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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>i</td>
</tr>
<tr>
<td>Preface</td>
<td>v</td>
</tr>
<tr>
<td>Purpose</td>
<td>v</td>
</tr>
<tr>
<td>Audience</td>
<td>v</td>
</tr>
<tr>
<td>Organization</td>
<td>v</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>vi</td>
</tr>
<tr>
<td>Product Naming Conventions</td>
<td>vi</td>
</tr>
<tr>
<td>Conventions</td>
<td>vii</td>
</tr>
<tr>
<td>Obtaining Documentation and Submitting a Service Request</td>
<td>viii</td>
</tr>
<tr>
<td>Field Alerts and Field Notices</td>
<td>viii</td>
</tr>
<tr>
<td>Documentation Feedback</td>
<td>viii</td>
</tr>
<tr>
<td>Unified CCMP Overview</td>
<td>9</td>
</tr>
<tr>
<td>Operational Overview</td>
<td>9</td>
</tr>
<tr>
<td>Basic Administration Tasks</td>
<td>10</td>
</tr>
<tr>
<td>Configuration of Unified CCMP Security</td>
<td>10</td>
</tr>
<tr>
<td>First Steps for Host Administrators</td>
<td>11</td>
</tr>
<tr>
<td>Configuring Imported Resource Data</td>
<td>11</td>
</tr>
<tr>
<td>Equipment Mapping</td>
<td>11</td>
</tr>
<tr>
<td>Automatic Resource Movement</td>
<td>11</td>
</tr>
<tr>
<td>Shared Remote Resources</td>
<td>12</td>
</tr>
<tr>
<td>Creating a Tenant Administrator</td>
<td>12</td>
</tr>
<tr>
<td>Assigning Administrator Privileges</td>
<td>13</td>
</tr>
<tr>
<td>Using the Agent Password Reset Utility</td>
<td>13</td>
</tr>
<tr>
<td>To change a password</td>
<td>14</td>
</tr>
<tr>
<td>Password Complexity Rules</td>
<td>14</td>
</tr>
</tbody>
</table>
Unified CCE Password Compliancy .................................................. 14

System Architecture .................................................................................. 15

Web Application .......................................................................................... 16

Application Server ....................................................................................... 16

Identity Server .............................................................................................. 16

Data Import Server ...................................................................................... 16

Provisioning Server ..................................................................................... 16

High Availability ........................................................................................... 17
  Application Server to Database Connections ............................................. 17
  Database Server Component Failover ....................................................... 18

Remote Resource Provisioning ................................................................. 19

System Management ................................................................................... 19

Remote Resource States ............................................................................ 19
  State Descriptions .................................................................................. 20
  Pending Active ..................................................................................... 21
  Ready .................................................................................................. 21
  Error ................................................................................................... 21
  Delete Pending .................................................................................... 21
  Deleted ............................................................................................... 22
  User Interface ...................................................................................... 22
  Database Codes ................................................................................... 22
  Memberships ......................................................................................... 23
  State Machine Scenarios ....................................................................... 23

Provisioning Non-CCE Peripheral Types .................................................. 24

Unified CCE Purge Logic ............................................................................ 25

Mobile Agent Support .................................................................................. 26
  About Mobile Agents .............................................................................. 26
  Configuring Mobile Agent Support in Unified CCE ......................... 26
  Configuring Mobile Agents .................................................................... 26
  About Configuring Mobile Agents ....................................................... 26
  Configuring the Agent Desk Settings for Mobile Agents ............... 27
  Configuring CTI Ports and Device Targets for Mobile Agents ....... 27

Partitioned Internet Script Editor ............................................................... 28
  About the Partitioned Internet Script Editor ...................................... 28
  Configuring ISE Integration with Unified CCMP ................................. 28
Contents

Database Backup and Recovery ................................................................. 53

Troubleshooting ....................................................................................... 54

DBCheck ................................................................................................... 54
  Overview ............................................................................................... 54
  Architectural Background ................................................................. 55
  Installation .......................................................................................... 55
  Configuration ...................................................................................... 55
  Running DBCheck ............................................................................... 57
  Logging and Error Reporting ............................................................ 59
  Reviewing Logs .................................................................................. 59
  Troubleshooting DBCheck ............................................................... 59

Unified System CLI ................................................................................... 60
  About Unified System CLI ............................................................... 60
  Installing Unified System CLI .......................................................... 60
  Starting Unified System CLI ............................................................. 60
  Getting Help ...................................................................................... 60
  Unified System CLI Command Reference ....................................... 61

General Troubleshooting ......................................................................... 63
  Delays in Importing Agent Changes ............................................... 63
  Web Portal Timing Dialogs ............................................................... 63
  Installing the UCCE Config Web Service Certificate .................. 63
    Installing the Security Certificate in the User Certificate Store .... 64
    Installing the Security Certificate in the Computer Certificate Store 65
    Installing the Security Certificate for ICE Users ......................... 66
  Unable to Associate Domain User Account with a Supervisor ...... 66
Preface

Purpose

This document explains how to administer and provision the Unified Contact Center Management Portal (Unified CCMP) platform.

Audience

This document is intended for all users of Unified CCMP, from high-level administrators to team supervisors. The reader needs no technical understanding beyond a basic knowledge of how to use computers.

Organization

The sections of this guide are as follows:

Chapter 1 Unified CCMP Overview
This chapter provides a general overview of Unified CCMP.

Chapter 2 Basic Administration Tasks
This chapter explains the basic principles behind the day-to-day administration tasks required for unified CCMP.

Chapter 3 System Architecture
This chapter gives an overview of the Unified CCMP system architecture.

Chapter 4 Remote Resource Provisioning
This chapter explains how remote resources are provisioned by Unified CCMP.

Chapter 5 Auditing and Monitoring
This chapter describes the auditing and monitoring features in Unified CCMP.

Chapter 6 Standard Administrative Operations
This chapter describes standard administration operations.

Chapter 7 Advanced Administrative Operations
This chapter describes some advanced administration operations.

Chapter 8 Troubleshooting
This chapter provides some troubleshooting advice.
Related Documentation

Documentation for Cisco Unified ICM/Contact Center Enterprise & Hosted, as well as related documentation, is accessible from Cisco.com at:

- Related documentation includes the documentation sets for Cisco CTI Object Server (CTIOS), Cisco Agent Desktop (CAD), Cisco Agent Desktop - Browser Edition (CAD-BE), Cisco Unified Contact Center Domain Manager, Cisco Unified Customer Voice Portal (CVP), Cisco Unified IP IVR, Cisco Unified Intelligence Center, and Cisco Support Tools.
- For documentation for these Cisco Unified Contact Center products, go to http://www.cisco.com/cisco/web/psa/default.html, click Voice and Unified Communications, then click Customer Contact, then click Cisco Unified Contact Center Products or Cisco Unified Voice Self-Service Products, then click the product/option you are interested in.
- For troubleshooting tips for these Cisco Unified Contact Center products, go to http://docwiki.cisco.com/wiki/Category:Troubleshooting, then click the product/option you are interested in.
- Documentation for Cisco Unified Communications Manager is accessible from: http://www.cisco.com/cisco/web/psa/default.html.
- The Product Alert tool is accessible from (sign in required): http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice.


Product Naming Conventions

In this release, the product names defined in the table below have changed. The New Name (long version) is reserved for the first instance of that product name and in all headings. The New Name (short version) is used for subsequent instances of the product name.

Note This document uses the naming conventions provided in each GUI, which means that in some cases the old product name is in use.
### Old Product Name | New Name (long version) | New Name (short version)
--- | --- | ---
Cisco IPCC Enterprise Edition | Cisco Unified Contact Center Enterprise | Unified CCE
Cisco IPCC Hosted Edition | Cisco Unified Contact Center Hosted | Unified CCH
Cisco Intelligent Contact Management (ICM) Enterprise Edition | Cisco Unified Intelligent Contact Management (ICM) Enterprise | Unified ICM
Cisco Intelligent Contact Management (ICM) Hosted Edition | Cisco Unified Intelligent Contact Management (ICM) Hosted
Cisco CallManager/Cisco Unified CallManager | Cisco Unified Communications Manager | Unified CM

### Conventions

This document uses the following conventions:

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

**Obtaining Documentation and Submitting a Service Request**

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at:


Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

**Field Alerts and Field Notices**

Cisco products may be modified or key processes may be determined to be important. These are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Log into [www.cisco.com](http://www.cisco.com) and then access the tool at [http://www.cisco.com/cisco/support/notifications.html](http://www.cisco.com/cisco/support/notifications.html)

**Documentation Feedback**

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.
Unified CCMP Overview

Operational Overview

The Unified Contact Center Domain Manager (Unified CCMP) is a suite of server components that simplify the operations and procedures for performing basic administrative functions such as managing agents and equipment.

Unified CCMP consists of the following components:

- The **Database Server** component holds information about all the resources (such as agents and dialed numbers) and actions (such as phone calls and agent state changes) within the system.

- The **Application Server** component manages security and resilience, enabling one side of a dual-sided Unified CCMP to use the other side’s servers if one of the servers or connections fails.

- The **Identity Server** component provides a lightweight authentication service that includes Local, Windows, and ADFS authentication.

- The **Web Server** component provides the user interface that enables users to perform resource management and administrative tasks.

- The **Data Import Server** component imports resources (for example Agents, Skill Groups) into the Unified CCMP Database and synchronizes changes made to those resources outside of the Unified CCMP environment.

- The **Provisioning Server** component provides the mechanism to commit resource changes made by Unified CCMP users to back-end contact center systems, for example the Cisco Unified Contact Center Platform.

These components are normally installed on more than one machine.
Basic Administration Tasks

Unified CCMP is a browser-based management application designed for use by contact center/system administrators, business users and supervisors. The Host Administrator user is created when the application is installed. This user does not manage the Unified CCMP application on a day-to-day basis, but will set up tenant administrator users to do so for each configured tenant in the system.

Configuration of Unified CCMP Security

The Unified CCMP web application has a typically small number of different user types:

- **Host Administrator** is responsible for the whole platform and therefore has a view across all the equipment and resources
- **Tenant Administrator** is responsible for the slice of the system assigned to the tenant by the host administrator
- **Tenant User** has access only to the resources and tools assigned by the tenant administrator. Several sub-classes of tenant user may be created by the tenant administrator using user groups and roles to achieve their business requirements.
- **Supervisor User** has access to one or more Agent Teams that they supervise in the contact center. They will have permissions to create Agents and assign them to Teams and Skill Groups

On a new system the Host and Tenant Administrators perform their respective tasks before the Tenant and Supervisor users are given access to the system.

A host administrator is responsible for global platform security management, whereas a tenant admin will be responsible for security management of only the resources in their domain. Security management can be thought of as the process of determining which users can perform which actions in which folders.

This involves creating and managing the following entities:

- **Folders.** The security system used by Unified CCMP is based on a hierarchical folder structure where child folders may inherit permissions from their parent. This means that the folder hierarchy should ideally be designed with security requirements in mind.
- **Users and Groups.** Users can be assigned to groups of users with the same security permissions. A number of predefined groups with commonly required permissions are provided.
- **Roles and Tasks.** Control the actions that can be performed within a folder. Each task is an individual kind of action, such as browsing resources or managing information notices. These tasks are collected together into roles. For example,
you could create an Auditor role that included the ability to manage audit reports, browse audit reports, and browse resources, and then assign certain groups or even individual users the permission to perform that role within certain folders.

For each role a user or group is assigned, they must also be assigned an equivalent global role. Removing a global role removes that user’s ability to perform the corresponding non-global roles anywhere within the system, meaning it is possible to remove permissions in a single click where necessary. The default groups have the correct global permissions pre-assigned.

Security is explained in more detail in the Security Management chapter of the User Guide for Cisco Unified Contact Center Domain Manager.

First Steps for Host Administrators

The Host administrator is responsible for:

- Ensuring that the remote resources (such as Skill Groups, Agents and Call Types) are correctly located in the tenant folder
- Creating a Tenant Administrator user for each tenant
- Adding them to the administrators group for the tenant and assigning any specific roles

Configuring Imported Resource Data

After the initial data import, remote resources imported from Unified CCE and Unified CM are associated with their respective tenants and will be automatically stored in their associated folders.

Equipment Mapping

After installation the host administrator should configure the remote equipment mappings for the system so that resources are placed in the appropriate segregated tenant folders.

An equipment mapping provides a link between a folder in Unified CCMP and the remote equipment, telling the Unified CCMP importer where resources should be placed. To define an equipment mapping, use the Integrated Configuration Environment (ICE) Cluster Configuration tool, Equipment Mapping tab.

For more information see Integrated Configuration Environment (ICE) for Cisco Unified Cisco Unified Contact Center Domain Manager.

Automatic Resource Movement

Prefixes may be used to manage the automatic movement of remote resources to associated folder locations.
To map a prefix to a tenant for the importing of Unified CCE or Unified CM data, the user must have host administrator privileges.

You can only map a prefix to a tenant folder. Any individual item moved to a folder is then excluded from the prefix management import job to prevent it from being automatically moved by the system.

Additional information on creating Prefixes is available in the *User Guide for Cisco Unified Contact Center Domain Manager*.

**Shared Remote Resources**

Where multiple tenants share a Unified CCE or Unified CM then resources will be put into the system unallocated folder. An administrator must then place these remote resources into the appropriate tenant folder through either the Unified CCMP user interface or through the use of Unified CCMP Prefix mappings. Related resource items, such as IP Phones and their Directory Numbers or Agents and their associated Person should be moved to the same folder.

Resources associated with more than one tenant, such as peripherals, media routing domains and phone types should be placed in a folder that should be readable by users from those tenants. More information on how to manage security in Unified CCMP can be found in the *User Guide for Cisco Unified Contact Center Domain Manager*.

**Creating a Tenant Administrator**

1. Click **Tools** link at the top right of the web page to display the Tools page.
2. In the Security Manager section, click **User Manager**.
3. Click **Users** tab to access the User Browser page.
4. Select the tenant folder and click **New**.
5. Fill in the following fields:
   - **User Name** field enter the name as it will appear in the system for the new user
   - **Password** field enter the password for the new user
   - **Confirm Password** field re-enter the selected password
   - **First Name** and **Last Name** fields enter the user's details
   - **Email** field enter the email address of the new user
   - **Description** field enter any explanatory text, if required
6. Select **Advanced Mode** check box and any of the following check boxes if applicable:
Basic Administration Tasks

Using the Agent Password Reset Utility

- **Enabled** check box to ensure that the user is live in the system. If cleared the new user exists in the system, and so can be granted security permissions, but cannot log in
- **User must change password at next Logon** check box to prompt the new user to change their password after their first login
- **Password Never Expires** check box to assign the password to the new user indefinitely
- **User cannot change password** check box to prevent the new user from being able to change their password

Only the User Name, Password and Confirm Password fields are required.

7. Click **OK**.

Assigning Administrator Privileges

Now you must give the tenant administrator the permissions necessary to manage the system. This is done by assigning the new user to the administration group that was automatically created when you created the tenant.

1. In the User Manager, click **Administrator User** to display the Edit User page.
2. Click **Groups** tab.

All users created are automatically assigned to the group Everyone.

3. Select **Advanced Users**. The user’s permissions are automatically updated so that they can manage users, folders, information notices and folder security within the tenant folder.

It is possible to create your own groups with custom permissions, or to grant specific permissions to individual users. See the Security Management section of the User Guide for Cisco Unified Contact Center Domain Manager for details.

Using the Agent Password Reset Utility

Cisco Unified CCMP provides a Change Your Agent Password utility from which agents can change their own passwords.

This page is reached by navigating to the URL: https://<CCMP Server>/Portal/agent_manage_password.aspx. You do not need to have a Portal user account to use the Change Your Agent Password page.
To change a password

1. Enter the Agent Username. This is the login name that you use to log into the peripheral.
2. Enter the Agent’s current password.
3. Enter your new password for the Agent, and confirm.]

You cannot change a password for an Agent using SSO.

Password changes are subject to a small time delay while they are committed to Cisco Unified CCE.

Password Complexity Rules

Passwords for agents must conform to the password complexity rules defined in the Cisco Unified CCMP.

The following settings can be configured:

- Password Format.
- Minimum Password Length.
- Maximum Password Length.

For more information about changing the password complexity rules in Cisco Unified CCMP, please refer to the section on Security Settings located in the User Guide for Cisco Unified Communications Domain Manager.

Unified CCE Password Compliancy

When using the resource management functionality of Unified CCMP to configure Agent and Person entries Unified CCMP will prompt the end user for the entry of logon credentials that agents will use to logon to their equipment.

Minimum length rules applied in Unified CCE will be honored through the Unified CCMP Web User Interface to ensure that agents created/edited within Unified CCMP may logon to their equipment with no further change.

Unified CCE provides the ability to set the minimum password length by accessing the System Information section of Configuration Manager on the AW.
System Architecture

The Unified CCMP system architecture is shown below. The top half of the diagram is a traditional three-tier application. This includes a presentation layer (an ASP.NET web application), a business logic application server, and a SQL Server database. The lower half of the system architecture is a process orchestration and systems integration layer called the Data Import Server and the Provisioning Server, provisioning a connection to Unified Communications Manager (Unified CM) and Unified CCE. Web Application

Figure 3-1 Unified CCMP Architecture
Web Application

The user interface to Unified CCMP is by a web application that is accessed by a web browser (Microsoft Internet Explorer). Access is gained through a secure login screen. Every user has a unique user name. This user name is assigned privileges by the system administrator, which defines the system functions the user can access and perform.

The web application is hosted on the server by Microsoft Internet Information Services (IIS).

Application Server

The Unified CCMP Application Server component provides a secure layer in which all business logic is implemented. The application server component runs in a separate service and is always hosted with the web server component. The application server component also includes caching to improve performance and audits all actions taken by logged in users.

Identity Server

The Unified CCMP Identity Server component provides a two factor identification system that allows implementation of single sign-on, and access control. The lightweight authentication service includes Local, Windows, and ADFS authentication. Users can have mixed authentication modes, which define how a user can access the system.

Data Import Server

The Data Import Server component is an Extract, Transform and Load application for Unified CCMP. The Data Import Server component imports the data used in Unified CCMP.

The Microflow Runtime is the heart of the Data Import Server component. It orchestrates systems without resorting to low level programming languages. The Microflow Runtime is a general purpose scripting environment and can be applied to a wide range of problems. The term microflow describes any modular, reusable and independent unit of business logic. An example microflow might update an agent on the Cisco Unified CCE platform when changes are made through Unified CCMP web server component.

Provisioning Server

The Provisioning Server component is also responsible for monitoring changes in the Unified CCMP system and ensuring that those changes are updated onto Unified CCE. The provisioning server component orchestrates the creation, deletion and update of resources to Unified CCE and Unified CM.
The Unified CCMP Provisioning Service utilizes the Unified CCE ConAPI interface to commit changes to the Unified CCE.

Provisioning changes are managed via periodic cycles performed by the provisioning server. After a change has been committed by the ConAPI interface the Provisioning Server will wait a configurable period of time (5 seconds by default), before moving onto the next operation. This configurable throttle reduces the possibility of overloading Unified CCE during busy times.

The provisioning characteristics of this service are as follows:

- For Agent > Skill Group relationships, the provisioning server will batch together up to 100 requested operations into one request executed every provisioning cycle.
- For all other items (for example Agents, Agent Teams and so on), all items and relationships are treated as separate provisioning operation. These are executed one by one honoring the configured provisioning throttle between operation executions.
- By default this would mean that the creation of an Agent that is linked to one Agent Team and two Skill Groups would create the following provisioning operations:
  - Agent Creations
  - Agent to Agent Team relationship
  - Bulk Agent to Skill Group relationship

High Availability

The Unified CCMP software provides a high-availability deployment option to ensure that in the event of failure the system will remain operational and able to support end user requests.

The high availability model is implemented across all components in the system. Some components provide an automated failover and others require manual intervention to restore operation.

The Unified CCMP High Availability model is an Active – Active model, where all Unified CCMP and dependent services should be active and running under standard operation.

Application Server to Database Connections

In a high availability deployment, there are two Database Servers. These database servers have their information replicated using SQL Server Transactional Replication. If a failure occurs on one side of the system then all data up to the point of failure will have been replicated on the other database server.

The Application Servers test the databases periodically to identify health. If both databases are healthy then the Application Server will connect to the local Database Server. If one of the database health checks fails then the Application Server will
automatically switch the connection to the other Database Server. There may be a minor loss of service whilst the monitoring test and connection switch occurs, but the Application Server will restore service to end users automatically once the next test is performed.

**Database Server Component Failover**

The Database Server contains the Data Import Server and Provisioning Server components of Unified CCMP. These components are essential to the standard operation of Unified CCMP.

- The Data Import Server imports resources from the AW into the Unified CCMP database.
- The Provisioning Server sends changes made in Unified CCMP (via the Web Service APIs, or the web application) to Unified CCE.

Both the Data Import Server and the Provisioning Server monitor the connection to the Unified CCE AW (or AWs) which they are configured to provision to. If one of these tests fails, both services will automatically switch to perform import and provisioning activity from the other side of Unified CCE.

Under normal operation, the Data Import Server and Provisioning Server will be running on both sides of the Unified CCMP system. Both will maintain the required connections to the AW which they then use for importing and provisioning. One side of the Unified CCMP system will be marked as active and one side will be disabled. This means that all provisioning and import activity is performed on only one of the database servers.

To move provisioning and import activity to the other Database Server in a Unified CCMP installation, use the Integrated Configuration Environment (ICE) Failover Manager. For more information, see *Integrated Configuration Environment (ICE) for Cisco Unified Contact Center Domain Manager*.

Only use the Unified CCMP Failover Manager to perform a planned manual failover, for example to perform maintenance on one of the servers. The service to be switched must be running and fully operational on both servers, and the data must have previously been synchronized between the servers. Do not use the Failover Manager to switch between servers in a disaster recovery scenario, for example if one of the servers has failed or has corrupt data.

Provisioning and import activity must always be performed on the same server. This is to avoid race conditions during high volume provisioning operations.
Remote Resource Provisioning

All system and security management for Unified CCMP is performed through the Unified CCMP web application. Most system and security management after the initial setup is performed by individual tenant administrators.

System Management

The Resource Manager tool enables the user to create and manage resources and resource folders within a hierarchical folder structure. Users with sufficient security privileges can access and manage the entire contents of the system via the Resource Manager interface. This lets you remotely configure and administer key aspects of your Unified CC system.

How to manage resources is explained in more detail in the System Management chapter of the User Guide for Cisco Unified Contact Center Domain Manager.

Remote Resource States

A remote resource is any kind of entity on Unified CCE or Unified CM, for example: agents, teams, skill groups, and phones. All the remote resources in Unified CCMP participate in a state machine. A state machine is a collection of states which a resource will progress through during its lifetime. It is important to understand the state machine when troubleshooting problems in Unified CCMP.

The states are shown in Figure 4-1 below:
Provisioning changes are managed via periodic cycles performed by the Unified CCMP Provisioning Server. After a change has been committed, the Provisioning Server will wait a configurable period of time (five seconds by default), before moving onto the next operation. This configurable throttle reduces the possibility of overloading the remote equipment during busy times.

**State Descriptions**

As a remote resource progresses through the state machine its status is reflected as follows:

- **Pending Active**: Initial state for all resources created through the Unified CCMP interface.
- **Ready**: The normal stable state for a resource. Indicates resource has been fully provisioned on external systems.
- **Delete Pending**: Signals the resource is in the process of deletion from all external systems.
- **Deleted**: Final state for all resources. Resources deleted from external systems are retained in Unified CCMP for audit purposes.
- **Error**: Signals a problem with provisioning a resource. Resources can be edited while in this state.
Pending Active

Pending Active is the initial state for all resource items created through Unified CCMP. Pending Active tells us that the resource exists in Unified CCMP, but has not yet been created on the remote equipment. This may be a result of the remote item being configured with an effective from data or simply mean that the change has not yet been made yet.

When a resource item is in the Pending Active state, no updates are accepted from importer microflows or user interface, with the exception that the item may be changed to the Delete Pending state. This business logic ensures that the Unified CCMP database acts as conflict master.

Ready

Ready is the normal state of a resource item in the Unified CCMP database. It indicates that the resource item has been fully provisioned on all the remote equipment controlled by Unified CCMP.

If the user interface edits a resource item then it is changed to the Pending Active state. If an importer microflow updates a resource item, then it changes to the respective state depending on the change.

Error

The Error state signals that an error has occurred while provisioning a resource item. It means that the current status of the item in Unified CCMP is not reflected on the remote equipment.

Using the Resource Manager user interface, additional information about the error may be source by viewing the history tab of the remote resource. This information will help the user identify why the remote resource could not be provisioned allowing them to update the configuration and re-save the remote resource.

The user may choose to remove the remote resource using the Unified CCMP Resource Manager or the Unified CCE / Unified CM tools which will then result in it progressing to deleted status.

When an item enters Error state then a Purge button will be displayed in the status tab allowing the resource to be marked as purged in the Unified CCMP database. This allows changes in Unified CCMP to be cleared, forcing the importer to re-create the item on the next cycle. This will also separate the historical data for the item at the point in time the purge is performed, linking all new historical data to the new resource that will be created by the importer.

Delete Pending

This state signals that the resource item is to be deleted from all external systems.

The DELETED flag and EFFECTIVE_TO fields on the resource item rows in the corresponding dimension pkey map table are set in the transition to this state. For the agent dimension, for example, the corresponding table is TB_DIM_AGENT_PKEY_MAP.
User interface operations are not allowed on a resource item which is Delete Pending – editing in particular. Once it has been changed to Delete Confirmed then the resource item can be reactivated.

The underlying delete business functions in the Unified CCMP Unified CCE and Unified CM connectors always check to see if the resource item is valid before starting a delete operation.

**Deleted**

A resource item changes to the Deleted state once it has been deleted from all externally controlled systems. The Delete Pending microflow runtime ensures all externally controlled systems are updated before the transition occurs. The workflow must also ensure any memberships are reset, for example the deletion of an agent may first require it to be removed from any agent teams.

**User Interface**

The user interface can only edit resource items which are in the Error and Ready states. Resource items in the Pending Active and Delete Pending states cannot be edited until the provisioning system has processed the resource item. There are a number of exceptions to this rule where effective dates can still be changed in the Pending Active state.

The Error state is particularly important as it catches all the resource items that could not be provisioned. The normal use of the Error state is to hold resources that need to be edited before being provisioned again (by changing them to the Pending Active state).

**Figure 4-2 Editable Resource States**

**Database Codes**

The resource state field in the corresponding dimension pkey map table uses these codes. For the agent dimension, for example, the corresponding table is `TB_DIM_AGENT_PKEY_MAP`.

<table>
<thead>
<tr>
<th>Code</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>Ready</td>
<td>Ready is the normal state of a resource item in the Unified CCMP database. It indicates that the resource item has been fully provisioned on all externally controlled systems.</td>
</tr>
<tr>
<td>S</td>
<td>Pending Active</td>
<td>Pending Active is the initial state for all resource items created/edited through Unified CCMP.</td>
</tr>
</tbody>
</table>
### Remote Resource Provisioning

#### Remote Resource States

<table>
<thead>
<tr>
<th>Code</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>Delete Pending</td>
<td>The Delete Pending state signals the resource item is to be deleted from all externally controlled systems. The EFFECTIVE_TO and DELETED fields are also set in the corresponding dimension pkey map table.</td>
</tr>
<tr>
<td>D</td>
<td>Delete Confirmed</td>
<td>A resource item transitions to the Delete Confirmed state once it has been deleted from all externally controlled systems.</td>
</tr>
<tr>
<td>E</td>
<td>Error</td>
<td>The Error state signals an error occurred provisioning a resource item.</td>
</tr>
</tbody>
</table>

#### Memberships

Memberships in the Unified CCMP database also have effective dating and a status. The Pending Active workflows ensure that changes to memberships are reflected on any externally controlled system. The state of a resource item shows whether it has been provisioned on all external systems (for example, whether an agent has been added to Unified CCE). The state also reflects whether all its memberships are up to date and fully provisioned. This approach makes it easy in the user interface to show an item’s state.

### State Machine Scenarios

The following table explores the state machine through some user case scenarios.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimension item is created and provisioned (transitioning it to the <strong>Ready</strong> state). It is then deleted from one of the externally controlled systems.</td>
<td>Dimension item is transitioned to the <strong>Delete Confirmed</strong> state in Unified CCMP.</td>
</tr>
<tr>
<td>Dimension item in the <strong>Delete Pending</strong> state is deleted from a different external system.</td>
<td>Dimension item is transitioned to the <strong>Delete Confirmed</strong> state in Unified CCMP.</td>
</tr>
<tr>
<td>Dimension item in the <strong>Delete Pending</strong> state is reactivated on an externally controlled system.</td>
<td>Dimension item is left in the <strong>Delete Pending</strong> state and will be deleted on all externally controlled systems</td>
</tr>
<tr>
<td>Dimension item in the <strong>Delete Confirmed</strong> state is reactivated on an external system.</td>
<td>Dimension item is transitioned to the <strong>Ready</strong> state in Unified CCMP.</td>
</tr>
<tr>
<td>Scenario</td>
<td>Expected Result</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dimension item fails to provision correctly; perhaps there is a network connectivity issue between Unified CCMP and the Unified CM.</td>
<td>Dimension item is transitioned to the <strong>Error</strong> state. Any systems it was correctly provisioned on are reflected in Unified CCMP database. Details of the provisioning problem are available in the audit tables.</td>
</tr>
<tr>
<td>Dimension item fails to provision correctly and is then deleted in Unified CCMP system.</td>
<td>Dimension item is transitioned to the <strong>Delete Pending</strong> state in Unified CCMP.</td>
</tr>
<tr>
<td>Dimension item partially fails to provision correctly and is then deleted in an externally controlled system.</td>
<td>Dimension item is transitioned to the <strong>Delete Confirmed</strong> state in Unified CCMP.</td>
</tr>
<tr>
<td>Dimension item in the <strong>Error</strong> state is deleted from an externally controlled system.</td>
<td>Dimension item is transitioned to the <strong>Delete Confirmed</strong> state in Unified CCMP.</td>
</tr>
<tr>
<td>Unified CCMP server suffers a total database crash and has to be restored from backup.</td>
<td>Support technician uses the Recovery Console to change the state of all non-deleted dimension items to <strong>Ready</strong>. The import synchronization may take some time to run but ensures all externally controlled systems are in line with Unified CCMP database.</td>
</tr>
<tr>
<td>Just prior to a server crash, a dimension item was created on an externally controlled system but was not updated in Unified CCMP database.</td>
<td>The next time the <strong>Synchronize</strong> microflow runs, it brings back the existing primary key for the dimension item on the externally controlled system and updates its identity in the corresponding dimension pkey map table. For the agent dimension, for example, the corresponding table is <code>TB_DIM_AGENT_PKEY_MAP</code>.</td>
</tr>
</tbody>
</table>

**Provisioning Non-CCE Peripheral Types**

By default items may only be provisioned through Unified CCMP on peripherals of client type Enterprise Agent, System PG and IPCC Enterprise Gateway. These are the supported peripheral types that Unified CCMP has been configured and tested with. It is however possible to configure Unified CCMP to provision items to peripherals that are not constrained to the types listed above.
To configure Unified CCMP to support another peripheral client type follow these steps:

1. On the primary database server, launch Integrated Configuration Environment (installed as part of Unified CCMP).
2. Select the System Properties tool from the drop-down list.
3. Locate the Supported Peripheral Types option in the Miscellaneous section and from the drop-down list, select the check box beside the Peripheral Types you want to be supported.
4. Click Save and close ICE.

When performing an update to the supported peripheral client types ensure that the existing types are not removed from the comma separated list as this will change standard product behavior. The standard supported types are 30,50,51.

5. Restart all Unified CCMP Application Server Services on all of the servers hosting the Application Service.
6. On each Unified CCMP Web Server, in the Run command dialog box, enter IISReset.

**Unified CCE Purge Logic**

When remote equipment resources are deleted in Unified CCMP then they are set to the Delete Pending state in the Unified CCMP database. This forces the Provisioning Server to remove the associated resource(s) on the related equipment.

Some resource types in Unified CCE implement purge logic, causing items to be propagated to a resource pool (similar to a recycle bin in Windows). This stops any properties that are associated with these items from being reused for new resources configured on that Unified CCE instance. For example, a Person in Unified CCE is allocated a Login Name which is a unique identity used to log the agent onto Unified CCE. If a Person is deleted in Unified CCE then it will be moved to the Deleted Objects section of the Unified CCE Configuration Manager tool. The Login Name associated with that Person cannot be re-used until the Person has been manually removed from the Deleted Objects section.

When Unified CCMP’s Unified CCE provisioning capability is configured, the user can select whether the associated CCE instance supports purge on delete logic. If purge on delete is enabled, then resources deleted through Unified CCMP are automatically removed from the Unified CCE Deleted Objects section. This enables their associated properties to be re-used immediately.

If purge on delete is not enabled then Unified CCMP reports an error if you try to reuse a property that is associated with a resource in the Unified CCE Delete Objects section of Configuration Manager. A typical error message for this scenario is:
“Login Name duplicate detected - the login name you are trying to use is currently assigned to another resource”.

Mobile Agent Support

About Mobile Agents

Unified CCE offers a feature called Unified Mobile Agent, which allows any agent with a PSTN phone and a broadband VPN connection to access contact center calls as if they were in the contact center.

This means that:

- agents have the added flexibility of working remotely
- temporary staff can be added to deal with high call volumes at peak times
- geographically dispersed agents with the required skillsets can operate as a team within the contact center environment.

A mobile agent can operate in one of two modes:

- **Call by Call**: the agent is called individually for each connected call and disconnected at the end of the call.

- **Nailed Connection**: the agent is called at logon and their connection with the contact center remains until they logoff.

For more information about Unified Mobile Agent, please refer to *Mobile Agent Guide for Cisco Unified Contact Center Enterprise & Hosted*.

Configuring Mobile Agent Support in Unified CCE

There are several steps required to configure the system to support mobile agents. These steps must be performed in Unified CCE before mobile agents can be created. For detailed instructions see *Mobile Agent Guide for Cisco Unified Contact Center Enterprise & Hosted*.

Configuring Mobile Agents

About Configuring Mobile Agents

When you have configured the system to support mobile agents, you can configure individual agents as mobile agents. To do this, you need to:

- configure the agent desk settings (Agent Desktops in CCMP) to support mobile agents

- configure two CTI ports (IP Phones in CCMP) for each mobile agent: you need a remote CTI port to initiate the call, and a local CTI port to be the mobile agent’s virtual extension
• configure a device target for the local CTI port (in CCMP, this is automatically done via the Directory Number resource).

The agent desk settings can be configured from the CCMP Web Application. If Unified CM provisioning is enabled, the CTI ports and device target can also be configured from the CCMP Web Application or the Resource Management Web Service APIs. The instructions for performing these steps in the CCMP Web Application are below.

If Unified CM provisioning is not enabled you will need to configure the CTI ports and device targets using Unified CM or the domain manager for that equipment. For more information see Mobile Agent Guide for Cisco Unified Contact Center Enterprise & Hosted.

Configuring the Agent Desk Settings for Mobile Agents

To configure the agent desk settings for mobile agents, in the CCMP Web Application:

1. Create an Agent Desktop.

2. On the Details tab for the Agent Desktop, set the Remote Agent Type field to one of Call by Call Routing, Nailed Connection Routing or Agent Chooses at Login, depending on your requirements.

3. Assign this Agent Desktop to the Agents that are to be mobile agents.

Configuring CTI Ports and Device Targets for Mobile Agents

To configure the CTI ports and device targets for a mobile agent (if Unified CM provisioning is enabled), in the CCMP Web Application:

1. Create an IP Phone for the local CTI port. The name used for the IP Phone must begin with the characters LCP. This allows Unified CCE to identify this as a local CTI port.

2. Create an IP Phone for the remote CTI port. The name used for the IP Phone must begin with the characters RCP. This allows Unified CCE to identify this as a remote CTI port.

3. Create a Directory Number and associate it with the IP Phone that corresponds to the local CTI port.

4. On the Details tab for the Directory Number associated with the local IP phone, select Contact Center Enabled. This automatically configures the device target for the local CTI port.

For more information, see Mobile Agent Guide for Cisco Unified Contact Center Enterprise & Hosted.
Partitioned Internet Script Editor

About the Partitioned Internet Script Editor

Cisco’s Internet Script Editor (ISE) can be integrated with Unified CCMP, which allows routing scripts and the resources within those routing scripts to be partitioned using Unified CCMP security. ISE users see only the scripts and the resources within those scripts that they are authorized to access, according to the Unified CCMP security model. For example, when creating a routing script element to route to a dialed number, the ISE user will only see the dialed numbers that the corresponding Unified CCMP user is authorized to access. Similarly, when viewing the available routing scripts, the ISE user will only see the scripts available to the corresponding Unified CCMP user.

ISE integration with Unified CCMP uses the Unified CCMP Analytical Data Web Service to implement the secure partitioning, and requires specific configuration settings in both Unified CCE and Unified CCMP in order to work properly.

Secure partitioning using Unified CCMP is currently only supported for the Cisco Internet Script Editor (ISE). Users of the standard Script Editor on the Unified CCE AW will still see all resources on their associated Unified CCE instance.

Configuring ISE Integration with Unified CCMP

About the Configuration Steps

To configure ISE integration with Unified CCMP, you need to:

1. Configure Unified CCE to use Unified CCMP security partitioning.
2. Create one or more linked Unified CCE and Unified CCMP users with appropriate permissions. The Unified CCE user and the Unified CCMP user are both linked to the same Windows active directory user, which must already exist on the domain on which Unified CCE and the Unified CCMP servers are located. The Unified CCMP user must be a local account, and must match the unique principal name of the Active Directory user. For example, user@domain.local. The password of the Unified CCMP user account must match the password of the corresponding Active Directory user.

Configuring Internet Script Editor to use Unified CCMP Security Partitioning

To configure the Internet Script Editor to use Unified CCMP security partitioning:

1. Log in to the Unified CCE Admin Workstation.
2. In the Unified CCE Web Setup, navigate to Component Management - Administration and Data Servers section. Check the Administration and Data server check box and click Edit.
3. Click **Next** until you see **Database and Options tab**, then select the following options:
   - Select **Internet Script Editor (ISE) server**.
   - Select **Authorization Server**.
   - In **Authorization Server Name**, enter the name of the Authorization Server. This is the Unified CCMP App/Web Server that will be used to apply Unified CCMP security to partition the resource data.
   - In **Authorization Server Port**, enter the port on which the Unified CCMP Analytical Data Services Web Service has been hosted. By default, this is port 8087, but if this has been changed for your installation, enter the value that your installation uses.
   - Fill out the **Central Controller Connection** details tab as appropriate. Check the **Summary**, and click **Finish**.

4. Ensure that the firewall on the server running the Unified CCE AW has been configured to allow inbound traffic from ISE on the appropriate port. For more information, consult the relevant Unified CCE documentation.

5. Ensure that the specified Authorization Server port on the Unified CCMP Authorization Server has been configured in the firewall to allow inbound HTTPS traffic.

When you have completed these configuration steps, when you run ISE, you must specify a Unified CCE user that corresponds to a linked Unified CCMP user. You will not be able to log in otherwise. When you have logged in, you will see only the script items that the linked Unified CCMP user is able to see.

**Creating a Linked Unified CCE and Unified CCMP User**

There are two ways to create a linked Unified CCE and Unified CCMP user so that Unified CCMP security can be applied to ISE scripts and resources. Normally you will create the user in Unified CCMP, specify that it is ISE-enabled and Unified CCMP will automatically create the linked Unified CCE user. But if a suitable user already exists in Unified CCE, Unified CCMP will automatically import it. You then can configure the user as ISE-enabled in Unified CCMP.

**Creating a Linked User in Unified CCMP**

To create a Unified CCMP user that can be used to apply Unified CCMP security to ISE scripts and resources:

1. In Unified CCMP, select **Security > Users** and create a Unified CCMP user with the same name as the corresponding Windows active directory user which is to be associated with the linked Unified CCMP and Unified CCE users. The Unified CCMP user name must be specified as `<username>@<domainname>`. where
<username> is the Windows user name and <domainname> is the fully qualified Windows domain name, for example, iseuser1@testdomain.local.

The user must be created under a tenant.

2. Select Account Enabled, and Internet Script Editor Enabled.
3. On the Password tab, select Reset Password to reset the password. The User must change password at next logon check box will be selected automatically. The user must set the password to match the Active Directory password on login.
4. Enter a temporary password into the Password and Confirm Password fields.
5. Click Save.
6. Give this user Browse Dimensions permission to the Unified CCE folders and resources to which they require permissions. You can do this in one of the following ways:
   • Select the Groups tab and add the user to a group that already has the required permissions.
   • Alternatively, after you have finished the remaining steps in this section, select the “hamburger” icon in the menu bar, to show the tools menu. Select Security. On the Users tab, select the check box beside the user you have just created, then click Change Permissions. Identify a suitable folder role that includes Browse Dimensions, and assign it to this user for each of the folders containing the scripts and resources you want this linked user to be able to access.
7. Click Save to create the Unified CCMP user and a linked Unified CCE user. The Unified CCE user is created on the Unified CCE instance that is associated with the folder where the Unified CCMP user has been created.

Configuring an Imported Unified CCE User for ISE Integration

To configure an imported Unified CCE user to apply Unified CCMP security to ISE scripts and resources:

1. In Unified CCMP, locate the imported Unified CCE user. The Unified CCMP user name will be formatted as <username>@<domainname>, where <username> is the Windows user name and <domainname> is the fully qualified Windows domain name, for example, iseuser1@testdomain.local. The imported user will be in your default import location unless you have moved the user after the import.
2. Click the user to view the details.
3. Select Account Enabled, and Internet Script Editor Enabled.
4. On the **Password** tab, select **Reset Password** to reset the password. The **User must change password at next logon** check box will be selected automatically. The user must set the password to match the Active Directory password on login.

5. Enter a temporary password into the **Password** and **Confirm Password** fields.

6. Give this user **Browse Dimensions** permission to the Unified CCE folders and resources to which they require permissions. You can do this in one of the following ways:
   - Select the **Groups** tab and add the user to a group that already has the required permissions.
   - Alternatively, after you have finished the remaining steps in this section, select the “hamburger” icon in the menu bar, to show the tools menu. Select **Security**. On the **Users** tab, select the check box beside the user, then click **Change Permissions**. Identify a suitable folder role that includes **Browse Dimensions**, and assign it to this user for each of the folders containing the scripts and resources you want this linked user to be able to access.

7. Click **Save** to update the user details for the linked Unified CCMP user.

8. If your Unified CCMP installation does not use single sign on, then before this user can be used to access ISE, you must log in to Unified CCMP as this user and supply a password when prompted. This password must be the same as the password for the corresponding Windows active directory user. If your Unified CCMP installation uses single sign on, this step is not required.

**Supported Objects**

The Script Editor can partition the following resources in a routing or administration script.

Resources that are not supported for Unified CCMP partitioning in this release of the Script Editor are shown in the table below in **italics**. In this release, all resources of these types will be available to the ISE user, regardless of the Unified CCMP partitioning.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Related Resources</th>
<th>Script Node(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>Route</td>
<td>Agent Node</td>
<td></td>
</tr>
<tr>
<td>Peripheral (for Peripheral Number)</td>
<td>Agent To Agent Node</td>
<td>Select by:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Peripheral/Peripheral Number</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enterprise Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Skill Target ID</td>
<td></td>
</tr>
<tr>
<td>Resource</td>
<td>Related Resources</td>
<td>Script Node(s)</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Peripheral, Enterprise Skill Group, Enterprise Route, Route</td>
<td>Queue To Agent Node</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent, Route</td>
<td>Route Select Node</td>
<td></td>
<td>Using Agent(s) as selector</td>
</tr>
<tr>
<td><strong>Call Type</strong></td>
<td>N/A</td>
<td>Call Type Node</td>
<td>Two modes: Static Dynamic by Name or ID</td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Dialed Number</strong></td>
<td>N/A</td>
<td>Dialed Number Node</td>
<td></td>
</tr>
<tr>
<td><strong>Enterprise Service</strong></td>
<td>Service, Route</td>
<td>Enterprise Service Node</td>
<td></td>
</tr>
<tr>
<td><strong>Enterprise Skill Group</strong></td>
<td>Service, Route</td>
<td>Route Select Node</td>
<td>Using Enterprise Service as selector</td>
</tr>
<tr>
<td><strong>Label</strong></td>
<td>Routing Client</td>
<td>Label Node</td>
<td>Labels defined by Routing Client</td>
</tr>
<tr>
<td><strong>Media Routing Domain</strong></td>
<td>N/A</td>
<td>Media Routing Domain Node</td>
<td>By default: Cisco_Voice, Email and Multisession</td>
</tr>
<tr>
<td><strong>Precision Queue</strong></td>
<td>N/A</td>
<td>Precision Queue</td>
<td>Dynamic not supported for this release</td>
</tr>
<tr>
<td><strong>Service</strong></td>
<td>Route</td>
<td>Service Node</td>
<td></td>
</tr>
<tr>
<td><strong>Route</strong></td>
<td>Route Select Node</td>
<td></td>
<td>Using Service(s) as selector</td>
</tr>
<tr>
<td><strong>Skill Group</strong></td>
<td>Route</td>
<td>Skill Group Node</td>
<td></td>
</tr>
<tr>
<td><strong>Skill Group</strong></td>
<td>Route</td>
<td>Queue To Skill Group Node</td>
<td></td>
</tr>
<tr>
<td><strong>Skill Group</strong></td>
<td>Route</td>
<td>Route Select Node</td>
<td>Using Skill Group(s) as selector</td>
</tr>
<tr>
<td>Resource</td>
<td>Related Resources</td>
<td>Script Node(s)</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------</td>
<td>----------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>VRU Script</td>
<td>N/A</td>
<td>Run External Script Node</td>
<td></td>
</tr>
</tbody>
</table>

**Troubleshooting ISE Integration with Unified CCMP**

**Error Reporting**

If there are problems with the ISE integration with Unified CCMP, ISE may report an error. Some error scenarios may also result in an entry in the log file on the Unified CCMP Application Server that was specified as the Authorization Server.

**Error when starting ISE**

**Problem**

ISE takes a long time to open, then reports the following errors:

- Web server access forbidden.
- Cannot connect to distributor. Script Editor will now exit.

**Sample Log File Entry**

None.

**Causes and Solutions**

<table>
<thead>
<tr>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The AW Distributor service is not running</td>
<td>Start the Distributor service on the AW.</td>
</tr>
<tr>
<td>The AW Distributor service is running but ISE cannot connect to it.</td>
<td>Ensure that the firewall on the server running the Unified CCE AW has been configured to allow inbound traffic from ISE on the appropriate port. For more information, consult the relevant Unified CCE documentation.</td>
</tr>
</tbody>
</table>

**Failed to connect to Authorization Server**

**Problem**

When logging into ISE, the following error is reported:

- Failed to connect to the Authorization Server.
Sample Log File Entry 1
2013-01-14 10:58:37,421 ERROR [2736] ErrorHandling.ErrorHandlerBehaviorAttribute WS Exception: Unauthorized (Unknown Username or Incorrect Password) [Authentication] [401] [Sender/Unauthorized]

Sample Log File Entry 2

Sample Log File Entry 3

Causes and Solutions

<table>
<thead>
<tr>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>With no corresponding Unified CCMP Application Server log file entry</td>
<td></td>
</tr>
<tr>
<td>Cause</td>
<td>Solution</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>The AW cannot connect to the Unified CCMP Authorization Server</td>
<td>Ensure that the specified Authorization Server port on the Unified CCMP Authorization Server has been configured in the firewall to allow inbound HTTPS traffic.</td>
</tr>
<tr>
<td>With an entry in the Unified CCMP Application Server log file similar to sample log file entry 1</td>
<td></td>
</tr>
<tr>
<td>There is no corresponding linked Unified CCMP user.</td>
<td>Create a Unified CCMP user with a login name in the correct format, for example, <a href="mailto:iseuser1@testdom.local">iseuser1@testdom.local</a>.</td>
</tr>
<tr>
<td>The corresponding linked Unified CCMP user has not been enabled.</td>
<td>In the Unified CCMP Web Application, select Tools &gt; Users, select the Unified CCMP user and tick the Account Enabled option.</td>
</tr>
<tr>
<td>The corresponding Unified CCMP user account has been locked due to multiple unsuccessful login attempts.</td>
<td>In the Unified CCMP Web Application, select Security Manager &gt; Users, navigate to the Unified CCMP user and check that User Exceeded Maximum Login Attempts is not selected. If it is, clear it to reset the user account.</td>
</tr>
<tr>
<td>The corresponding Unified CCMP user does not have the same password as the Windows active directory user that is being used to log into ISE (only for installations that do not use single sign on).</td>
<td>In the Unified CCMP Web Application, modify the password for the corresponding Unified CCMP user to match the password of the domain user. If the linked Unified CCMP user was created by importing from Unified CCE, and the linked Unified CCMP user has never logged in to Unified CCMP, then the Unified CCMP password may never have been set. In this case, log into Unified CCMP using the linked Unified CCMP user and set the password when prompted.</td>
</tr>
<tr>
<td>With an entry in the Unified CCMP Application Server log file similar to sample log file entry 2</td>
<td></td>
</tr>
<tr>
<td>With an entry in the Unified CCMP Application Server log file similar to sample log file entry 3</td>
<td></td>
</tr>
<tr>
<td>The corresponding Unified CCMP user does not have permission to see the ICM.</td>
<td></td>
</tr>
<tr>
<td>In the Unified CCMP Web Application, select Security Manager &gt; Users, and ensure that this Unified CCMP user has a folder role that includes the Browse Dimensions task on the ICM folder, or is in a group that has such a folder role.</td>
<td></td>
</tr>
<tr>
<td>Cause</td>
<td>Solution</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>There is a mismatch between some or all of:</td>
<td>Check the various ICM names as below (called ICR in some places), and ensure that the last three match the ICM name in the registry on the AW.</td>
</tr>
<tr>
<td>• the ICM name in the registry on the AW</td>
<td>The ICM name in the registry on the AW:</td>
</tr>
<tr>
<td>• the ICM name in the CCE AW</td>
<td>The ICM Instance Name in the AW:</td>
</tr>
<tr>
<td>• the ICM name in Unified CCMP</td>
<td><img src="image" alt="Registry Editor" /></td>
</tr>
<tr>
<td>• the ICM name supplied to ISE.</td>
<td><img src="image" alt="The ICM Instance Name in the AW" /></td>
</tr>
</tbody>
</table>
## Cause

<table>
<thead>
<tr>
<th>The ICM name in the Unified CCMP database:</th>
</tr>
</thead>
</table>

## Solution

<table>
<thead>
<tr>
<th>The ICM name entered in ISE:</th>
</tr>
</thead>
</table>

### Unable to see required resources

#### Problem
ISE starts but the logged in user cannot see the required scripts or resources.

#### Sample Log File Entry
None.
## Causes and Solutions

<table>
<thead>
<tr>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Unified CCMP user does not have a folder role that includes <strong>Browse Dimensions</strong> on the folder containing the required scripts or resources.</td>
<td>In the Unified CCMP web application, select the “hamburger” icon in the menu bar, to show the tools menu. Select <strong>Security</strong>. On the <strong>Users</strong> tab, select the check box beside the user, then click <strong>Change Permissions</strong>. Assign a suitable folder role that includes Browse Dimensions to the folders containing the scripts and resources you want this linked user to be able to access.</td>
</tr>
</tbody>
</table>
Auditing and Monitoring

Unified CCMP enables provisioning users to view the audit histories of individual items.

These audit trails display events that relate to operations that have been performed within the platform, such as move agent, delete skill group and so forth.

In addition to the standard platform audit information admin users can use system logs and performance counters to further aid problem diagnosis or establish system status.

Audit Histories

Resource Audit History

Each individual resource has its own audit history, showing all the events that have occurred on that resource. This can be accessed from the History tab when examining the resource in the Unified CCMP Resource Manager (see the User Guide for Cisco Unified Contact Center Domain Manager). This information can be used for problem diagnosis relating to a particular remote resource or to identify when a particular change was made and by whom.

Using the Edit Filter link available on the History tab allows you to view only events which were successful, events which failed, or to view events that took place between certain dates. You can click on some of these events to see more details.

Activity Monitor

The Unified CCMP Resource Manager includes an Activity Monitor tool which enables you to:

- view the items currently in the provisioning queue
- view audit details for resources, filtered by any or all of the resource type, location, date range, and the provisioning outcome (success or failure).

You can click on an item to see more information about the event. See the User Guide for Cisco Unified Contact Center Domain Manager for more information.

Logging

Logging Levels

Unified CCMP provides an extensive logging framework for each of the components of the system to aid troubleshooting in the event of a problem.
Logging trace levels are stored in the registry for each separate component and may be set to one of the four following values:

<table>
<thead>
<tr>
<th>Logging Level</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ERROR</td>
<td>This is the lowest level of logging. It will only log information relating to exceptions that occurred in the application.</td>
</tr>
<tr>
<td>1</td>
<td>WARN</td>
<td>Warn provides ERROR level logging plus warnings raised for potential system issues.</td>
</tr>
<tr>
<td>2</td>
<td>INFO</td>
<td>Info is the default logging level. It provides ERROR and WARN as well as standard diagnostic information.</td>
</tr>
<tr>
<td>3</td>
<td>DEBUG</td>
<td>Debug is the highest level of logging. It provides detailed information of every operation that is performed. Debug logging has an adverse effect on performance, its usage should be kept to a minimum.</td>
</tr>
</tbody>
</table>

Logging levels are defined on a per component basis and may be configured at the following registry locations:

<table>
<thead>
<tr>
<th>Component</th>
<th>Registry Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Application</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Exony\Components\Web\TraceLevel</td>
</tr>
<tr>
<td>Application Server</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Exony\Components\Application Server\TraceLevel</td>
</tr>
<tr>
<td>Partitioning Service</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Exony\Components\Partitioning\TraceLevel</td>
</tr>
<tr>
<td>Provisioning Server</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Exony\Components\Provisioning\TraceLevel</td>
</tr>
<tr>
<td>Data Import Server</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Exony\Components\Data Pipeline\TraceLevel</td>
</tr>
</tbody>
</table>

Updating the logging level in the registry will require the associated process to be restarted before the change will take effect.

**Log File Locations**

The following table gives the location of the various CCMP log files. In the table, `<install-folder>` is the folder where CCMP was installed on that server. If the default
location was selected when CCMP was installed, `<install-folder>` will be `C:\Program Files\Domain Manager\`.

<table>
<thead>
<tr>
<th>Log File</th>
<th>Server</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application server logs</td>
<td>App/Web Server</td>
<td>`&lt;install-folder&gt;\Application Server\LOGS.</td>
</tr>
<tr>
<td>Web application logs</td>
<td>App/Web Server</td>
<td>`&lt;install-folder&gt;\WebLogs.</td>
</tr>
<tr>
<td>Data import server logs</td>
<td>Database Server</td>
<td>`&lt;install-folder&gt;\Data Import Server\LOGS.</td>
</tr>
<tr>
<td>Provisioning server logs</td>
<td>Database Server</td>
<td>`&lt;install-folder&gt;\Provisioning\LOGS.</td>
</tr>
<tr>
<td>Partitioning logs</td>
<td>Database Server</td>
<td>`&lt;install-folder&gt;\Partitioning\LOGS.</td>
</tr>
<tr>
<td>ICE logs</td>
<td>Database Server</td>
<td>`&lt;install-folder&gt;\ICE\Logs.</td>
</tr>
<tr>
<td>Installer and uninstaller logs</td>
<td>All servers</td>
<td>`&lt;install-folder&gt;\InstallLogs (Windows Installer logs). &lt;install-folder&gt;\InstallLogs (Windows Installer custom action logs). These allow diagnosis of custom exceptions (often reported by Windows Installer as Error 1001).</td>
</tr>
<tr>
<td>IIS logs</td>
<td>App/Web Server</td>
<td><code>C:\inetpub\logs\LogFiles\W3SVC1\u_ex&lt;YYMMDD&gt;.log</code>. These contain details of all web server transactions. They contain standard HTTP status codes. See <a href="http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html">http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html</a> (link checked 30th October 2014) for a full list of HTTP status codes. Some common codes are: 200: OK 401: Failed Authorization 404: Page Not Found 500: Internal Server Error</td>
</tr>
</tbody>
</table>

**Performance Counters**

Unified CCMP integrates with Windows performance counters (accessed by running the `perfmon` command) to provide real time activity monitoring. Unified CCMP appears across several objects in perfmon, each with a number of associated performance counters.
The perfmon graph can combine many different performance counters. Furthermore, perfmon can be configured to trace specific counters at scheduled times of the day. These performance logs can then be exported to Excel for further analysis. Perfmon can also connect to remote computers, if necessary.

For information on how to use and configure perfmon, see the Microsoft documentation on Performance Logs and Alerts.

**Unified CCMP Data Pipeline Object**

<table>
<thead>
<tr>
<th>Counter</th>
<th>Monitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Cache Reloads</td>
<td>Number of times a cache has been reloaded</td>
</tr>
<tr>
<td>Total Database Downloads</td>
<td>Total number of database downloads</td>
</tr>
<tr>
<td>Total Database Requests</td>
<td>Total number of database requests</td>
</tr>
<tr>
<td>Total Database Statements</td>
<td>Total number of TSQL statements</td>
</tr>
<tr>
<td>Total Database Transactions</td>
<td>Total number of database transactions</td>
</tr>
<tr>
<td>Total Directory Rollbacks</td>
<td>Total number of import directories rolled back</td>
</tr>
<tr>
<td>Total Microflow Validation Errors</td>
<td>Total number of microflows that have failed validation testing</td>
</tr>
<tr>
<td>Total Microflows Run</td>
<td>Total number of microflows run</td>
</tr>
<tr>
<td>Total Number Imports</td>
<td>Total number of imports started</td>
</tr>
<tr>
<td>Total Replication Imports</td>
<td>Total number of directories imported on the Subscriber</td>
</tr>
<tr>
<td>Total Replication Publisher Requests</td>
<td>Total number of directories sent for replication</td>
</tr>
<tr>
<td>Total Rows Imported</td>
<td>Total number of rows imported</td>
</tr>
</tbody>
</table>

**Unified CCMP Application Server Object**

<table>
<thead>
<tr>
<th>Counter</th>
<th>Monitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Requests/Second</td>
<td>Application requests processed per second</td>
</tr>
<tr>
<td>Application Requests/Total</td>
<td>Total application requests processed</td>
</tr>
<tr>
<td>Available I/O Threads</td>
<td>The difference between the maximum number of thread pool IO threads and the number currently active</td>
</tr>
</tbody>
</table>
### Auditing and Monitoring

#### Performance Counters

<table>
<thead>
<tr>
<th>Counter</th>
<th>Monitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Worker Threads</td>
<td>The difference between the maximum number of thread pool worker threads and the number currently active</td>
</tr>
<tr>
<td>Max IO Threads</td>
<td>The number of requests to the thread pool that can be active at the same time. All requests above that number remain queued until thread pool IO threads become active.</td>
</tr>
<tr>
<td>Max Worker Threads</td>
<td>The number of requests to the thread pool that can be active at the same time. All requests above that number remain queued until thread pool worker threads become active.</td>
</tr>
<tr>
<td>Min IO Threads</td>
<td>The minimum number of idle asynchronous IO threads currently maintained by the thread pool.</td>
</tr>
<tr>
<td>Min Worker Threads</td>
<td>The minimum number of idle worker threads currently maintained by the thread pool.</td>
</tr>
<tr>
<td>Total Failed Logons</td>
<td>Total number of failed logons</td>
</tr>
<tr>
<td>Total Failed Logons/Second</td>
<td>Total number of failed logons per second</td>
</tr>
<tr>
<td>Total Logon Attempts</td>
<td>Total number of logon attempts</td>
</tr>
<tr>
<td>Total Logon Attempts/Second</td>
<td>Total number of logon attempts per second</td>
</tr>
<tr>
<td>Total Successful Logons</td>
<td>Total number of successful logons</td>
</tr>
<tr>
<td>Total Successful Logons/Second</td>
<td>Total number of successful logons per second</td>
</tr>
</tbody>
</table>

#### Unified CCMP Provisioning Object

<table>
<thead>
<tr>
<th>Counter</th>
<th>Monitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total ConAPI Add Requests</td>
<td>Total number of add requests sent on each ConAPI connection since the service last started</td>
</tr>
<tr>
<td>Total ConAPI Get (Alternate) Requests</td>
<td>Total number of get (alternate) requests sent on each ConAPI connection since the service last started</td>
</tr>
<tr>
<td>Total ConAPI Get (Primary) Requests</td>
<td>Total number of get (primary) requests sent on each ConAPI connection since the service last started</td>
</tr>
<tr>
<td>Total ConAPI Remove Requests</td>
<td>Total number of remove requests sent on each ConAPI connection since the service last started</td>
</tr>
</tbody>
</table>
Counter | Monitors
---|---
Total ConAPI Update Requests | Total number of update requests sent on each ConAPI connection since the service last started

**Unified CCMP <Service Type> Connection Health Object**

<table>
<thead>
<tr>
<th>Counter</th>
<th>Monitors</th>
</tr>
</thead>
</table>
| Health | The health of the connections from this service to each of the listed servers.

**Unified CCMP <Service Type> Connection Requests**

<table>
<thead>
<tr>
<th>Counter</th>
<th>Monitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Requests/Second</td>
<td>Connection requests that this service has processed per second</td>
</tr>
<tr>
<td>Connection Requests/Total</td>
<td>Total connection requests that this service has processed</td>
</tr>
</tbody>
</table>

**Configuring SNMP Traps**

Simple Network Management Protocol (SNMP) traps may be raised from Unified CCMP by configuring Windows to send selected events to an SNMP monitor. This is achieved using a Windows utility called `evntwic.exe`. This utility converts events written to the Windows Event log into SNMP traps that are raised and forwarded by the Windows SNMP service to an SNMP management tool.

To configure SNMP traps for use with Unified CCMP follow these steps:

**Enable the Windows SNMP Feature**

To configure Windows event forwarding to SNMP, the SNMP feature in Windows must be enabled. To do this, on the Unified CCMP server containing the component for which traps are required:

1. Launch the **Server Manager** application.
2. In the Server Manager left hand pane, right-click the **Features** option and select **Add Features**.
3. In the Add Features Wizard window, select **SNMP Services** and expand it to ensure that both **SNMP Service** and **SNMP WMI Provider** are also selected.
4. Click **Next** and then **Install** to complete the deployment of SNMP. Close the Server Manager.
5. Launch the Services application. Locate the SNMP Service, right-click and select Properties.

6. In the Security tab ensure Send authentication trap is selected and, in the Accepted community names section, click Add.

7. Select READ ONLY for community rights and enter a custom Community Name to restrict access through SNMP.

8. Click OK to complete the configuration of the SNMP Service. Close the Services window.

Configure the SNMP Service for Trap Forwarding

Next, the SNMP Service must be configured to forward traps to the management tool that is being used for reporting and alerting.

1. Launch the Services application.

2. In the list of services, locate the SNMP Service, right-click and select Properties.

3. On the Traps tab, enter public in the Community name field and click Add to List.

4. Click Add below the Trap destinations field and in the SNMP Service Configuration dialog box, enter the host name or IP address of the system that will be receiving the trap information (that is, the server hosting the management agents or reporting and alerting tools). Click Add to add the trap destination.

5. If there is more than one system that needs to receive the trap information, repeat step 4 for each of the other servers.

6. Click OK, then close the Services window.

Configure Windows Events to forward to SNMP

Finally, use the evntwin.exe tool to configure the Windows events to be forwarded as SNMP traps. Any event that is raised in the Windows Event Log may be configured to generate an SNMP trap.

1. In the Run command dialog box, enter evntwin.exe.

2. Select Custom, then click Edit.

3. In the Event Sources list, expand the Application source to see the available Unified CCMP events. The Unified CCMP events and their meanings are given in the table below.
<table>
<thead>
<tr>
<th>Event Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCCMP Application Server Monitoring</td>
<td>The core monitoring service for the application server. This posts connection change events to the event log.</td>
</tr>
<tr>
<td>UCCMP Data Import Server Monitoring</td>
<td>The data import service used for importing data from CCE etc.</td>
</tr>
<tr>
<td>UCCMP Partition Table Manager Monitoring</td>
<td>Connection monitoring for the partition manager service (which creates partitioning tables in the database).</td>
</tr>
<tr>
<td>UCCMP Provisioning Server Monitoring</td>
<td>Service used for provisioning changes on remote equipment, for example, CCE etc.</td>
</tr>
<tr>
<td>UCCMP: Partition Table Manager</td>
<td>Core application service for creating partitioning tables in the database.</td>
</tr>
<tr>
<td>X_ANALYTICALDATA, X_HIERARCHY, X_IMPORTER etc.</td>
<td>These are the individual services configured in Windows for Unified CCMP. These applications can be used for subscribing to standard service events, for example, start/stop events etc.</td>
</tr>
</tbody>
</table>

4. To configure an event source to generate SNMP traps, select the event source, wait a few moments, then click Add once it is enabled. In the Properties dialog, specify the trap properties required, then click OK.

5. When you have finished setting the SNMP traps you require, click Apply.
Standard Administrative Operations

This section provides basic information on performing every-day administrative procedures that are required for the system to operate correctly. This includes such activities as the resetting of system account passwords should a domain policy be enforced that requires passwords to be reset within a given time range.

Service Restart Configuration

All Unified CCMP services are configured to start automatically, and restart automatically on failure. However three consecutive failures of a service will cause a system restart. To alter this behavior:

1. Launch the Services application.
2. Double-click to open each Unified CCMP service in turn.
4. Set the response to all the failures to be Restart the Service (changing the Subsequent Failures entry).
5. Click OK.

Resetting Default Database Connections

Unified CCMP provides a Windows client utility allowing for default database connections to be updated for the various components of the system. When Unified CCMP is installed configured connection strings are encrypted and stored in the configuration files specific to each component. In some scenarios it is necessary to update these encrypted connection strings so that the component is able to establish a connection to the database. Common scenarios where this is required are as follows:

- Moving the Unified CCMP Database to a new server
- Expiry of a SQL Server account used at install time

This section outlines the usage of the Connection Updater Tool. This tool is for resetting the connection settings for the relational database used by various Unified CCMP components.

The Connection Updater tool is installed on the system alongside each of separate Unified CCMP component. The tool can be found in the installation directory of an installed Unified CCMP component. This tool is intended to be used when the connection settings to the Unified CCMP relational database defined at install time, have been setup incorrectly. This tool can also be used to change the settings for any
other reason like, switching between Windows Authentication and SQL Server Authentication.

Connection Updater Features

The Connection Updater tool can be launched using the ConnectionUpdater.exe file contained in the installation folder for each component.

To find the tool navigate to the installation directory of the Unified CCMP component using Windows Explorer. Typically, this path would be `C:\Program Files\Domain Manager\Application Server` for the Application Server component. Double-click the executable `ConnectionUpdater.exe`. The Connection Updater tool will open:

Figure 6-1 Connection Updater Tool

When the tool loads, it will check all the installed Unified CCMP components on this server and list the Unified CCMP Services which support resetting of the default database connection settings. In the above screen you can see all the Unified CCMP components are installed on a single server.

The Connection Updater tool enables you to change the connection settings for an individual component one by one or all the components together. The following
The figure shows the default relational database connection settings for the Unified CCMP Data Import Server.

**Figure 6-2  Connection Settings for Unified CCMP Data Import Server**

In this example, you can switch to view the connection settings for other Unified CCMP component services by clearing the Data Import Server check box and selecting the check box for any other component.

If you select more than one Unified CCMP Service the tool will show the default Connection Settings and not the active configuration of any specific Services.

### Connection Updater Usage

The Connection Updater tool enables you to change the following details for the relational database connection settings:

- **Server Name.** This is the database server name when the Unified CCMP database is installed. Default is *localhost*.

- **Catalog.** The Unified CCMP database name. Default is *Portal*.
• **Authentication.** The authentication method for the database connection. The default is Windows Authentication. You may change this to use SQL Server Authentication. If SQL Server Authentication is used then you will need to provide details for the SQL Server User Name and Password.

Select one or more Unified CCMP Services in the Services list by checking the check boxes provided. Change the connection credentials in the **Connection Settings** section and click the **Update** button to apply the changes.

**Testing Connections**

You can use the **Test** button to test the connection details provided.

This test will be a valid if you have chosen SQL Server Authentication to connect to the database. If you have chosen to authenticate using Windows Authentication, then the test will use the credentials of the user running the Connection Updater tool. This may not be the user configured to run the respective services (typically **NETWORK SERVICE**).

**Restart Services**

Any changes to the connection settings made through the Connection Updater tool will require the related services to be restarted before they will take effect. Checking the check box **Restart Services** will automate the restart of the associated services when the Update button is pressed.

**Actions After Upgrading Unified CCE**

When Unified CCE is upgraded to a newer version, the ICE cluster configuration must be updated to ensure that Unified CCMP can communicate with the new version of Unified CCE. To do this, after Unified CCE has been upgraded:

1. On the primary database server, launch **Integrated Configuration Environment** (installed as part of Unified CCMP). The Database Connection dialog box is displayed.
2. Enter the credentials for your database. If you see a dialog box showing errors and warnings, click **OK**.
3. In the ICE Cluster Configuration tool, select the **Setup** tab and click **Configure Cisco Unified CCE Servers** to start the wizard.
4. On the **Select Task** page, select **Modify an existing instance**. Select the Unified CCE instance that has been updated, and click **Next**.
5. Click **Next** to go through the remaining pages in turn, without changing anything.
6. When you see the confirmation message indicating that the wizard has completed successfully, click **Exit** to close the wizard.
7. To save and action your changes, either click the Save icon in the tool bar or select File > Save from the menu.

8. On each of the database servers, restart the Unified CCMP Data Import service and the Unified CCMP Provisioning service.

**User Migration Tool**

To convert old users and keep their settings, you must run the User Migration Tool on the Application Server.

You can access the User Migration Tool from the CCDM CD Drive, by opening the SSO folder, and then the MigrateUsers folder.

The User Migration Tool can be run post upgrade on the application server. It converts old user’s settings by updating ISE users to local users. Their username must match the unique principal name of the Active Directory user, for example "user@domain.local". The password must be set and marked as "must change at next login". The user must set the password to be the same as the Active Directory password on login. Any other users that are using SSO need to have their login name set to "DOMAIN\user".

On running the tool, there are the following options:

- **SSO**: Whether the system was in SSO mode before upgrade.
- **Authentication Types**: The type of authentication you want the tool to look for. The tool will look for ISE users by default. Set to True to look for all authentication types.
- **ActiveDirectoryPath**: The Active Directory path. If left empty, the tool will attempt to bind to the global catalog of the domain the application server is connected to with default settings.
- **UserPassword**: The password you want to set local users to use, mark as "must change at next login".
- **HashingAlgorithm**: The hashing algorithm that the system uses to hash passwords. Set to "SHA256Salt = 6" by default.
- **DeleteUsersThatFailToMigrate**: Select to delete local users that have a "NULL" password or Active Directory users with the wrong name format. Default is set to false. All deleted users can be restored if necessary.

Once the tool has been run, a log file is generated. The log file displays the User IDs of all the users that have been updated, and for all that have failed.

The tool can be run as many times as necessary.
Advanced Administrative Operations

This section provides information on advanced administrative operations. This includes the configuration and management of cluster resources in the event of a failure and advanced procedures to be performed to restore a failed system.

Enabling and Disabling Cluster Configuration Components

This section describes the effects of enabling and disabling the various components in the Unified CCMP cluster configuration model. Each of these components has an Enabled property which can be true or false. To set the Enabled property for a component, use the Integrated Configuration Environment (ICE) Cluster Configuration tool, Servers tab. For more information see Integrated Configuration Environment (ICE) for Cisco Unified Contact Center Domain Manager.

When you disable a connection in the cluster configuration model, the connection is no longer available for use. In a single-sided system that functionality is unavailable until the connection is re-enabled. A dual-sided system will reconfigure itself to use an alternate connection if possible. In this case, the system chooses to use the connection that has the lowest cost from those that are available and enabled. If a connection with a lower cost subsequently becomes available and enabled, the system will automatically reconfigure itself to use that connection.

Table 7-1 lists the components in the cluster configuration model and the effects of changing the Enabled property for each of these components. For more information about these components see Integrated Configuration Environment (ICE) for Cisco Unified Contact Center Domain Manager.

Table 7-1 Using Cluster Configuration to Enable and Disable Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Indicates if this server is enabled. This is a calculated field, and indicates whether all physical resource components on this server are enabled. Changing this value updates the enabled property of all physical resource components on this server.</td>
</tr>
<tr>
<td>Physical Resource Component</td>
<td>Indicates if this physical resource component is enabled. Changing this value also changes the enabled state of the connections to and from the component.</td>
</tr>
<tr>
<td>Physical Resource</td>
<td>Indicates if this physical resource is enabled. This is a calculated field and indicates whether all physical resource components in this physical resource are enabled. Changing this value updates the enabled flag of all physical</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logical Resource</td>
<td>Indicates if this logical resource is enabled. This is a calculated field and indicates whether all physical resources in this logical resource are enabled. Changing this value updates the enabled flag of all physical resources in this logical resource.</td>
</tr>
<tr>
<td>Physical Connection</td>
<td>Allows or prevents monitoring from using the connection.</td>
</tr>
</tbody>
</table>

Using the ICE Cluster Configuration tool to enable or disable items in the cluster (as described in this section) is a different and distinct activity from using the ICE Failover Manager to switch from a healthy active service to a healthy but inactive service in a dual-sided system.

A disabled item will not be considered for use until the item is re-enabled. An inactive item may still be used if it supports the connection with the lowest cost.

**Database Backup and Recovery**

The Data Import Server component has a configuration attribute to stop it processing microflows at a specified time of the day. This allows the Data Import Server component service to be left running even though microflows are not being processed. The advantage of this approach is that health monitoring applications will not raise alerts, such as SNMP traps, because the service is up and running.

Disabling the Data Import Server can be used to stop importing when SQL Server backups are taken. Do not allow backups at the same time as data is being imported because the database does not have a consistent state. Database backups are typically automated and run at a predefined time of the day.

The Data Import Server is enabled through the **EnabledTime** attribute in the Data Import Server service configuration file (**DataPipelineService.exe.config**). In the example below, the Data Import Server processes microflows from 3:00 through to 2:00 (24 hour clock). This effectively disables the Data Import Server for an hour at 2am. Note that an import cycle could start just before 2:00 and so may still be running after 2:00.

```xml
<add key="EnabledTime" value="03:00-02:00" />
```
Troubleshooting

This section provides information on commonly observed issues and the steps to be performed to identify and resolve Unified CCMP related issues. It also includes information on support tools provided with Unified CCMP.

DBCheck

The DBCheck utility automates the execution of health check queries and repairs for the Unified CCMP database. DBCheck provides an automated summary of potential data integrity issues that may affect system stability.

The Unified CCMP database holds the core resources and state machine states that drive the closed loop provisioning operations of the Unified CCMP product. The DBCheck tool is a Support utility that enables the health of the Unified CCMP database catalog to be checked and repaired.

To run DBCheck, you need SQL admin permissions on the Portal database catalog.

Ensure that you have a current back up of the Portal database before executing any repair operations with DBCheck.

The DBCheck tool must be used with caution. Although DBCheck is designed for detecting and repairing potential data integrity issues, do not run this tool repeatedly, since the repair process impacts database performance and may appear to make minor problems worse. If you have frequent issues with data integrity, contact your vendor for help with addressing the underlying issues.

Overview

DBCheck is a console tool that is installed with the Database component of Unified CCMP. It uses a set of rules located in XML files to perform a range of check operations on the database, if errors are found the user can choose to repair them.

During the check process if errors are found then the tool can save the error records plus the relevant product logs so that detailed off-line analysis may be performed.

Rules files can be updated independently of the DBCheck tool itself. Only Unified CCMP supplied rules files can be used with the DBCheck tool. Rules files are signed, so if a rules file is edited DBCheck will no longer accept the file.
Architectural Background

The Unified CCMP database is a Microsoft SQL Server database that holds the configuration, security, and provisioning and audit data for the product. The product may be operated in a high availability mode using a pair of Side A and Side B database servers synchronized with standard SQL Server transactional replication.

The Unified CCMP database catalog is written to by the following services:

- **Web/Application Server.**
  User requests are received via the product web pages and persisted into the catalog. The usual operation here is users peruse their data and make the occasional provisioning request. Some sites use bulk provisioning to make large number of provisioning requests. These are all validated and queued into the Unified CCMP database catalog.

- **Provisioning Server.**
  This service reads the provisioning requests and uses the appropriate workflows to apply them to the related Unified CCE(s) and Unified CM(s) using the Cisco ConAPI and AXL APIs. This is a regulated activity that protects the back-end equipment when very large bursts of activities occur. The results of the provisioning operations are written back to the Unified CCMP database catalog as either successful (items are ready/deleted) or failed (error state).

- **Data Import Server.**
  This service operates in the reverse direction of the Provisioning Server and reads the configuration data from the Unified CCE(s) and Unified CM(s). It applies read data to the data model held in the Unified CCMP database. By default, this operation occurs every 15 minutes.

- **Transactional Replication.**
  Write operations committed into the partner Unified CCMP database catalog are replicated across the network and written to the local database catalog. For information on this standard technology please see http://technet.microsoft.com/en-us/sqlserver/cc511480.aspx

Installation

DBCheck is installed with the Unified CCMP Database component. The DBCheck tool is located in C:\Program Files\Domain Manager\Database\DbCheck if the default installation options are selected.

Configuration

The DbCheck.exe.config file contains the configuration information which may need editing to match a specific installation.
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProvLogLocation</td>
<td>The directory path to the Provisioning Server logs that will be collected as part of the Save command or when run in batch mode.</td>
<td>C:\Program Files\Domain Manager\Provisioning Server\LOGS</td>
</tr>
<tr>
<td>ImportLogLocation</td>
<td>The directory path to the Data Import Server logs that will be collected as part of the Save command or when run in batch mode.</td>
<td>C:\Program Files\Domain Manager\Data Import Server\LOGS&quot;</td>
</tr>
<tr>
<td>RuleLocation</td>
<td>The directory path to the location of the Rules files.</td>
<td>.\Rules\</td>
</tr>
<tr>
<td>OutputLocation</td>
<td>The directory path to the location where the summary and logs files will be saved as part of the Save command or summary rules.</td>
<td>.\Output\</td>
</tr>
<tr>
<td>PrimaryConnectionString</td>
<td>The connection string to the Unified CCMP SQL Server database which is the primary database in case of a dual sided Unified CCMP setup.</td>
<td>Integrated Security=SSPI; Persist Security Info=False; Initial Catalog=Portal; Data Source=(local)</td>
</tr>
<tr>
<td>SecondaryConnectionString</td>
<td>The connection string to the secondary Unified CCMP SQL Server database in case of a dual sided setup.</td>
<td></td>
</tr>
<tr>
<td>SqlCmdTimeOut</td>
<td>The command timeout in seconds used when reading and writing to the SQL Server Portal database.</td>
<td>600</td>
</tr>
<tr>
<td>ErrorTextColor</td>
<td>The console color used in interactive mode to highlight the rules that have errors after a Check command is executed.</td>
<td>Red</td>
</tr>
<tr>
<td>InfoTextColor</td>
<td>The console color used in interactive mode to show the error row’s details when using the Results &lt;rule id&gt; command.</td>
<td>Yellow</td>
</tr>
<tr>
<td>MonitoredServiceNames</td>
<td>The service name fragments that a Repair operation will shut down before beginning the repair operation. <strong>Note: this setting should not be changed.</strong></td>
<td>&quot;_IMPORTER;_PROVISIONING&quot;</td>
</tr>
</tbody>
</table>
Ensure the configuration matches the system configuration before executing the DBCheck tool.

**Running DBCheck**

DBCheck can be executed from the command line by running the DBCheck.exe file from the installation location (typically C:\Program Files\Domain Manager\Database\DbCheck).

In a dual sided Unified CCMP Database setup, the DBCheck must be executed against the database server that acts as the Primary (Publisher) Unified CCMP Database. The tool will do the relevant checks using the Primary Connection to the Unified CCMP database. The tool will exit immediately if it being run against the Secondary Unified CCMP database.

Once initiated the following commands may be executed to monitor system data integrity and repair data in the event of a reported issue.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>A brief description of all the interactive commands is displayed.</td>
<td>help</td>
</tr>
<tr>
<td>list</td>
<td>Displays the titles of all the rules that have been read from the Rules directory.</td>
<td>list</td>
</tr>
<tr>
<td>list &lt;rule id&gt;</td>
<td>Displays detailed information for the specified rules.</td>
<td>list R01 R02 R05</td>
</tr>
<tr>
<td>check</td>
<td>Runs the check functionality of all the rules and displays the summary details to the screen.</td>
<td>check</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The results are not logged to the output directory. Use the save command immediately after the check command to save the results to the output directory.</td>
<td></td>
</tr>
<tr>
<td>check &lt;rule ids&gt;</td>
<td>Runs the check functionality of just the specified rule(s) and displays the summary details to the screen.</td>
<td>check R01 R02 R05</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The results are not logged to the output directory. Use the save command immediately after the check &lt;rule ids&gt; command to save the results to the output directory.</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| repair        | Runs the check functionality of all the rules and, if there is an error, runs the corresponding repair actions. Note the results are only shown to the screen and are not logged to the output directory. If required, the “save” command should be used after the repair operation to write the results to the output directory.  
**Note**: The results are not logged to the output directory. Use the save command immediately after the repair command to save the results to the output directory.  
**Note**: Before executing a repair operation, DBCheck stops the Data Import and Provisioning services. After the repair, DBCheck restarts the services. It is important to check that the services have restarted correctly. | repair   |
| repair <rule ids> | Runs the check functionality for the specified rule(s) and, if there is an error, runs the corresponding repair actions. Note the results are only shown to the screen and are not logged to the output directory. If required, the “save” command should be used after the repair operation to write the results to the output directory.  
**Note**: Before executing a repair operation, DBCheck stops the Data Import and Provisioning services. After the repair, DBCheck restarts the services. It is important to check that the services have restarted correctly. | repair R01 R02 R05 |
| results       | Shows the summary details of the last run check.                                                                                                                                                             | results  |
| results <rule ids> | Shows the detailed rows of the specified rules.                                                                                                                                                           | results R01 R02 R05 |
| save          | Saves the results of last check or repair operation to the output directory. If there were no errors detected then a simple summary is saved otherwise the detailed error rows plus the Data Importer and Provisioning Server logs are saved. | save     |
| clean         | Deletes all the saved sessions from the output directory. The user is first prompted to confirm before deletion takes place.                                                                               | clean    |
| cls           | The screen contents are cleared                                                                                                                                                                              | cls      |
| exit          | Exit interactive mode and restart the Data Import and Provisioning Service.                                                                                                                                  | exit     |
Logging and Error Reporting

By default, DBCheck writes all of its console output to a text file in the installation directory called `DbCheck.log`. This log file can be used to troubleshoot potential issues for example, database connectivity errors, when the tool is used.

If a save command or a batch operation is performed then the tool executes the check queries, records the results, copies the essential log files for the last 24 hours and generates a high level summary of results. A new folder is created in the Output folder with a name derived from the date-time in the following format:

```
yyyy_MM_dd_hh_mm_ss_<Flag>
```

where `Flag` = `E` for errors found or `S` for success (no errors)

This folder contains the following items:

- `Dbcheck Check Summary.html`
- Dump files containing query results for any check queries that returned results.
- `ProvisioningServerLogs` folder containing log files for the Provisioning Server for the last 24 hours.
- `IMPORTERLogs` folder containing log files for the Data Import Server for the last 24 hours.

Reviewing Logs

When check rules return errors then the saved logs should be analyzed before a repair is performed. Some rules such as “In Error Items” return items that have been in the Error status for longer than 24 hours.

It may be perfectly valid that items are in error state, for example the creation of an IP Phone may have failed because Unified CM has reached a license limit. In this scenario, running a repair would remove the IP Phones in error status from the Unified CCMP database and they would not be provisioned on the Unified CM.

The correct process for this scenario would be to identify the licensing exception from the logs, add additional licenses to Unified CM and then re-save the IP Phones through the Unified CCMP Resource Manager.

Troubleshooting DBCheck

If a DBCheck repair returns an error, review the execution log. If a database timeout occurred, then change the timeout configuration, reload the tool and execute the command again.
Unified System CLI

About Unified System CLI
Cisco Unified System CLI is a command line support tool for Cisco support engineers. It provides a common interface to control logging and diagnostics. Cisco Unified System CLI can be run from Unified CCMP to configure and collect diagnostic information from Unified CCMP.


Installing Unified System CLI
Unified System CLI is installed with the Diagnostic Framework (see Installation and Configuration Guide for Cisco Unified Contact Center Domain Manager for more information).

Starting Unified System CLI
To start Unified System CLI, in a command window:
1. Launch Unified System CLI (installed as part of Unified CCMP). A command window opens.
2. At the Enter username: prompt, enter wsmadmin.
3. At the Enter password: prompt, enter the password that was specified for the wsmadmin user when the Diagnostic Framework was installed.
4. At the Enter Instance[ ][Optional]: prompt, press Enter. Do not change the instance you specified on the command line using the devicetype keyword as the Unified CCMP implementation of Unified System CLI does not support this.

See section To see more complete help for a command, <command>, including a description of the command and the options available, enter help <command>
where <command> is one of the commands in the table below.
Unified System CLI Command Reference for a list of commands available.

6. To exit Unified System CLI, type exit.

Getting Help
To get help about Unified System CLI syntax, enter

c
To see the list of available commands, enter
To see the options for a command, `<command>`, enter

`<command> ?`

You can add one or more optional parameters to `<command> ?` to show the next level of options available. For example:

- **show ?** lists the various items you can view using the show command.
- **show log ?** lists the options for controlling the log information.
- **show log redirect ?** lists the options for redirecting the location that the log output is sent to.
- **show log redirect file ?** lists the valid syntax options for specifying the filename if you have chosen to send the log output to a file.

To see more complete help for a command, `<command>`, including a description of the command and the options available, enter

`help <command>`

where `<command>` is one of the commands in the table below.

### Unified System CLI Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture start</td>
<td>Not supported.</td>
</tr>
<tr>
<td>capture stats</td>
<td>Not supported.</td>
</tr>
<tr>
<td>capture stop</td>
<td>Not supported.</td>
</tr>
</tbody>
</table>
| debug level     | Sets the logging level for the Unified CCMP components installed on the system.  
                   
                   Valid values are:  
                   0  Error  
                   1  Warn  
                   2  Info  
                   3  Trace  
                   4  Debug  
                   5  Not supported  
                   99  Not supported |
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show all</td>
<td>Returns a combined set of results from the various show commands in single zip file (by default, covering the last 24 hours).</td>
</tr>
<tr>
<td></td>
<td>Filter results using <strong>component</strong>, <strong>reltime</strong> and <strong>absdatetime</strong>. Specifying the output location using <strong>redirect file</strong> to send the output</td>
</tr>
<tr>
<td></td>
<td>to a text file, or <strong>redirect dir</strong> to send the output to a zip file in a folder.</td>
</tr>
<tr>
<td>show component</td>
<td>Returns a list of components installed on the system. You can specify a component on the command line to return only the results for that component.</td>
</tr>
<tr>
<td></td>
<td>If the component name includes spaces, enclose the name in double quotes (&quot; &quot;). For example:</td>
</tr>
<tr>
<td></td>
<td><strong>show component &quot;CCMP:Application Server&quot;</strong></td>
</tr>
<tr>
<td>show config</td>
<td>Extracts the registry content for Unified CCMP components to the specified file.</td>
</tr>
<tr>
<td></td>
<td><strong>Note.</strong> This command has limited use for Unified CCMP since it is not possible to apply the extracted registry configuration to other machines.</td>
</tr>
<tr>
<td>show debug</td>
<td>Prints the current trace level for the installed components. If passed a component name then only the trace level for that component is returned.</td>
</tr>
<tr>
<td>show devices</td>
<td>Shows the name of the installed product.</td>
</tr>
<tr>
<td>show license</td>
<td>Not supported.</td>
</tr>
<tr>
<td>show log</td>
<td>Obtains log files for the specified date/time range and components, and store them at the specified location.</td>
</tr>
<tr>
<td></td>
<td>Filter results using <strong>component</strong>, <strong>reltime</strong> and <strong>absdatetime</strong>. Specifying the output location using <strong>redirect file</strong> to send the output</td>
</tr>
<tr>
<td></td>
<td>to a text file, or <strong>redirect dir</strong> to send the output to a zip file in a folder.</td>
</tr>
<tr>
<td>show perf</td>
<td>Not supported.</td>
</tr>
<tr>
<td>show platform</td>
<td>Returns system related information about the machine on which Unified System CLI is running.</td>
</tr>
<tr>
<td>show processes</td>
<td>Not supported.</td>
</tr>
<tr>
<td>show sessions</td>
<td>Not supported.</td>
</tr>
</tbody>
</table>
### Troubleshooting

#### General Troubleshooting

**Delays in Importing Agent Changes**

If you make a change to an Agent in Unified CCE, most changes will be imported into CCMP promptly. But if you change the domain account for a Supervisor Agent in Unified CCE, then there may be a delay of up to 24 hours before the change is reflected in CCMP. This is the expected behavior.

**Web Portal Timing Dialogs**

If you run the Unified CCMP web application from a browser session on the web/app server itself, you will see some diagnostic timing information about the web page display times in the top right of the browser window. You can:

- click on an individual time to see more details about the actions taken
- click on \( c \) at the bottom right of the list to clear the current list
- click on \( m \) at the bottom left of the list to minimize the list.

If you run the Unified CCMP web application from anywhere else, the diagnostic timing information is not displayed.

**Installing the UCCE Config Web Service Certificate**

By default, CCMP ignores untrusted certificate warnings about the Unified CCE ConfigWebService certificate (the `Ignore Certificate Warnings` property for the Unified CCE config web service is `True` by default). But if the `Ignore Certificate`
Warnings property for the Unified CCE config web service has been set to False in the ICE tool, then you will need to install the Unified CCE ConfigWebService security certificate before CCMP will work properly.

If you do not do this, CCMP will not work properly and you will see the error “Could not establish trust relationship for the SSL/TLS secure channel with authority” in the system log. The ICE tool will also report this error if you try to test the connection to the Unified CCE instance.

To fix this error you need to:

- install the certificate in the user certificate store of each CCMP database server
- install the certificate in the computer certificate store of each CCMP database server
- (optionally) install the Unified CCE ConfigWebService security certificate in the user certificate store of each user who wants to run ICE and test connections, on each machine they want to be able to run ICE from.

Installing the Security Certificate in the User Certificate Store

To install the Unified CCE ConfigWebService security certificate in the user certificate store, you need to locate the certificate and import it into your certificate store.

On each CCMP database server:

1. On the primary database server, launch Integrated Configuration Environment (installed as part of Unified CCMP). The Database Connection dialog box is displayed.

2. Enter the credentials for your database. If you see a dialog box showing the errors and warnings, click OK.

3. In the ICE Cluster Configuration tool, select the Resources tab and navigate to the Unified CCE instance. Select the Components tab. Select the Inbound connections and expand by clicking on the "...". Select the last node in the Provisioning Server branch. When using the URL replace the %SINK_SERVER% with the server name or address.

4. In Internet Explorer, navigate to the URL you found above. If the certificate has not been installed on this server, you will see a certificate error.

5. Click Certificate Error in the top right hand corner of the window.

6. In the Untrusted Certificate dialog box, select View Certificates.

7. In the Certificate dialog, note the “Issued to:” name (you will need this name to locate the certificate again below) and click Install Certificate.

8. In the Certificate Import Wizard, click Next.
9. In the Certificate Store dialog box, select **Place all certificates in the following store**, and click **Browse**. Choose **Trusted Root Certificate Authorities** and click **OK** to return to the Certificate Store dialog box.

10. In the Certificate Store dialog box, click **Next**. Review the settings and click **Finish** to complete the certificate import wizard.

11. If you see a security warning, click **Yes**, to import the certificate. When the import completes, click **OK**.

### Installing the Security Certificate in the Computer Certificate Store

To install the Unified CCE ConfigWebService Security Certificate in the computer’s certificate store, you need to export the security certificate from the user certificate store where you saved it above and import it into the computer certificate store.

To export the certificate, on each CCMP database server:

1. In the **Run** command dialog box, enter `mmc` to open Microsoft Management Console (MMC).
2. Click **File > Add/Remove Snap-in**, click **Certificates**, then **Add**.
3. In the Certificates Snap-in dialog box, select **My user account** and click **Finish** to add the Certificates snap-in to MMC. Click **OK**.
4. In MMC, expand the Certificates – Current User node, Trusted Root Certificate Authorities node, then click **Certificates** to see the available certificates.
5. Locate the certificate you imported in the section above, right-click on it, and select **All Tasks > Export**.
6. In the Certificate Export Wizard, select **Next**.
7. In the Export File Format dialog box, accept the default format and click **Next**.
8. In the File to Export dialog box, specify a file name and click **Next**. Review the settings and click **Finish** to complete the certificate export wizard.

To import the certificate, on each CCMP database server:

1. In the **Run** command dialog box, enter `mmc` to open MMC.
2. Click **File > Add/Remove Snap-in**, click **Certificates**, then **Add**.
3. In the Certificates Snap-in dialog box, select **Computer account** and click **Next**.
4. In the Select Computer dialog box, select **Local computer** and click **Finish** to add the Certificates snap-in to MMC. Click **OK**.
5. In MMC, expand the Certificates (Local Computer) node Trusted Root Certificate Authorities node, then right-click **Certificates** and select **All Tasks > Import**.
6. In the Certificate Import Wizard, click **Next**.
7. In the File to Import dialog box, browse to the certificate file you exported above, click **Open**, then click **Next** again.

8. In the Certificate Store dialog box, select the option, **Place all certificates in the following store**, then **Browse** and locate the Trusted Root Certificate Authorities store and click **OK** to return to the Certificate Store dialog box.

9. In the Certificate Store dialog box, click **Next**. Review the settings and click **Finish** to complete the certificate import wizard.

### Installing the Security Certificate for ICE Users

This step is only required if an ICE user wants to be able to test Unified CCE connections using the ICE tool.

To install the certificate in a user’s certificate store, each ICE user must repeat the steps in Installing the Security Certificate in the User Certificate Store on Page 64 on the server or servers on which they want to be able to run ICE.

### Unable to Associate Domain User Account with a Supervisor

When you create or edit a supervisor agent in the web application, you can optionally select a domain user account to associate with the supervisor agent. The available domain user accounts are identified from the Active Directory Organizational Unit that was selected when the equipment was configured in ICE.

If you do not see the domain account you want to use in the list of available accounts, then ensure that, on the Domain Controller, the User logon name has been set for that domain user (see the example here).