimum | days

set password complexity character minimum-length
Use this commands to enable or disable password complexity rules.

**set password expiry** `maximum-age` `minimum-age`

**set password history** `number`

**set password inactivity** `enable` | `disable` | `period (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.

**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 only 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 CUCM 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** Use this command to set 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** Use this command to set 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 \(enable \mid disable\)

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: set smtp host

PARAMETER host indicates the hostname for the smtp server.

set syslog

This command set the syslog as enabled or disabled.

COMMAND: set syslog enable \mid disable

set timezone

This command changes or sets the timezone. You must restart the system after you change the timezone.

COMMAND: 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 (page 133) command.

Be aware that the timezone name is case-sensitive.

set trace

Use these commands to set or change the log levels and trace setting for the subsystems of two server processes (cuicserver and oampserver) to basic or detailed.

COMMAND:

\text{set trace basic} cuicserver \{subsystem\} none

\text{set trace basic} oampserver \{subsystem\} none
set trace infrastructure cuicserver [subsystem] [TRACE_FLAGS | none]

set trace infrastructure oampserver [subsystem] [TRACE_FLAGS | none]

set trace subsystem cuicserver [subsystem] [trace_mask1 trace_mask2]

set trace subsystem oampserver [subsystem] [trace_mask1 trace_mask2]

For cuicserver, the valid subsystems are:

- Infrastructure
- CUIC
- CUIC_MODEL_OBJECTS
- CUIC_DATA_PROCESSING
- CUIC_SECURITY
- CUIC_DISPLAY
- CUIC_MIGRATION
- CUIC_USER_HISTORY
- CUIC_JSP
- CUIC_STATISTICS

For oampserver, the valid subsystems are:

- Infrastructure
- OAMP_BO
- OAMP
- WSM_BO

Detailed log levels are set by enabling trace flags, which allows debug statements to appear in the logs. You can control debug tracing for specific functionalities (specified in the TRACE flag name), within specific subsystem components. See Infrastructure Trace Definitions (page 22).

basic indicates to set a basic level of tracing. With this setting, messages and warnings are displayed.

detailed indicates to set a debug level and allows you to turn on tracing for specific components.

subsystem indicates the subsystem you are setting and displays the list of all valid subsystems.
none indicates that you do not want to set a flag for tracing

set web-security

This command sets the web security certificate information for the operating system.

COMMAND: set web-security  <orgunit> <orgname> <locality> <state> <country>

PARAMETERS: (All five 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.

set workingdir

These commands set the CLI working directory for activelog or inactivelog.

COMMANDS:

set workingdir activelog directory

set workingdir inactivelog directory

PARAMETER directory must be a valid sub-directory of the activelog or inactivelog.

Show Commands

- show account (page 115)
- show accountlocking (page 116)
- show cert (page 116)
- show cli (page 116)
- show cuic-properties (page 116)
- show cuis-component-status (page 117)
- show cuis-license-info (page 117)
- show diskusage (page 118)
show account

This command lists all accounts except the master admin account.
COMMAND: **show account**

**show accountlocking**

This command shows the current account locking settings.

COMMAND: **show accountlocking**

**show cert**

These commands show certificate information about the selected certificate type.

COMMANDS:

**show cert list type**

PARAMETER *type* is mandatory 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: **show cli pagination**

**show cuic-properties**

These commands show information about cuic properties.

COMMANDS:

**show cuic-properties purge-retention**

This command shows the number of day(s) that data in the cuic database is retained before it gets purged

**show cuic-properties purge-time**

This command shows the time of day when the cuic database will be purged

**show cuic-properties session-timeout**

This command shows the Session Timeout for cuic web application.
show cuic-properties host-to-ip

This command shows the current host-to-ip translation for CUIC databases in the cluster.

show cuis-component-status

These commands show the status of the Unified IC components.

COMMANDS:

show cuis-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.

[ICMUserStatus] shows the status of Unified ICM user integration.

[EmailStatus] shows status of the emailer component.

[SchedulerStatus] shows status of the report scheduler.

[DataSourceConnectionStatus] shows data source connection status.

show cuis-license-info

This command shows information about the license that the cluster is using.

• License Type: standard; premium; demo or trial

• Node Count: the number of licensed nodes in the cluster. If not provided, the default value (8) is assumed.

• User Count: the number of simultaneous reporting users allowed. If omitted in the license file, the default is assumed, which is no limit.

• Start Date: The date from which the license is valid.

• Expiry Date: Shows "permanent" or a specific expiry date

See License File Management (page 34).
show diskusage

These commands show disk usage of the given directory as well as the usage of the disk partition the directory exists on.

COMMANDS:

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 name] 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.

COMMANDS:

show environment fans
show environment power-supply
show environment temperatures

show hardware

This command retrieves some basic platform hardware information.

COMMAND: show hardware
show ipsec

Use these commands to display ipsec policies.

COMMANDS: `show ipsec information [policy_group] [policy-name]` Use to display detailed information about the specified ipsec policy.

`show ipsec policy_group` Use to display the list of ipsec policy names with specified policy group.

`show ipsec policy_name` Use to view a policy with a given policy name and group. Example: `set ipsec policy_name group1 name1`

`show ipsec status` Use to display the status of all ipsec tunnels defined in the system.

show logins

This command show the last number of platform admin logins. The default is to show 20 logins.

COMMAND: `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.

COMMANDS:

`show memory count`

`show memory module module number`

`show memory module ALL`

`show memory size`

show myself

This command show information about the current account: machine name, account name, admin privilege level, output setting and logging setting. Use the commands `set commandcount (page 104)` and `set logging (page 106)` to modify current account settings.

COMMAND: `show myself`
show network

show network all

This command retrieves all basic platform network information.

COMMAND: **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: **show network all**

show network dhcp eth0 status

This command displays the DHCP status on eth0.

COMMAND: **show network dhcp eth0 status** [options]

show network failover

This command shows network fault tolerance information.

COMMAND: **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: **show network ip_conntrack** [options]
show network max_ip_conntrack

This command retrieves ip_conntrack_max information.

COMMAND: show network all

show network route

This command retrieves some basic platform network route information.

COMMAND: 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: 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.

COMMANDS:

show open files all
This command displays all the open files on the machine.

**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 processed.

**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.

COMMANDS:

**show open ports all**

This command shows all open ports.

**show open ports regex** "*string*"

This command shows displays 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.

COMMANDS:

**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.

COMMANDS:

`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.

`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.

`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: `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.

COMMANDS:

`show perf list categories`

This command lists all categories in the perfmon system.
**show perf list classes** [options]

This command lists perfmon classes.

**show perf list counters** *class-name* [options]

This command lists perfmon counters in a particular perfmon class.

**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.

COMMANDS:

**show perf query class** *class-name*

This command queries the perfmon class to show all instances and counter values of each instance.

Most Unified IC counters display with this command. For example *show perf query class SchedulerInfo* shows the the SchedulerIntervalLength, SchedulerJobsCompletedCount, SchedulerJobsFailedCount, SchedulerJobsRunningCount, and SchedulerState.

**show perf query counter** *class-name* <counter-name, counter-name...>

This command queries a counter to show the counter value of all instances.

**show perf query instance** <class-name> <instance-name, instance-name...>

This command queries an instance to show its all counter values.

**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: 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 "num" number of processes using the most cpu or memory or time.

COMMAND: 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
[threads] - 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

The command is used get the details of processes that share the same name. This also displays parent-child relationship.

**COMMAND:** `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:** `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:** `show process search regexp [file]`

**PARAMETER** `regexp` specifies the regular expression.

**OPTION** `[file]` is the file-name for the output.

### show process using-most

These commands show the processes using the most cpu or the most memory.

**COMMANDS:**

- `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: **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: **show smtp**

show stats io

This command shows system I/o stats of the machine.

COMMAND: **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 some basic platform status.

COMMAND: **show status**
show subsys

These commands show subsystem information.

COMMANDS:

This command displays all the subsystems present on the server.

show subsys trace all subsystem

This command displays the trace masks for the given subsystem.

PARAMETER subsystem must be a valid subsystem name.

show tech

show tech activesql

This command shows the active queries to the database taken in the last one minute.

COMMAND: 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: show tech all [options]

OPTIONS:

[page] displays one line at a time.

[file fname] outputs to a file to saved in platform/cli/fname.txt.

show tech cuic

These commands display information about the Unified IC database.

COMMAND: show tech cuic procedures

This command shows the procedures in use for the Unified IC database.

COMMAND: show tech cuic systables

This command displays the name of all tables in the Unified IC database.

COMMAND: show tech cuic table <tablename>
This command shows the contents of a table on the Unified IC database.

PARAMETER `tablename` is mandatory and must be the name a table in the Unified IC database

COMMAND: **show tech cuic triggers**

This command displays Unified IC table names and the triggers associated with those tables.

**show tech database**

These commands show database information.

COMMANDS:

**show tech database dump [options]**

This command dumps the database so that you can sent 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 IC database

**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: **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: **show tech dbintegrity**

**show tech dbinuse**

This command displays the database in use.

COMMAND: **show tech dbinuse**
show tech dbschema

This command displays the database schema in a CSV file.

COMMAND: show 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 IC database

show tech dbstateinfo

This command shows the database state information and outputs it to a file.

COMMAND: show tech dbstateinfo

show tech dumpCSVandXML

This command collects csv and xml files into a single tar file.

COMMAND: show tech dumpCSVandXML

show tech network

These commands shows network aspects of the system.

COMMANDS:

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: 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.

COMMANDS:

show tech params all  shows all parameters.

show tech params enterprise shows enterprise parameters.

show tech params service  shows service parameters.

show tech procedures

This command displays the stored procedures in use for the database.

COMMAND: show 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 IC database

show tech repltimeout

This command shows the replication timeout setting.

COMMAND: 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: show tech sqlhistory
show tech systables

This command displays the name of all tables in the database.

COMMAND: show 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 IC database

show tech system

These commands show various aspects of the system.

COMMANDS:

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 to saved in platform/cli/fname.txt.

show tech table

This command redirects the contents of the specified database table into a file.

COMMAND: show 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 \texttt{cuic} option, this command shows only tables in the operating system database.

[cuic] - Unified IC database

This example shows the cuicversion table from the cuic database: \texttt{show tech table cuicversion cuic}.

\texttt{show tech triggers}

This command displays table names and triggers associated with those tables.

\textbf{COMMAND:} \texttt{show tech triggers [options]}

\textbf{OPTIONS:}

[ccm] - operating system database. This is the default. If you do not include the \texttt{cuic} option, this command shows the table name and triggers associated with the operating system database.

[cuic] - Unified IC database

\texttt{show tech version}

This command displays the version of all RPMs (RedHat Package Manager) installed on the system.

\textbf{COMMAND:} \texttt{show tech version}

\texttt{show timezone}

These commands display the currently-configured timezone or list of all zones.

\textbf{COMMANDS:}

\texttt{show timezone config} shows the timezone currently set for the server.

\texttt{show timezone list} displays a list of all timezones.

See also \texttt{set timezone (page 112)}.

\texttt{show trace}

This command show the log level and trace masks of the given subsystem. If the logging level is set to DEBUG, displays the tracemask. If the logging level is set to INFO, no tracemasks display.

\textbf{Note:}

- This command is case-sensitive.
• This CLI command can only be run on the Controller node. To set traces on the Member nodes you must use the Operations Console command **Device Management > Log And Trace Settings**

**COMMANDS:**

**show trace** `<cuicserver> <oampserver>`

**PARAMETER:** *CUIC*

**PARAMETER:** *INFRASTRUCTURE*

Options: Subsystems: OAMP| OAMP_BO | Infrastructure | WSM_BO

**show ups status**

This command communicates with an attached Uninterruptible Power Supply and displays status.

**COMMAND:** `show ups status`

**show version**

This command displays the software version on the active or inactive side.

**COMMAND:** `show version [active | inactive]`

The indicator to the **active** or **inactive** partition is required.

**show web-security**

This command displays web security information.

**COMMAND:** `show web-security`

**show workingdir**

**COMMAND:** `show workingdir`

This command displays the current working directories for the activelog and inactivelog.

**Unset Command**

• *unset cuic-properties* (page 135)

• *unset ipsec* (page 135)
• unset network dns (page 135)

unset cuic-properties

Use this command to unset the translation of host-to-ip

COMMAND: unset cuic-properties host-to-ip hostname

unset ipsec

Use these commands to disable ipsec policies.

COMMAND: unset ipsec policy_group [group | all] Use to disable all policies within a group or all groups.

COMMAND: unset ipsec policy_name [policy_group] [policy_name] Use to disable a policy with a given policy name and group. Example: set ipsec policy_name group1 name1

unset network dns

COMMANDS:

unset network dns options [options] This command unsets DNS options and will cause 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.

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 configuration that were defined with the command set cuic-properties host-to-ip (page 105)

Running this command removes the node-specific override for the IP address of the UCCE databases and reverts to the default for the UCCE databases as configured in the Data Sources page.
COMMAND: unset_host-to-ip

Utils Commands

- utils audid (page 136)
- utils core (page 137)
- utils create report (page 137)
- utils csa (page 137)
- utils dbreplication (page 138)
- utils diagnose (page 140)
- utils disaster recovery (page 140)
- utils firewall (page 142)
- utils iostat (page 143)
- utils iothrottle (page 143)
- utils netdump (page 143)
- utils network (page 144)
- utils ntp (page 146)
- utils purge (page 146)
- utils raid (page 147)
- utils remote_account (page 147)
- utils reset (page 147)
- utils service (page 148)
- utils snmp (page 149)
- utils soap (page 150)
- utils system (page 150)

utils audid

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

**COMMANDS:**

- `utils auditd disable`
- `utils auditd enable`
- `utils auditd status`

**utils core**

These commands display information for core files.

**COMMANDS:**

- `utils core analyze core_file_name`
  
  This command displays backtrace for the specified core file.

  **PARAMETER** `core_file_name`.

- `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.

**COMMANDS:**

- `utils create report hardware`
- `utils create report platform`

**utils csa**

These commands enable, disable, or show the status of Cisco Security Agent.

**COMMANDS:**
utils csa enable
utils csa disable
utils csa status

utils dbreplication

utils dbreplication clusterreset HARI

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: `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: `utils dbreplication dropadmindb`

utils dbreplication repair

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

COMMANDS:
`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 execute `utils dbreplication stop`. If resetting all, stop replication on all nodes first. If resetting `<nodename>`, stop replication on that node first.
COMMAND: `utils dbreplication reset all`

COMMAND: `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.

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

COMMAND: `utils dbreplication runtimestate [nodename]`

`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: `utils dbreplication setrepltimeout integer 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: `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 execute the stop operation on the local node only.

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

COMMAND: `utils dbreplication stop all`

COMMAND: `utils dbreplication stop nodename`
**utils diagnose**

Use these commands for various diagnostic functions.

**COMMANDS:**

**utils diagnose fix**

This command runs diagnostic tests, displays the results, and if possible, attempt to repair the system.

**utils diagnose list**

This command lists all available diagnostic commands.

**utils diagnose module module name**

This command executes a test on a named module test and attempts to fix the problem if possible.

**utils diagnose test**

This command runs diagnostic tests and displays the results.

**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 at network drive or the tape

**COMMANDS:**

**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 to connect to 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: utils disaster_recovery cancel_backup confirm

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

utils disaster_recovery restore

These commands invoke a restore.

COMMANDS:

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 mandatory path to retrieve backup tar file from this location

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

userid is the user id to connect to remote machine.

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 to restore files from 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.
COMMANDS:

**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 to connect to remote machine.

**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:** **utils disaster_recovery show_registration**

**utils disaster_recovery show_tapeid**

This command show the list of tape IDs.

**COMMAND:** **utils disaster_recovery show_tapeid**

**utils disaster_recovery status**

This command show status of ongoing backup or restore operation.

**COMMAND:** **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.

**COMMANDS:**

**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 iostat**

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

**COMMAND:** `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.

**COMMANDS:**

- `utils iothrottle disable`
- `utils iothrottle enable`
- `utils iothrottle status`

**utils netdump**

**utils netdump client**

These commands configure the netdump client.

**COMMANDS:**

- `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.

- `utils netdump status`

This command starts the netdump client.
This command displays the status of the netdump client.

**utils netdump server**

These commands configure the netdump server.

**COMMANDS:**

- **utils netdump server add-client**
- **utils netdump server delete-client**
- **utils netdump server list-clients**
- **utils netdump server start**
- **utils netdump server status**
- **utils netdump server stop**

**utils network**

**utils network arp**

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

**COMMANDS:**

- **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.

- **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.

- **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: **utils network capture** [options]

OPTIONS:

[page] pauses output.

[numerical] show hosts as dotted IP addresses.

[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] indicates 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: **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: **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:** `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 an IP packets to a remote destination.

**COMMAND:** `utils network tracert dest`

**PARAMETER** `dest` is the dotted IP or host name of the destination.

utils ntp

This command displays the NTP status or configuration.

**COMMANDS:**

- `utils ntp status`
- `utils ntp config`

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

utils raid

See Also

Use these commands to maintain the RAID disk. They are needed only on servers utilizing software RAID.

COMMANDS:

utils raid disk maintenance disable This command stops the scheduled RAID service.

utils raid disk maintenance enable This command verifies the RAID scheduling.

utils raid disk maintenance status This command gives the status for the weekly scheduled software RAID 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.

COMMANDS:

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.

COMMANDS:
**utils reset_application_ui_administrator_name**

This command is used 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.

**utils reset_application_ui_administrator_name**

This command is used 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 reset_ui_administrator_name**

This command resets the user name for the administrator account.

**utils reset_ui_administrator_password**

This command resets the password for the administrator account. Entering it prompts for the new password.

**utils service**

**utils service list**

This command retrieves status for all services.

**COMMAND:** **utils service list** [page]

**OPTION** [page] pauses after each page.

**utils service restart**

This command restarts a service.

**COMMAND:** **utils service restart** serv

**PARAMETER** serv is the name of the service to restart.

**utils service start**

This command starts a service.

**COMMAND:** **utils service start** serv

**PARAMETER** serv is the name of the service to start.
utils service stop

This command stops a service.

COMMAND: `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: `utils snmp walk <version> <community> <ip-address> <object> [file]`

PARAMETERS:

`version` is 1 or 2c.

`community` is the community string.

`ip-address` is the IP address of the server.

`object` is the Object ID.

OPTION `[file]` is the filename to get.

utils snmp hardware-agents

COMMANDS:

`utils snmp hardware-agents restart`

This command restarts all of the SNMP agents provided by the vendor of the hardware.

`utils snmp hardware-agents status`

This command shows the status of the SNMP agents provided by the vendor of the hardware. Note that not all hardware agents provide status.

utils snmp test

This snmp test sends sample alarms to local syslog, remote syslog and snmp trap.

COMMAND: `utils snmp test`
utils snmp walk

This command is used to walk the SNMP MIB starting with the specified OID.

COMMAND: **utils snmp walk** <version> <community> <ip-address> <object> [file]

PARAMETERS:

version is 1 or 2c.

community is the community string.

ip-address is the IP address of the server.

object is the Object ID.

OPTION [file] is the filename to walk.

utils soap realtimeservice test

This soap test executes number of test cases on the remote server as specified by a parameter of remote-ip, remote-http-user, or remote-http-password.

COMMAND: **utils soap realtimeservice test** <remote-ip> <remote-http-user> <remote-http-password>

PARAMETERS: (At least one parameter is required.)

remote-ip = remote ip address of the machine under test

remote-http-user= remote http user who has role to access soap api

remote-http-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: **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:** `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.

**COMMAND:** `utils system switch-version`

`utils system upgrade`

This command allows you to upgrade the server.

**COMMAND:** `utils system upgrade <cancel> <get> <list | start>`

**PARAMETERS:**

`cancel` cancels the active upgrade.

`get {local | remote} file` gets an upgrade file from which to upgrade. Local specifies that the upgrade files are on a local drive. Remote specifies that the upgrade files are on a remote system.

`list {local | remote} path` lists the available upgrade files on the local or remote system.

`start` starts an upgrade with the upgrade file that is obtained with the `get` parameter.
Load Balancing

In cases where a Unified IC multi-node deployment experiences a heavy reporting workload, system administrators have the option to deploy server load balancing (SLB).

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.

It is beyond the scope of this guide to provide details on load balancing, and load balancing is optional for Unified IC.

The purpose of this Appendix is to present the configuration used for Unified IC on internal Cisco Quality Assurance lab environments.

Example of ACE Load Balancing Configuration

Cisco Quality Assurance set up load balancing using the Cisco Application Control Engine (ACE) module. In this environment:

- Users log in to Unified IC using the ACE virtual IP address, and not the IP Address of the node.

  ACE distributes the client login request to a physical Unified IC server.

- All nodes used the same UCCE data sources (historical and realtime).

The cluster consisted of eight nodes. The virtual address for ACE was http://10.86.yyy.xxx.
From the ACE console, enter the command `do show serverfarm CUIC_FARM_SRV` to monitor the loading.

**Step 1** Create the Ethernet interface:
- `interface gigabitEthernet 1/1 (using your port)`
- `description Ethernet port (port 1 is configured for speeds of 100 Mbps and full-duplex operation)`
- `switchport access vlan 300 (using your vlan number) no shutdown`

**Step 2** Create the resource server RC_Web

```
resource-class RC_Web
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 10.00 maximum unlimited
```

**Step 3** Associate the resource with Admin context: context

```
context Admin member RC_Web
```

**Step 4** Define the server nodes:

```
rserver host CUIC-SRV-1
  Ip address 10.86.228.30
  inservice
rserver host CUIC-SRV-2
  Ip address 10.86.228.31
  inservice
rserver host CUIC-SRV-3
  Ip address 10.86.228.32
  inservice
rserver host CUIC-SRV-4
  Ip address 10.86.228.33
  no inservice
rserver host CUIC-SRV-5
  Ip address 10.86.228.34
  no inservice
rserver host CUIC-SRV-6
  Ip address 10.86.228.35
  no inservice
rserver host CUIC-SRV-7
  Ip address 10.86.228.36
```
no inservice
rservr host CUIC-SRV-8
Ip address 10.86.228.37
no inservice

Step 5  Configure the server farm:

Serverfarm host CUIC_FARM_SRV
Probe CUIC_PROBE_SRV
rservr CUIC-SRV-1 8081
inservice
rservr CUIC-SRV-2 8081
inservice
rservr CUIC-SRV-3 8081
inservice
rservr CUIC-SRV-4 8081
inservice
rservr CUIC-SRV-5 8081
inservice
rservr CUIC-SRV-6 8081
inservice
rservr CUIC-SRV-7 8081
inservice
rservr CUIC-SRV-8 8081
inservice

Step 6  Configure probe (to determine if the Unified IC server is running):

Probe http CUIC_PROBE_SRV
  port 8081
  interval 6
  faildetect 3
  passdetect interval 6
  passdetect count 3
  receive 5
  request method get url /cuic/probe
  expect status 200 200
  open 1

Step 7  Configure sticky. (‘Sticky’ allows the same client to maintain multiple simultaneous or subsequent http connections with the same real server for the duration of a session.)

sticky ip-netmask 255.255.255.255 address source
srcip-sticky-CUIC timeout 10 serverfarm CUIC_FARM_SRV

Step 8  Configure map and policies:

class-map match-all CUIC_HTTP_CLASS_L3
  2 match virtual-address 10.86.yyy.xxx tcp any

policy-map type management first-match remote_mgmt_allow_policy
  class class-default
    permit

policy-map type loadbalance first-match CUIC_HTTP_POLICY_L7
  class class-default
    sticky-serverfarm srcip-sticky-CUIC

policy-map multi-match CUIC_CLIENT_POLICY
  class CUIC_HTTP_CLASS_L3
    loadbalance vip inservice
    loadbalance policy CUIC_HTTP_POLICY_L7
    nat dynamic 1 vlan 300
Step 9  
Create the vlan interface:

```
interface vlan 300
    description CUIC ACE Service on vlan 300
    ip address 10.86.yyy.xxx 255.255.254.0
    access-group input ALL
    nat-pool 1 10.86.yyy.xxx 10.86.yyy.xxx netmask 255.255.254.0 pat
    service-policy input remote_mgmt_allow_policy
    service-policy input CUIC_CLIENT_POLICY
    no shutdown
```
Index

ACE....153
active directory....29
  and reporting users....29
  configuring....29
adding
  devices....15
  member nodes....16
  super users....9
Administration console....1, 5
  logging in....6
Administrator User Management....9
certificates....81
Cisco Unified Administration....2, 92
Cisco Unified OS Administration....6, 81
Cisco Unified Serviceability....2, 6, 80, 92
CLI
  access to....92
  basic system commands....94
  disk and backup commands....94
  hardware information commands....94
  network utilities commands....94
  performance commands....94
  platform commands....94
  security commands....94
  see also Command Line Interface....93
  show commands....114
  system administration user....93
Unified IC commands....94
unset commands....134
utils commands....136
cluster
  controller node....5
member nodes....5
nodes....5
cluster status....81
Command Line Interface
  delete commands....96
  file commands....98
  logging in....93
  navigation....93
  run commands....102
  set commands....102
configuring
  active directory....29
  devices....15
  log and trace settings....19
  reporting....29
  SMTP for report schedule email....31
  super users....9
  control center....27
  controller node....5, 7, 15, 16
CUIC database....7, 82
Cuic Traps....43
database
  backup....83
  backup and restore....81
  CUIC database....82
  purge and time change....84
  purged tables....84
  purging....84
  replication....7, 83
  restore....84
  restore and rebuild....85
  system database....82
  UCCE database....82
delete commands (CLI)....96
deleting
devices...15
credentials...11
customer nodes...16
failure...12
member nodes...16
policies...12
restarting...27
retrieving...34
to Command Line Interface...93
super users...9

Device Management...15

configuring...18

configuration

control center...27

control center

device management...15

device management

devices...15

device management

restartability...27

device management

see also nodes...27

controller

starting...27

starting

status...27

status

stopping...27

stopping

Disaster Recovery System...2, 6, 81, 92

Disaster Recovery System

drawers...6, 87

Administrator User Management...9

Administrator User Management

device management...15

device management

tools...47

tools

editing

device configurations...15

device configuration

editing

deleting in operations console...17

deleting

file commands (CLI)...98

file commands (CLI)

IMS users...91

IMS users

license

best practices...89

license

license file...34

license file

obtaining...89

obtaining

replication...34

replication

retrieving...34

retrieving

types...90

types

load balancing...153

load balancing

log and trace settings...19

log and trace settings

log in...6

log in

log levels...21

log levels

logs

basic level...21

detailed level...22

detailed level

editing...20

editing

file commands...20

file commands

levels...21

levels

size...20

size

stored locations...21

stored locations

member nodes...5, 7, 15, 16

member nodes

accessing from the Controller node...27

accessing

adding...16

adding

defining in operations console...17

defining

deleting...16

deleting

navigation

drawers...6, 87

drawers

filtering lists...88

filtering

in Command Line Interface...93

in Command Line Interface

sorting items...88

sorting

title bar...89

title bar

Navigation dropdown...6

Navigation dropdown

network status...81

network status

online help...88

online help

passwords

active directory...29

active directory

changing...12

changing

expiration...12

expiration

hack count...12

hack count
SMTP....31
super users....11
system administrator user....92
performance objects....53, 55
remote support....81
replication....83
reporting configuration....29
RTMT....47
  and Unified IC....49
  download....48
  required services....48
  sign in....48
  user interface....51
run commands (CLI)....102
  scheduling
    reports....31
      Unified CCE User Integration....32
    session timeout....6
set commands (CLI)....102
show commands (CLI)....114
sign in
  credentials....11
  failure....13
  RTMT....48
SMTP
  CLI commands....97
    for report schedule email....31
SNMP....37
  Unified IC MIBs....38
super users....1, 9, 91
  adding....9
  and system application user....6
  credentials....11
  deleting....9
  editing....9
login policies....12
  multiple....10, 91
  supervisors
    importing into Unified IC....32
    system administrator user....92
      and Command Line Interface....93
      configuring at installation....92
    system application user
      is initial super user....6
      password....17
    system database....82
    system status....27, 81
    timeout....6
title bar....89
tools drawer....47
trace level definitions....21
  infrastructure trace....22
  subsystem specific....23, 24
UCCE database....82
UCCE User Integration
  about....32
  scheduling....32
Unified IC
  importing supervisors from Unified CCE....32
  MIBs....38
  performance objects....53
Unified IC MIBs....38
  CuicClusterInfo....42
  CuicDataSourceInfo....43
  CuicDbInfo....41
  CuicGeneralInfo....39
  CuicLicenseInfo....40
  CuicReporting....40
  CuicReportScheduler....41
  CuicSecurity....42
Cuic Traps...43
EnvInfo Events...46
ThreadPool Events...45
Unified IC performance counters...55
    Cuic Tomcat Connector...56
    Cuic Tomcat JVM...57
    Cuic Tomcat Web Application...57
    DB Change Notification Client...58
    DB Change Notification Server...58
    DB Change Notification Subscriptions...59
    DB Local DSN...59
    DB Performance Info...59
    DB User Host Information Counters...59
    Enterprise Replication DBSpace...59
    Enterprise Replication Perfmon Counters...60
    Intelligence Center General Information...60
    Intelligence Center JVM Statistics...60
    Intelligence Center License Information...61
    Intelligence Center System Condition...61
    Intelligence Center Thread Pool Section...63
    IP...63
    IP6...64
    Memory...65
    Network Interface...67
    Number of Replicates Created...68
    Partition...69
    Process...70
    Processor...71
    Ramfs...71
    Reporting Engine Info...72
    Scheduler Info...75
    System...75
    TCP...77
    Thread...77

Unified IC Reporting UI

accessing from Administration console...7
authenticating reporting users...29
title bar...89
unset commands (CLI)...134
utils commands (CLI)...136
Welcome page...6