



Integrated Configuration Environment (ICE) for Cisco Unified Contact Center Management Portal, Release 12.6(1)

For Unified Contact Center Enterprise

First Published: May, 2021

Americas Headquarters

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

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

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

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

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

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

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

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 <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)

Integrated Configuration Environment (ICE) for Cisco Unified Contact Center Management Portal: For Unified Contact Center Enterprise. May 12, 2021

© 2012-2021 Cisco Systems, Inc. All rights reserved.

Contents

- Preface7**
 - About This Guide 8
 - Product Naming Conventions 8
 - Document Conventions 9
 - Related Documentation 9
 - Obtaining Documentation and Submitting a Service Request 10
 - Documentation Feedback 10
 - Field Alerts and Field Notices 10

- Chapter 1: Introduction to ICE11**
 - About ICE 12
 - Using ICE 12
 - Starting ICE 12
 - ICE Menu and Toolbar 13
 - ICE Tool Selection 14
 - ICE Tool Area 14
 - ICE Output Pane 14

- Chapter 2: Cluster Configuration16**
 - About Cluster Configuration 17
 - The Cluster Configuration Model 17
 - Equipment Mappings 17
 - Equipment Mappings and Importer Behavior 17
 - Equipment Mappings and the User Interface 18
 - Resource Ownership Principles 18
 - Remote Tenant Mappings 19
 - Importing Remote Ownership Changes 20
 - Cluster Configuration Tool Reference 20
 - Cluster Configuration Actions 20
 - Cluster Configuration Preferences 21
 - Cluster Configuration Filters 22

Cluster Configuration User Interface	22
Cluster Configuration Error List Pane	23
Setup Page	23
Servers Page	24
Resources Page	26
Logical Resources	27
General Tab	27
Specific Tab	28
Physical Resources	30
Properties of Physical Resource Objects	31
General Tab	31
Specific Tab	31
Components Tab	32
Properties of Physical Resource Components	33
Managing Connections	35
Editing Connections	35
Managing Cost of Connections	38
Equipment Mappings Page	39
Folder Tree Section	40
Source Equipment Section	40
Association Options Section	40
Connections Page	42
Diagnostic Portal Support	43
Configuring the Diagnostic Portal	43
Accessing the Diagnostic Logs	44

Chapter 3: Replication Manager.....45

About Replication Manager	46
The Replication Manager Setup Tab	46
Unified CCMP Database Server Properties	46
Distributor Properties	46
The Replication Manager Monitor Tab	47
Monitor Panes	47
Starting Replication Manager	48
Configuring Replication	48
Disabling Replication	48

Monitoring Replication	49
Identifying Replication Errors	49
Performance Considerations	50
Chapter 4: Failover Manager	51
About Failover Manager	52
Preparing to Use the Failover Manager	52
Starting the Failover Manager Tool	52
Performing a Failover Operation	53
Performing Provisioning Service Failover	54
Performing Data Import Service Failover.	54
Chapter 5: Service Manager	55
About Service Manager	56
Starting Service Manager	56
Starting Services	56
Stopping Services	57
Restarting Services	57
Sorting Services	57
Filtering Services	58
Setting Filters	58
Clearing a Filter.	58
Refreshing the Filtered List.	58
Reloading the List of Services	58
Using the Shortcut Menu	58
Chapter 6: System Properties Manager	60
About System Properties Manager	61
Starting System Properties Manager	61
Setting Global Properties	61
Active Directory Lookup Configuration	61
Activity Monitor	62
Code Lookup, Supported Equipment Types	62

Database Lock Configuration	62
Gadget Management	62
Importer State	63
Local Login Security	63
Login Authentication Configuration	64
Media Upload	65
Miscellaneous	65
Other Security	66
Partitioning State	66
System Limits	66
User Provisioning	67
Setting Local Properties	67
Checksum	67
Partitioning State	68
Versioning Group	68
Setting Resource Properties	68
Resource Items	68
Resource Members	68
Setting Capacity Properties	68

Chapter 7: Custom Dimension Editor70

About the Custom Dimension Editor	71
Custom Dimensions	71
Starting the Custom Dimension Editor	71
Adding a Custom Dimension Item	71
Editing a Custom Dimension Item	72
Deleting a Custom Dimension Item	72
Moving a Custom Dimension Item	73

Chapter 8: ICE Diagnostic Support74

Diagnostic Features	75
Installing the Cisco Diagnostic Portal	75
Configuring ICE Integration with the Diagnostic Portal	75
Viewing Logs	76

Preface

- ▶ [About This Guide](#)
- ▶ [Product Naming Conventions](#)
- ▶ [Document Conventions](#)
- ▶ [Related Documentation](#)
- ▶ [Obtaining Documentation and Submitting a Service Request](#)
- ▶ [Documentation Feedback](#)
- ▶ [Field Alerts and Field Notices](#)

About This Guide

Integrated Configuration Environment for Cisco Unified Contact Center Management Portal explains how to administer and provision the Unified Contact Center Management Portal (Unified CCMP) platform.

Who Should Read This Document

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

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

Document Conventions

This guide uses the following typographical conventions.

Convention	Indicates
<i>Italic</i>	Emphasis, or the title of a published document.
Bold	An item in the user interface, such as a window, button, or tab.
Monospace	A file name or command.
<i>script</i>	A variable, which is a placeholder for user-specific text provided by the user. Or, text that must be typed by the user.

Document conventions

Related Documentation

Documentation for Cisco Unified ICM/Contact Center Enterprise & Hosted, as well as related documentation, is accessible from Cisco.com at: <http://www.cisco.com/cisco/web/psa/default.html>.

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 Contact Center Management Portal
- ▶ Cisco Unified Customer Voice Portal (CVP)
- ▶ Cisco Unified IP IVR, Cisco Unified Intelligence Center
- ▶ Cisco Support Tools

Documentation for these Cisco Unified Contact Center products is accessible from:

- ▶ <http://www.cisco.com/cisco/web/psa/default.html>.

Troubleshooting tips for these Cisco Unified Contact Center products is accessible from:

- ▶ <http://docwiki.cisco.com/wiki/Category:Troubleshooting>.

Documentation for Cisco Unified Communications Manager is accessible from:

- ▶ <http://www.cisco.com/cisco/web/psa/default.html>.

Technical Support documentation and tools are accessible from:

- ▶ <http://www.cisco.com/en/US/support/index.html>.

The Product Alert tool is accessible from (sign in required):

- ▶ <http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice>.

For information on the Cisco software support methodology, refer to *Software Release and Support Methodology: ICM/IPCC*, available from (sign in required):

- ▶ http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/prod_bulletins_list.html.

For a detailed list of language localizations, refer to the *Cisco Unified ICM/Contact Center Product and System Localization Matrix*, available from:

- ▶ http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html.

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:

<https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

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.

Documentation Feedback

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

We appreciate your comments.

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 and then access the tool at <http://www.cisco.com/cisco/support/notifications.html>

1

Introduction to ICE

- ▶ [About ICE](#)
- ▶ [Using ICE](#)

About ICE

The Integrated Configuration Environment (ICE) application is a centralized tool that provides easy access to most of the configuration options available within the Unified CCMP platform. Individual configuration tools are components within ICE.

The ICE application supplied with Unified CCMP has the following components:

- ▶ **Cluster Configuration:** Provides functionality for configuring the network topology used by the Unified CCMP system. This tool enables configuration of servers, resources (for example, Unified CCMP components, Unified CCE components) and the connections between them. It also provides monitoring capabilities.
- ▶ **System Properties Manager:** Provides functionality for configuring system wide properties that control a variety of Unified CCMP components.
- ▶ **Replication Manager:** Provides functionality for configuring and monitoring SQL Server replication between Unified CCMP databases and Microsoft Reporting Services Report Server databases.
- ▶ **Services Manager:** Provides functionality for monitoring and controlling all Unified CCMP services across servers from a single centralized location
- ▶ **Failover Manager:** Provides functionality for performing manual switch over of the Data Import, Provisioning and Mediator services between two servers.
- ▶ **Custom Dimension Editor:** Creates and edits custom dimensions.
- ▶ **Gadget Provider Manager:** This feature is not supported.

Using ICE

Starting ICE

To start ICE:

1. Launch Integrated Configuration Environment (installed as part of Unified CCMP). In the Database Connection dialog box, set the following:
 - **Server Name:** Enter the name of the primary database server.
 - **Database Name:** Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this is **Portal**.
 - **Authentication:** Select **Windows Authentication**.
2. Click **OK**. The ICE Cluster Configuration tool starts by default.

- If there were errors or warnings in the configuration, then the error details are shown in the Cluster Configuration Error List pane (see section “[Cluster Configuration Error List Pane](#)” on page 23).



Note: When ICE starts, the Error List pane shows both connection errors and validation errors. Subsequently, the Error List pane only shows validation errors. But the connection status can be seen at any time on the Connections page (see section “[Connections Page](#)” on page 42)

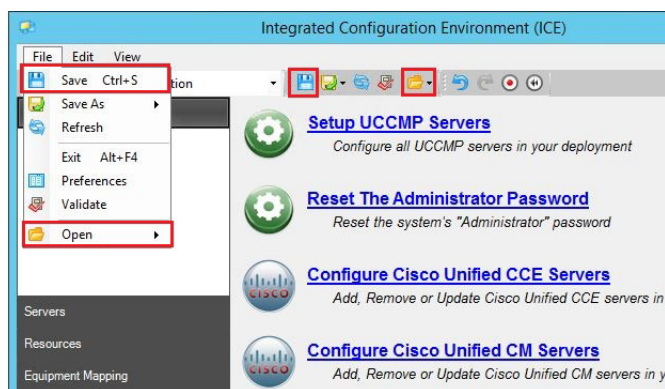
ICE Menu and Toolbar

Common actions are visible in the menu and the tool bars at the top of the screen. The common actions supported by ICE are described in the following table.

Icon	Description
Save	Save any changes.
Exit	Close the ICE application.
Preferences	View the ICE tool and component preferences.
View	Output View the standard output feedback window.
Undo	Undo the last change.
Redo	Redo the last change.

Configured actions may be shown in the menu, the toolbar or both. Generally, commonly used actions (for example, Undo, Redo) are displayed in both the tool bar and the menu, and less commonly used actions just appear in the menu.

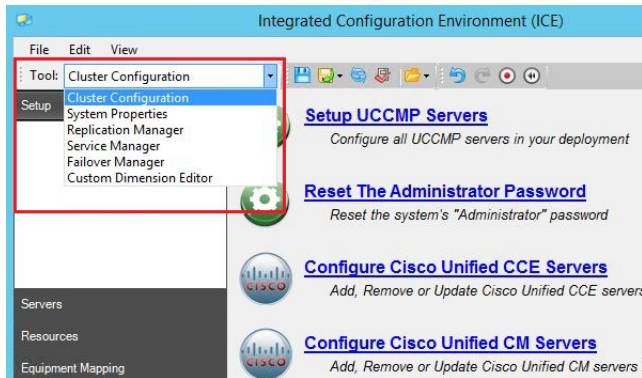
As an example, consider the File action shown in the following figure. **Save** and **Open** are shown on both the menu and tool bar, whereas **Exit** and **Preferences** are only shown in the menu. The ICE tool in this example is the System Properties tool.



Sample toolbar

ICE Tool Selection

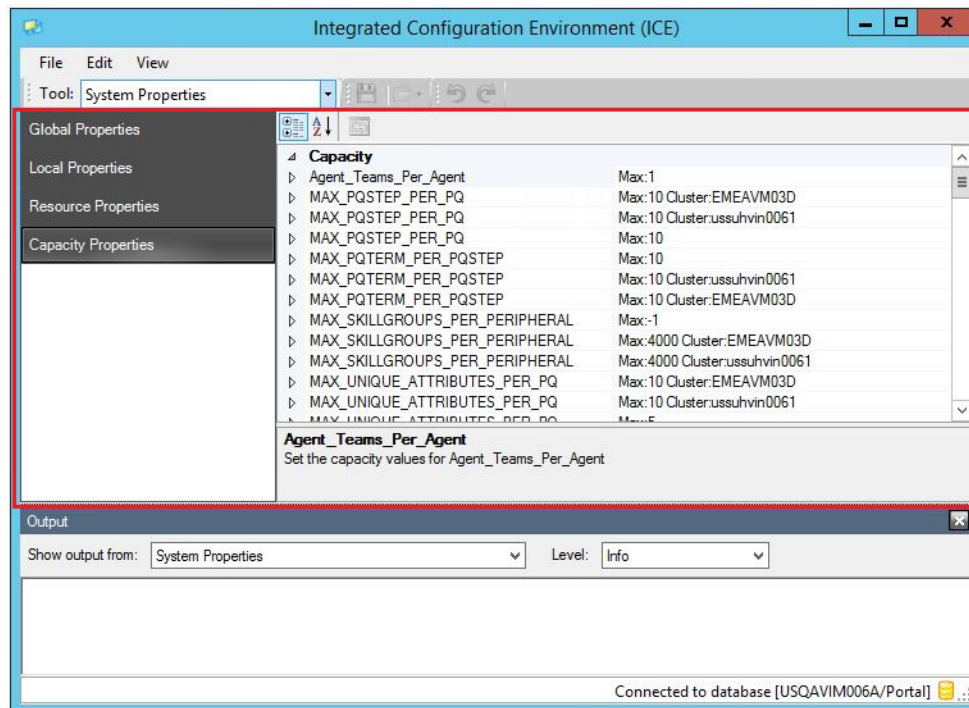
The ICE application toolbar contains a dropdown list below the menu. This contains the available ICE tools. To start an ICE tool, select it from the dropdown list.



Ice tool selection

ICE Tool Area

The central area of the ICE application is used by each ICE tool for their own interface.

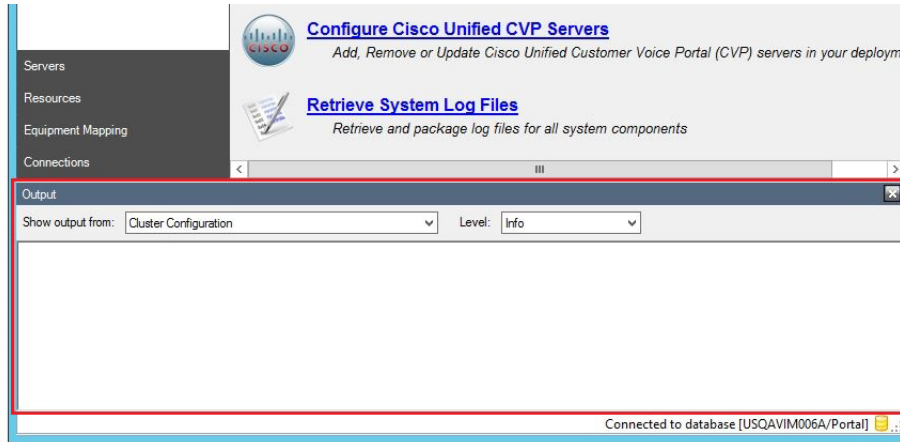


Central Pane for ICE System Properties Tool

ICE Output Pane

The bottom area of the ICE application contains an output pane showing the output from the active ICE tools. This area also contains any additional output panes from specific ICE tools.

If both the ICE output pane and a specific output pane are available, they are shown one on top of the other, with a tab to select the one that is visible. The following figure shows the ICE output pane and the error list pane from the ICE Cluster Configuration tool. In this example, the ICE output pane is currently visible.



Output and Error Panes for ICE Cluster Configuration Tool

You can control the display of the output panes in the following ways:

- ▶ You can change the height of the whole area by dragging the top edge up or down using the mouse.
- ▶ You can close the current pane, by clicking on the cross at the top right of the pane.
- ▶ You can show or hide any currently available pane from the View menu. You can control the output that is shown in the ICE output pane as follows:

Click on the **Show output from** drop down list at the top left of the pane to show output from one ICE tool or from all ICE tools. In the example, the output pane is showing the output from the **Cluster Configuration** tool only.

Click on the **Level** drop down list to choose the level of output you want to see. In the example, the output pane is showing the **Warn** level output messages.

Cluster Configuration

- ▶ [About Cluster Configuration](#)
- ▶ [Cluster Configuration Tool Reference](#)
- ▶ [Setup Page](#)
- ▶ [Servers Page](#)
- ▶ [Resources Page](#)
- ▶ [Equipment Mappings Page](#)
- ▶ [Connections Page](#)
- ▶ [Diagnostic Portal Support](#)

About Cluster Configuration

The Cluster Configuration tool enables you to configure the Unified CCMP and third party servers and components in an Unified CCMP deployment. It also enables you to define connections between these components and specify the connection credentials. The cluster configuration created using this tool provides individual Unified CCMP components with information about how to route data within the system.

The Cluster Configuration Model

The Cluster Configuration tool provides a graphical interface over a model that is used as part of the generic Unified CCMP monitoring component to test and provide connections to all services in the Unified CCMP platform.

The underlying cluster configuration model consists of the following core objects:

- ▶ **Servers:** A server represents a physical computer on the network.
- ▶ **Physical Resource Components:** A physical resource component represents a real service running on a server. For example a ConAPI service or AW Database on an ICM.
- ▶ **Physical Resource:** A physical resource is a grouping of physical resource components that all form part of the same system. For example, a Unified CCE system may consist of an HDS, an AW and a ConAPI component.
- ▶ **Logical Resources:** A logical resource is a grouping of several physical resources that represent replicated versions of a single system. For example, a Unified CCE system may be dual-sided, consisting of two distinct systems for fault tolerance and redundancy. In this situation there would be a single logical Unified CCE resource with 2 physical resources instances, one representing side A and the other representing side B.
- ▶ **Physical Connections:** A physical connection represents a link between two physical resource components. For example, the default component for a Mediator physical resource may be connected to the HDS and AW components of a Unified CCE physical resource. The component being connected to is known as the destination component, and the component connecting is known as the source component.

The Cluster Configuration tool supports loading and saving this model from both an Unified CCMP database and an XML file.

Equipment Mappings

Equipment mappings define mappings between folders and remote equipment which specify where imported items are placed in the Unified CCMP folder tree. They also control the visibility of remote equipment and their resources in the user interface.

Equipment Mappings and Importer Behavior

The importer uses the equipment mappings to determine which folder to place new items in. The folder is chosen by applying the following logic, in order:

- ▶ If the item being imported is owned by a remote tenant and there is a corresponding equipment mapping for that remote tenant, the importer chooses the folder defined by the mapping.

- ▶ If the item being imported is owned by a remote tenant but there is no corresponding equipment mapping for that remote tenant, the importer chooses the default import location folder, if one is defined.
- ▶ Finally, if there is no remote tenant mapping or default import location mapping specified, the importer chooses the **/Unallocated** folder within a subfolder named after the equipment, for example, **/Unallocated/CICM123**.

If an equipment mapping is changed after an initial import, the importer moves existing items to a new folder based on the logic above in the following scenarios:

- ▶ If an item is currently in the equipment's **/Unallocated** folder.
- ▶ If an item's location is no longer synchronized with its remote tenant ownership. See section [“Importing Remote Ownership Changes”](#) on page 20 for details.

Equipment Mappings and the User Interface

Using a combination of a user's security permissions and the equipment mappings, it can be determined which remote equipment the user has the right to access. This is applied when the equipment is listed in the Unified CCMP web application for example, on the person dimension edit screen and phone creation screen (Unified Communications Manager drop-down list).

The user has the right to view equipment if there is an equipment mapping to any tenant that contains any folder that the user has permission to view. For example, if there was a tenant: **/t1** and the user had the right to see folder **/t1/folder1** and there was an equipment mapping to **/t1/folder2** then the user has right to view the equipment. The user also has the right to view equipment which only has equipment mappings to folders outside of tenants.

For more information on moving resources through the Unified CCMP web application please refer to the *Management Portal User Guide*.

Resource Ownership Principles

Resources in Unified CCMP are owned by tenants. This section describes how this ownership is managed and the implications of item ownership on the importer and reports.

Unified CCMP Tenant Ownership

Unified CCMP tenant folders contain the items which they own. Moving an item to another tenant folder automatically changes its owner. Items located outside the tenant folders are not owned by a specific tenant. Depending on the security settings, these items can be shared between tenants or hidden from all tenants.

Default Domain Management

Each time the Default Domain setting is changed using the System Info Tool in the Config Manager, the Unified CCMP ICE wizard must be manually executed to retrieve this information and store it against the Unified CCE Cluster Resource in the Unified CCMP database. Failure to do so causes Unified CCMP to become inconsistent with Unified CCE.

Single Sign-On Management

Each time the Single Sign-On (SSO) mode is updated in Unified CCE, it is not automatically updated in Unified CCMP. The Unified CCE wizard must be manually executed to retrieve this information and store it against the Unified CCE Cluster Resource in the Unified CCMP database. Failure to do so causes Unified CCMP to become inconsistent with Unified CCE and does not display the correct options for configuring Persons in Unified CCMP. SSO mode for Unified CCMP can be set to Disabled, Enabled, or Hybrid mode.

Remote Tenant Ownership

Some Unified CCE items also have an additional level of ownership on the Unified CCE instance. The Unified CCE equivalent of a tenant is a customer definition, which can be associated with the following items:

- ▶ Dialed numbers
- ▶ Call types
- ▶ Labels
- ▶ Network VRU scripts
- ▶ Scheduled targets
- ▶ Routing scripts

These items are therefore capable of being owned by both an Unified CCMP tenant and a remote (Unified CCE) tenant.

Remote Tenant Mappings

Unified CCMP automatically determines which items belong to which remote tenant based on their location in the folder tree. An item which is located anywhere under a folder mapped to a remote tenant is associated with and owned by that remote tenant.

The remote tenant mappings control two Unified CCMP behaviors:

- ▶ The folder that remote tenant owned items are placed in by the importer.
- ▶ How the remote tenant ownership changes when a remote tenant owned item is moved through Unified CCMP.

Remote tenants are mapped to folders from the Equipment Mappings page (see section [“Equipment Mappings Page” on page 39](#)).

Changing the Ownership of an Item

An item’s ownership can be changed in any of the following ways:

- ▶ Moving the item or the folder containing the item to a different Unified CCMP tenant.
- ▶ Moving an item capable of being owned by a remote tenant to a folder located under a different remote tenant mapping.
- ▶ Changing the remote tenant mapping of an item on the remote equipment (for example, Unified CCE).

Changing Ownership by Moving Items

Since the ownership of items is governed by where it is in the folder tree, moving an item can result in a change of remote or Unified CCMP tenant ownership.

The ownership of an item is calculated from the closest remote tenant mapping above the item in the folder tree. If moving an item changes this mapping, the remote tenant ownership is updated and the change is provisioned to the remote equipment.

A change of remote tenant mapping during a move is not allowed if the item is referenced by a customer specific Unified CCE routing script or has a membership to any other items which also have a remote tenant mapping. For example, the user cannot move a label out of a folder which has a remote tenant mapping if it is referenced by a script which has a remote tenant association. To move the label, it must first be removed from the script or alternatively the script should be made visible to all customers using the Unified CCE Script Editor.

Provisioning of scheduled targets is not supported, so any move which requires a change of remote tenant is not allowed. Likewise, if script provisioning is disabled for the Unified CCE, any move of a routing script that requires a change of remote tenant is not allowed.

Items owned by remote tenants for which there are no remote tenant mappings do not have their remote ownership changed unless they are moved into a folder with a different remote tenant mapping.




Importing Remote Ownership Changes

The Data Import service ensures that any remote tenant owned items are correctly located in the folder tree according to the configured remote tenant mappings. If a remote tenant owned item has no corresponding remote tenant mapping, it is placed in the default import location. If the remote tenant of an item is changed on the Unified CCE the importer moves the item according to the defined remote tenant mappings so that the item's folder location continues to reflect the correct remote tenant ownership.





Cluster Configuration Tool Reference







Cluster Configuration Actions

The ICE Cluster Configuration tool supports the following ICE actions.

Icon	Description
 Save	Save any changes to the currently loaded configuration.
 Undo	Undo the last change made to the configuration.
 Redo	Redo the last change made to the configuration

The ICE Cluster Configuration tool also has the following additional actions.

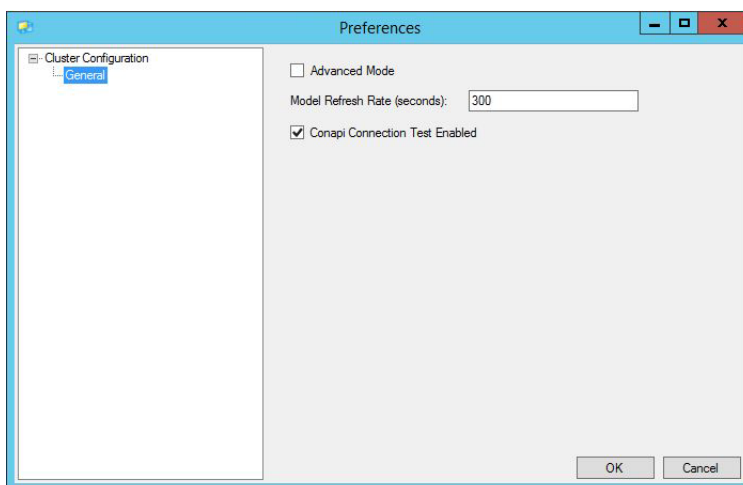
Icon	Description
 Save As	-
 Save As Database	Save the currently open configuration to a database
 Save As File	Save the currently open configuration to an XML file
 Refresh	Refresh the configuration from the current connection (database or file)

Icon	Description
 Validate	Validate the current configuration, and display any validation errors in the Error List pane. Note: Validate does not check connection errors, although the Error List pane does include connection errors at startup. If any connection errors were shown in the Error List pane, they are cleared when you select Validate.
 Open	-
 Open Database	Open configuration from a database.
 Open File	Open configuration from an XML file.
 Create Checkpoint	Create a checkpoint in the current configuration. Allows all changes from a given point to be easily reverted.
 Revert To Last Checkpoint	Revert the state of the configuration to the last checkpoint, reverting and clearing all changes since the checkpoint.

Cluster Configuration Preferences


The ICE Cluster Configuration tool has the following additional preferences.



Preference Name	Description
General: Advanced Mode	Indicates if the current user should be shown advanced properties on the cluster configuration objects within the user interface. This option is not required for day-to-day operations.
General: Connection Monitor Refresh Period	Indicates the rate in seconds at which the connection monitoring system checks the backing store for connection state changes. Default is 5 seconds



Cluster Configuration General Preferences User Interface

Cluster Configuration Filters

Some of the Cluster Configuration pages support a filter function to limit the number of items shown according to a user-specified filter. To access the filter, where available, click the **Show Filter**  button.

The actual filters that you can specify depend on the Cluster Configuration page. Within the filter area, click the **Clear Filter**  button to clear any filters you have specified and click the **Hide Filter**  button to hide the filter options.

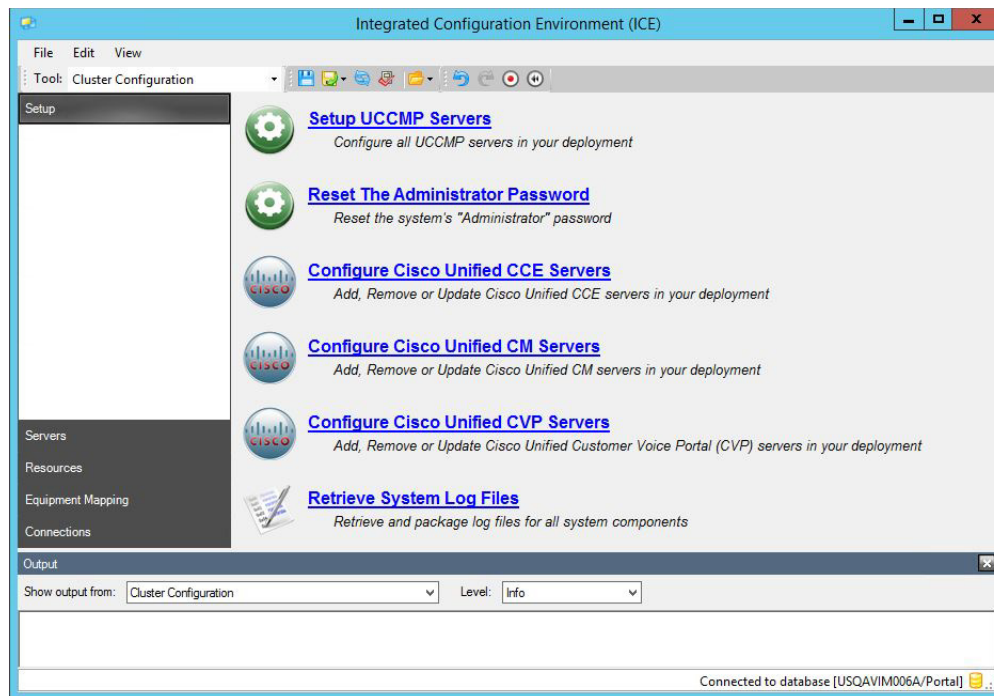
The following Cluster Configuration pages support a filter:

- ▶ Servers page
- ▶ Connections page
- ▶ Resources page

Cluster Configuration User Interface

When you run the Cluster Configuration tool for the first time you are automatically connected to a model using the shared Unified CCMP relational database connection. You are prompted for credentials to connect to the Unified CCMP relational database.

Once connected, you can see the following screen.



Cluster Configuration Initial Interface

On the left-hand side of the main interface there is a navigation menu that allows easy switching between the various configuration pages within the tool. These configuration pages include:

- ▶ **Setup:** Contains high-level wizards that are designed to make day-to-day configuration changes quick and easy.

- ▶ **Servers:** Allows physical servers within the model to be added, removed or updated.
- ▶ **Resources:** Shows the logical resources, physical resources, and physical resource components configured within the model. These items can be added, removed, or updated here.
- ▶ **Equipment Mapping:** Only enabled when connected to an Unified CCMP database. Enables you to create tenants and folders in Unified CCMP and to map equipment like Unified CCE systems to folders for import and provisioning.
- ▶ **Connections:** Allows Unified CCMP component connections to be viewed and edited.

Cluster Configuration Error List Pane

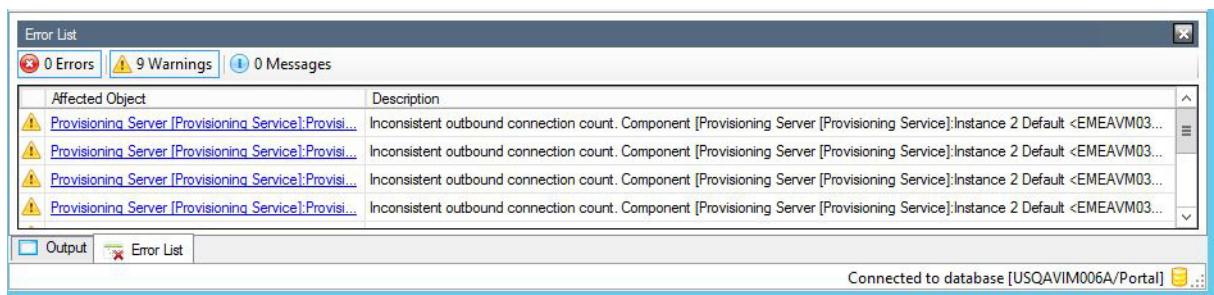
The Cluster Configuration has an additional output pane, the Error List pane. Click the **Error List** tab to view the errors and warnings from Cluster Configuration tool. You can click on the error details to see more information about an error.

Initially, this pane shows the connection errors and warnings (if any) and validation errors and warnings (if any) that were detected at start-up. Click **Save** or **Validate** to update the contents of the Error List pane with the current validation errors and warnings.



Note: When you click **Save** or **Validate**, any connection errors and warnings are cleared from the Error List pane. You can view connection problems at any time on the Connections page (see section [“Connections Page” on page 42](#))

You can click the buttons at the top of the error pane to choose the type of error you want view. See section [“ICE Output Pane” on page 14](#)) for general information about showing and hiding output panes.



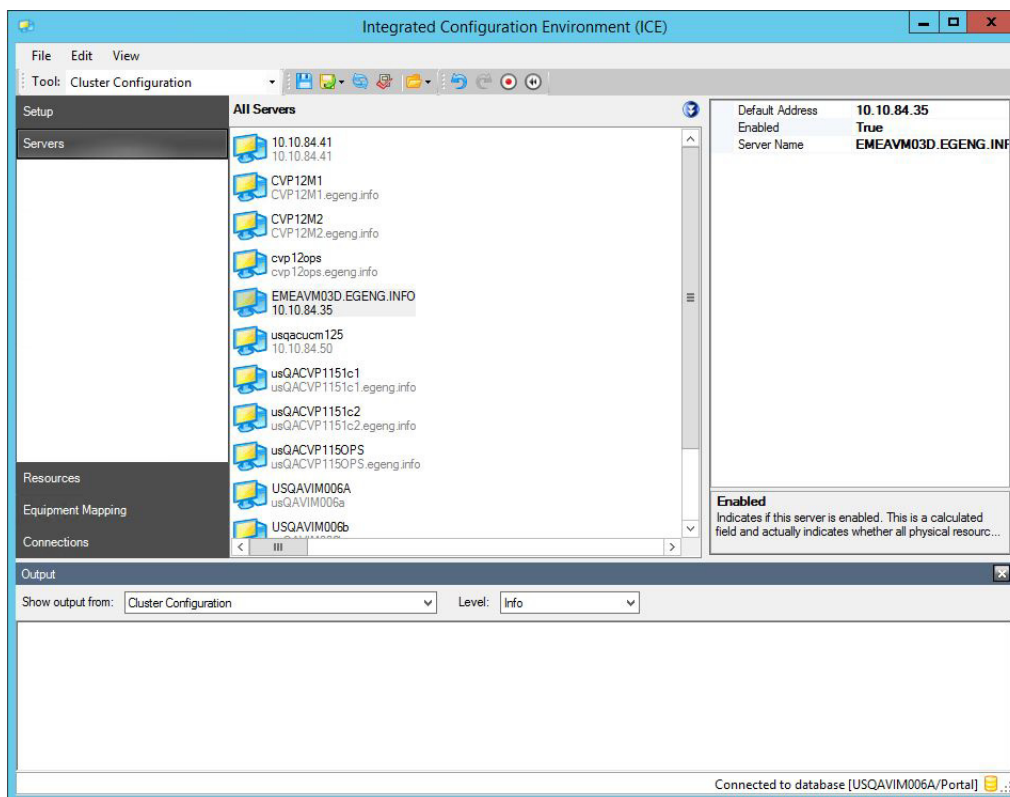
Cluster Configuration Error List Pane

Setup Page

For information about the Setup page in the Cluster Configuration tool, see the Setting Up the Unified CCMP Servers section in the *Installation and Configuration Guide for Cisco Unified Contact Center Management Portal*.

Servers Page

The Servers page within the Cluster Configuration tool enables physical servers within the Unified CCMP deployment to be added, removed, or updated.



Cluster Configuration Servers Page

The Servers page consists of a left and right pane. The left-hand pane contains a list view displaying all the servers configured in the open model. The right-hand pane is a property grid that displays the details of the currently selected server within the list view.




Server objects support the properties described in the following table.


Property Name	Advanced	Description
Default Address		The default address that is used when services within the Unified CCMP deployment connect to this server. This may be a host name or IP address.
Display Name	✓	A name used to represent this object when it is referred to in logs, performance counters etc.
Enabled		Indicates if this server is enabled. This is a calculated field and actually indicates whether all physical resource components on this server are enabled. Changing this value updates the enabled flag of all physical resource components on this server.

Property Name	Advanced	Description
Id	✓	A unique ID used to represent this object on the backing store.
Server Name		The machine name for this server. This is used to identify an Unified CCMP service's machine within the cluster model and should match the value returned by SQL server using @@SERVERNAME or SYSTEMPROPERTY('MachineName'). Viewing Computer properties on a Windows based computer and looking at the Computer Name property can typically find the correct value.
System	✓	Indicates if the Unified CCMP system installers created this object.

Click **Add New** within the list view to add a new server to the model. Clicking this automatically creates a new server in the model and select it ready for editing.

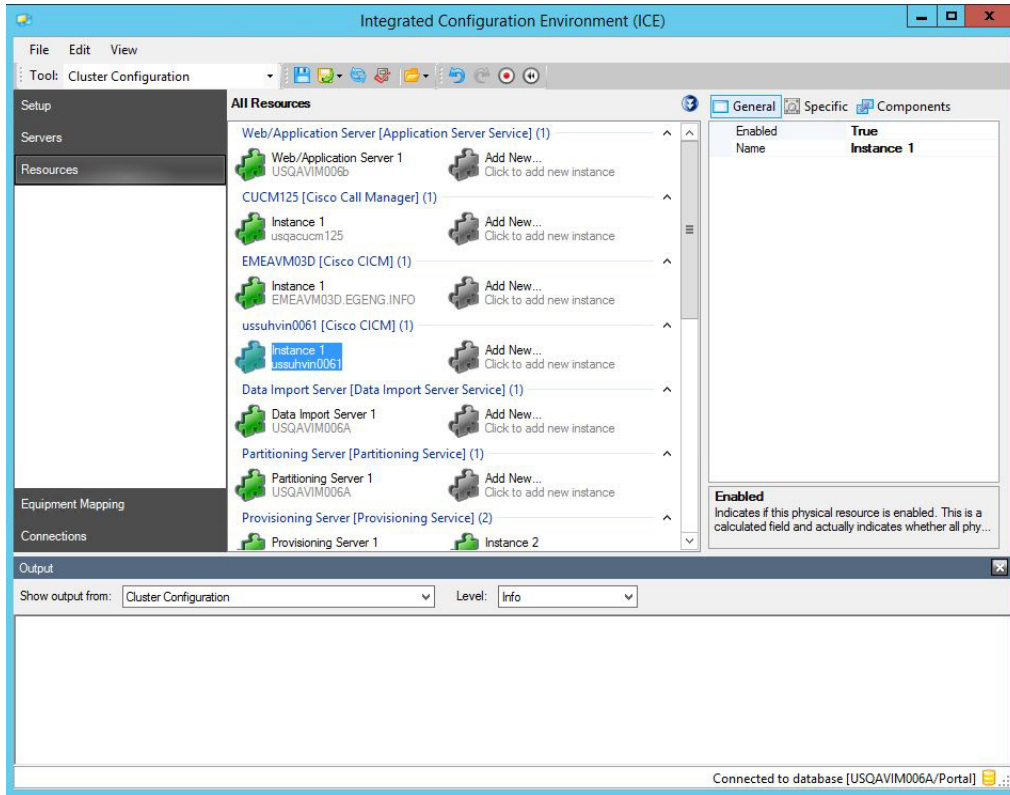
Right-click in the Servers page to see a shortcut menu with the following functions.

Icon	Description
 Add Server	Add a new server to the model.
 Remove Server	Remove the selected server from the model.
 View	Change the display style of the list view.

The Servers page includes a filter which enables you to filter by server name or address. Click **Show Filter**  to expand the filter area if it is not currently shown.


Resources Page

The Resources page within the Cluster Configuration tool enables logical resources, physical resources, and physical resource components within the model to be added, removed or edited.



Cluster Configuration Resources Page

The Resources page consists of a left and right pane, very similar to the layout of the Servers page. The left-hand pane contains a list view displaying all of the logical and physical resources configured in the open model. The right-hand pane is a property grid that displays the details of the currently selected object within the list view.

The Resources page includes a filter which enables you to filter by resource group type, resource type, server or resource name. Click **Show Filter**  to expand the filter area if it is not currently shown.

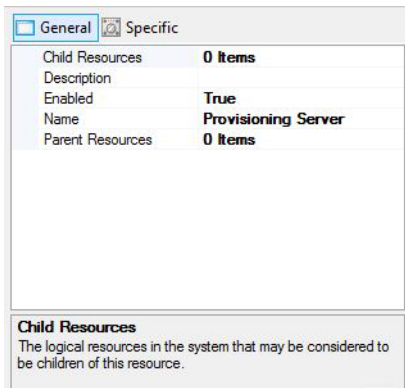
The list view on the Resource page contains multiple groups. Each group represents an individual logical resource within the model. Within each group there are one or more items, each representing a physical resource within that logical resource.



Example Logical Resource List View Group

Logical Resources

You can select a logical resource by clicking on the group header text. Selecting a logical resource displays its properties in the property grid pane.



Property Grid View for Logical Resource

The property grid for a logical resource has two tabbed sections - **General** and **Specific**. The **General** tab contains properties that are common to several logical resources. The **Specific** tab contains properties that relate to the specific type of logical resource that has been selected.

General Tab

Logical resource objects may support the following basic properties through the General tab.

Property Name	Advanced	Description
Cache Enabled Resource Types		The resource types that are cached by this server to enhance performance (applies to App/Web server and Mediator server only).
Child Resources		The logical resources in the system that are children of this resource.
Default Import Enabled Resource Types		The resource types that are imported by default. This can be overridden on a specific item of remote equipment if required (applies to Data Import Server only).
Description		A short description of the logical resource.
Display Name	✓	A name used to represent this object when it is referred to in logs, performance counters etc. (Read-only)
Enabled		Indicates if this logical resource is enabled. This is a calculated field and actually 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.
Id	✓	A unique ID used to represent this object on the backing store. Read only.

Property Name	Advanced	Description
Import Enabled Resource Types		The resource types that are imported from this item of remote equipment (applies to remote equipment objects only). The settings here override the settings in Default Import Enabled Resource Types. When a default setting is overridden for a resource type, that resource type is shown in bold.
Name		A unique name for this logical resource.
Parent Resources		The logical resources in the system that may be considered to be parents of this resource.
Provisionable		Whether provisioning has been enabled for this logical resource (applies to remote equipment only). Must not be enabled/checked for PCCE systems as Resource Management is not supported for PCCE.
System	✓	Whether this object was created by the system installers. Read only.
Version	✓	The source system version for this logical resource.

Specific Tab

The derived logical resource properties for the standard built in resource types are described in the following tables.

Cisco CICM

Property Name	Advanced	Description
Active Directory Global Catalog Domain or Server		The Active Directory Global Catalog Domain or Server for active directory access.
Active Directory Path		The active directory location from which users can be selected to provide supervisors with WebView login credentials. (Only shown if a ConAPI component is configured for the physical resource)
Anonymous		No authentication is performed.
CSV Export Enabled		Indicates whether data imported from the resource is enabled for export into CSV files via standard CSV writers.
Default Domain Name		The default domain name configured for the UCCE.
Delegation		Enables Active Directory Services Interface (ADSI) to delegate the user's security context, which is necessary for moving objects across domains.
Deployment Type		The deployment type for this CICM.

Property Name	Advanced	Description
Domain Password		The password to use when connecting to active directory if "Secure Authentication" has been specified. (Only shown if a ConAPI component is configured for the physical resource)
Domain User Name		The user to impersonate when connecting to active directory if "Secure Authentication" has been specified. (Only shown if a ConAPI component is configured for the physical resource)
Encryption		Attaches a cryptographic signature to the message that both identifies the sender and ensures that the message has not been modified in transit.
Fast Bind		Specifies that ADSI will not attempt to query the Active Directory Domain Services objectClass property.
Last Dimension Import Config Change Date	✓	The value of the ControllerConfigChangeTime field in the AWControl table on the AW the last time a dimension import ran for this resource. (Read-only)
Last Member Import Config Change Date	✓	The value of the ControllerConfigChangeTime field in the AWControl table on the AW the last time a member import ran for this resource. (Read-only)
Multi Media Enabled		Indicates if multimedia reskilling is supported for this CICM. (Only shown if a ConAPI component is configured for the physical resource)
Person Minimum Password Length		The minimum password length configured for this ICM. (Read-only)
Primary Domain Server		Primary domain server for active directory access. (Only shown if a ConAPI component is configured for the physical resource)
Purge Items on Delete		Indicates if items should be automatically purged on delete (or only marked for delete) on ICM. (Only shown if a ConAPI component is configured for the physical resource)
Read Only Server		This flag indicates that a writable server is not required for a serverless binding.
Script Lock User Name		User name for use when locking routing scripts for edit. (Only shown if a ConAPI component is configured for the physical resource)
Script Provisioning Enabled		Indicates if script provisioning is enabled for this ConAPI resource. (Only shown if a ConAPI component is configured for the physical resource)
Sealing		Encrypts data using Kerberos. The "Secure Authentication" flag must also be set to use sealing.
Secondary Domain Server		Secondary domain server for active directory access. (Only shown if a ConAPI component is configured for the physical resource)

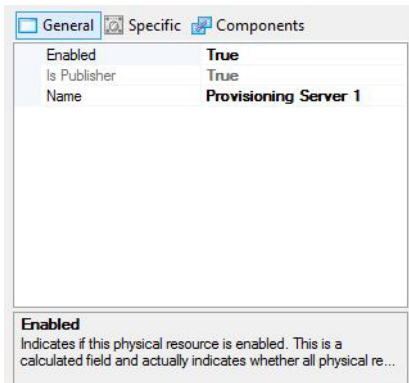
Property Name	Advanced	Description
Secure Authentication		Indicates whether a specific user should be impersonated when contacting to active directory. (Only shown if a ConAPI component is configured for the physical resource)
Server Bind		If your ADsPath includes a server name, specify this flag when using the LDAP provider.
Signing		Verifies data integrity to ensure that the data received is the same as the data sent. The "Secure Authentication" flag must also be set to use signing.
SSL		Secure Sockets Layer (SSL) encryption. Attaches a cryptographic signature to the message that both identifies the sender and ensures that the message has not been modified in transit.
SSO Enabled		Indicates if single sign on (SSO) is enabled for the UCCE resource.
Supervisor Domain Account Required		Select if the Supervisor Domain Account is required.
Time Zone		The timezone for the ICM.
Time Zone Display Name		Display name for the ICM timezone. (Read-only)

Data Import Server Service

Property Name	Advanced	Description
Import Cycle Delay	✓	The minimum delay between import cycles (in minutes).

Physical Resources

You can select an individual physical resource by clicking on physical resource in the list view. Selecting a physical resource displays its properties in the right-hand property grid pane.



Property Grid View for Physical Resource

The property grid for a physical resource is broken into three tabbed sections; General, Specific, and Components. The General tab contains properties that are common to all physical resources. The Specific tab contains properties that relate to the specific type of physical resource that has been selected. The Components tab displays details for each of the physical resource components associated with the currently selected physical resource. For example, when viewing a CICM resource, the Components tab may contain entries for the AW, HDS and ConAPI components.

Properties of Physical Resource Objects

General Tab

Physical resource objects support the following basic properties through the General tab.

Property Name	Advanced	Description
Display Name	✓	A name used to represent this object when it is referred to in logs, performance counters etc. (Read-only)
Enabled		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 resource components in this physical resource.
Id	✓	A unique ID used to represent this object on the backing store. (Read-only)
Is Publisher		Indicates if this physical resource is considered a publisher for replication within the logical resource.
Name		A unique name for this physical resource.
System	✓	Indicates whether this object was created by the system installers (read-only).

Specific Tab

Derived, resource type specific properties are exposed through the Specific tab of the property grid. The derived physical resource properties for the standard built in resource types are described in the following tables.

Application Server Service

Property Name	Advanced	Description
Notification Enabled		Indicates if this application server is responsible for raising resource notification events.

Data Import Server Service

Property Name	Advanced	Description
Last Import End	✓	The time when the last dimension import cycle ended. (Read-only)
Last Import Exception Count	✓	The number of errors that occurred on the last import cycle. (Read- only)
Last Import Start	✓	The time when the last dimension import cycle started. (Read-only)
Last Import Type	✓	The type of the last import cycle. (Read-only)

Relational Database

Property Name	Advanced	Description
Prefix Management Enabled		Whether this database server is responsible for running the prefix management scheduled job.
Purge Enabled		Whether this database server is responsible for running the purge scheduled job.
Scheduling Enabled		Whether this database server is responsible for running schedules. Setting this flag enables scheduling for all application servers that are connected to this database as their primary.

Components Tab

The Components tab on the property grid displays the properties for all physical resource components that belong to the selected physical resource. The following table lists the component types supported and required for each of the built-in physical resource types.

Physical Resource Type	Component Type	Required	Description
Application Server Service	Default	✓	
Cisco Call Manager	Default	✓	

Physical Resource Type	Component Type	Required	Description
Cisco CICM	AWS	✓	The Admin Workstation component. Used for dimension/member import.
	ConAPI		The Cisco ConAPI server. Used for provisioning changes to CCE.
	HDS		The historical data server. Used for fact data import.
	UnifiedConfigWebService		Unified Config Web Service Component.
Cisco CVP Call Server	Default	✓	
Cisco CVP Reporting	Callback	✓	The database on Cisco CVP that is the source for Server courtesy call-back data.
	Core	✓	The database on Cisco CVP that is the source for historical and real-time data.
Data Import Server Service	Default	✓	
Partitioning Service	Default	✓	
Provisioning Service	Default	✓	
Relational Database	Default	✓	

Properties of Physical Resource Components

All physical resource components support the following properties.

Property Name	Advanced	Description
Application Name	✓	Application name used for this component when it is the source of a SQL connection. Can be used to identifier this resource in a SQL profile. (Read-only)
Display Name	✓	A name used to represent this object when it is referred to in logs, performance counters etc. (Read-only)
Id	✓	A unique ID used to represent this object on the backing store. (Read-only)
Inbound Connections		All connections to this component from other systems.
Outbound Connections		All connections from this component to other systems.

Property Name	Advanced	Description
Server		The server on which this component resides.
System		Indicates whether this object was created by the system installers. (Read-only)

In addition, the following derived properties are supported.

Cisco CICM: AWS

Property Name	Advanced	Description
Catalog	✓	The database catalog name.
Custom Connection Test		SQL query containing custom connection test logic for this component. The query should return a single row with a BIT column indicating the state of the component.

Cisco CICM: HDS

Property Name	Advanced	Description
Catalog		The database catalog name.
Custom Connection Test	✓	SQL query containing custom connection test logic for this component. The query should return a single row with a BIT column indicating the state of the component.

Cisco CICM: UnifiedConfigWebService

Property Name	Advanced	Description
Ignore Certificate Warnings		Indicates whether to ignore certificate warnings from this web service instance.

Provisioning Service: Default

Property Name	Advanced	Description
Auto Restart on Critical Config Change		Indicates if the hosting service should be automatically restarted when a critical configuration change takes place.

Relational Database: Default

Property Name	Advanced	Description
Catalog		The database catalog name.
Custom Connection Test	✓	SQL query containing custom connection test logic for this component. The query should return a single row with a BIT column indicating the state of the component.

Logical resources, physical resources and physical resource components may be added/removed from the model via a context menu that can be accessed by right-clicking on the main list view area.

Managing Connections

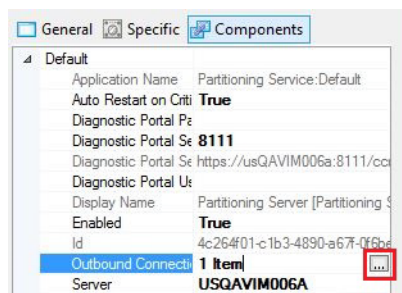
Connections can be created between two physical resource components within the cluster configuration model. Components may support inbound connections (that is other components may connect to them), outbound connections (that is, they can connect to other components) or both inbound and outbound connections. Each physical resource component type has a connection type associated with it that defines how other components should connect with it.

Unified CCMP supports the following connection types.

Connection Type	Description
Microsoft SQL Server	Provides support for connections to a Microsoft SQL Server database.

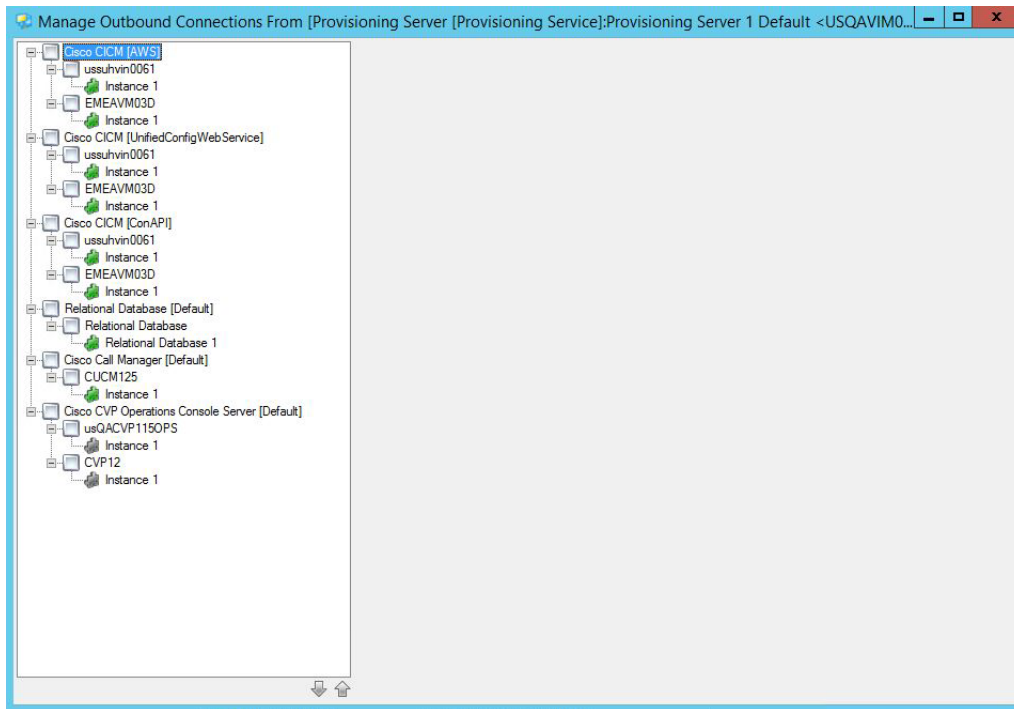
Editing Connections

Connections can be added, removed or updated by clicking on the **Inbound Connections** or **Outbound Connections** property on a component entry in the property grid. To edit connections from the selected component to other components use the **Outbound Connections** property. To edit connections to the selected component from other components use the **Inbound Connections** property. These properties are only visible on components where connections are supported.



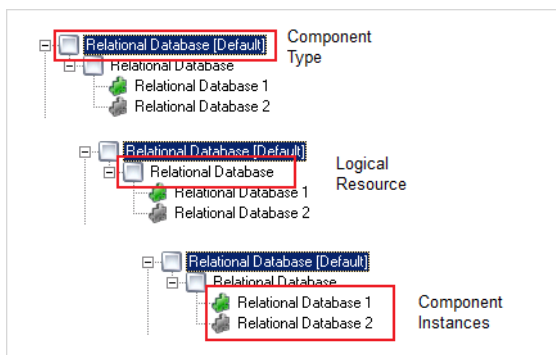
Edit connection

For example, in the Manage Outbound Connections from dialogue box, you can view two main panes. The left-hand pane contains a tree view showing all the components that are available to connect to or from.



Manage Outbound Connections Dialog Box

The tree view groups all the available components by physical component type and logical resource.



Tree View

When a connection exists to a component instance, the icon on the component is highlighted in green. When no connection exists, the icon is grayed out.

Within each logical resource grouping, the component instances in the logical resource are listed in order of cost. The cost of a connection is an indication of the resources it has available to it and how well it performs – connections with a lower cost can be expected to perform better than connections with a higher cost. For example, it may be more efficient to make a connection to a server that is co-located with the server requesting the connection than to make a connection to a server in another country. In this case, you would define the local server as having a lower cost than the server in another country.

Unified CCMP uses the lower cost connection if it is available. For example, if a Provisioning server was connected to a dual sided database then one of the two sides would be the preferred (lowest cost) connection and the other would be the redundant (highest cost) connection.



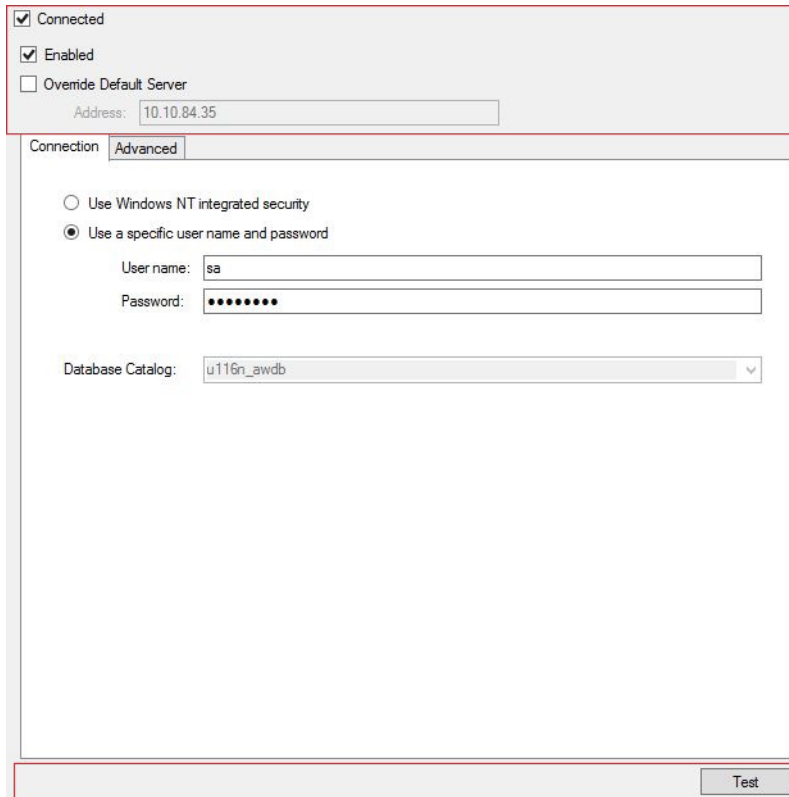
Note: Connections are tested within the context of the ICE application so tests may provide inaccurate results. When the connections are used by the Unified CCMP system they are created on remote servers and subject to any firewalls, network address translation or environment issues that may exist on those servers. The connections also are established using the windows credentials of the service rather than the credentials being used to run the ICE application.

To edit a connection:

1. In the list view, select the required provisioning server.
2. In the property grid pane, click the Components tab.
3. Click on the **Outbound Connections** property.
4. Click on the ellipsis beside the **Outbound Connections** property. This displays the Manage Outbound Connections From window.

Managing Cost of Connections

When a component is selected in the tree view, the right-hand pane automatically populates with the details for the connection. The connection details pane is broken into three sections; a common header, a connection type specific properties page and a generic footer.



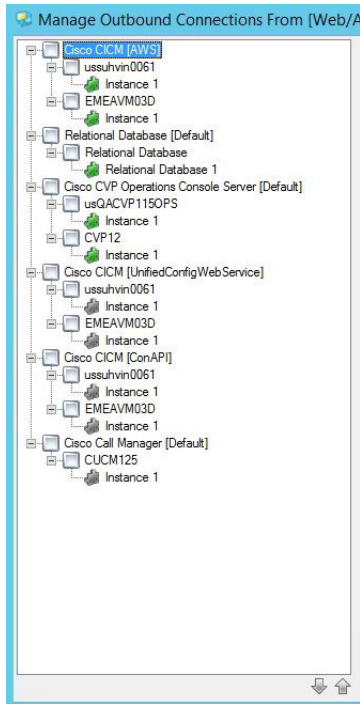
The screenshot shows a 'Connection Details Pane' with a header section containing three checkboxes: 'Connected' (checked), 'Enabled' (checked), and 'Override Default Server' (unchecked). Below these is an 'Address' field with the value '10.10.84.35'. The main pane is divided into 'Connection' and 'Advanced' tabs. The 'Advanced' tab is active, showing two radio buttons: 'Use Windows NT integrated security' (unchecked) and 'Use a specific user name and password' (checked). Below these are fields for 'User name' (containing 'sa') and 'Password' (masked with dots). A 'Database Catalog' dropdown menu is set to 'u116n_awdb'. A 'Test' button is located at the bottom right of the pane.

Connection Details Pane

- ▶ The common header consists of the following.
 - **Connected:** Indicates if a connection exists to the selected component. Checking this box creates a connection. Clearing this box deletes the connection.
 - **Enabled:** Indicates if this connection is enabled. Disabled connections are not used by the Unified CCMP monitoring service.
 - **Override Default Server:** By default, the host name for the server on which component resides is selected from the server objects **Default Address** property. However, there may be situations where the actual host name used for a specific connection between two components needs to be altered (for example when using network address translation). In these situations, the host name can be set by checking the **Override Default Server** box and entering the new host name in the **Address** field.
- ▶ The middle pane contains connection type specific properties. For example, when editing a SQL connection this pane contains settings for the authentication mode and database catalog etc. For web service connections, it prompts for a URL.
- ▶ The common footer contains the **Test** button. Clicking this button tests the connection using the details provided in the details section.

To change the relative cost of connections:

- ▶ Select a component in the tree view and click the up or down arrow at the bottom right of the pane to reduce or increase the cost.



Change the relative cost of connections

Equipment Mappings Page

The Equipment Mapping tab of the ICE Cluster Configuration tool enables you to create Unified CCMP tenants and folders, and to specify the way that resources on the contact center are mapped to Unified CCMP.

The Equipment Mappings page is divided into three vertical sections.

- ▶ Folder Tree section
- ▶ Source Equipment section (shown when an item is selected in the folder tree)
- ▶ Association Options section (shown when an item is ticked and highlighted in the source equipment section).

To configure your equipment mapping, in the Cluster Configuration tool, select **Equipment Mapping** in the left-hand navigation pane.

Folder Tree Section

This section enables you to create new tenants and folders in the Unified CCMP Folder Structure. To create a new tenant or a folder, right-click on the location in the tree where you would like to create the item and select **Add Tenant** or **Add Folder**.



Note: Tenants can only be created under the root folder. Folders can be created anywhere in the tree. A Tenant is a special folder that maintains ownership of an item. For example, in a hosted environment, the host's customers map directly to individual tenants, each of which is assigned their own individual resources, for example, Agents, Teams, Call Types etc.

Right-clicking and selecting the **Refresh** option refreshes the folder structure from the database, reflecting any changes that may have been made through the Unified CCMP web application.

Right-clicking and selecting the **Properties** option displays a window in which an Azure AD directory ID can be mapped to the tenant to allow the use of company credentials to authenticate if synchronized with Azure. For more information about setting up Azure AD authentication, see the *Unified CCMP Installation and Configuration Guide*.

Source Equipment Section

This section lists all the configured source equipment. If none are configured then this list is empty and you are not able to do any associations.

When you select one of the items of configured equipment in the list, you can see options to map the resources belonging to that equipment to the selected folder in the Association Options Section.

Association Options Section

This section offers a list of association options between the folder or tenant in the folder tree and the source equipment. There are two types of association options.

- ▶ **Default Import Location:** All resources from the highlighted contact center equipment are imported into the selected folder or tenant in Unified CCMP.
- ▶ **Customer Resource Mapping:** Allows more control over the import process. You can specify the items on the highlighted contact center equipment to be placed in the selected folder or tenant in Unified CCMP. If you select this option you can:
 - Click **+** to add a new customer resource mapping that defines the resource types and the specific resources of that type to be mapped to the selected import location. Select the resource type from the Type dropdown list (one of **Peripheral**, **Routing Client**, **Media Routing Domain**, and **Remote Tenant**) then select the specific item of that type that you want to map from the **Resource** dropdown

list. Click **OK**. Repeat to map other customer resources on this item of contact center equipment to the specified import location.



Note: Multiple Global Catalogs for different customer definition mapping should not be configured if a default domain for Unified CCE has been configured. Global Catalog mapping overrides the default domain configuration, which then requires that full valid values for UPN or SAM format must be provided when saving supervisor agents. For more information about default domains and how to configure supervisor agents, see the *Unified CCMP User Guide*.

- Click **✗** to delete an existing customer resource mapping.

If **Customer Resource Mapping** is selected, then any resources on the contact center equipment that are not associated with the selected mapping are placed in the source equipment subfolder under the **Unallocated** folder.

Important things to note:

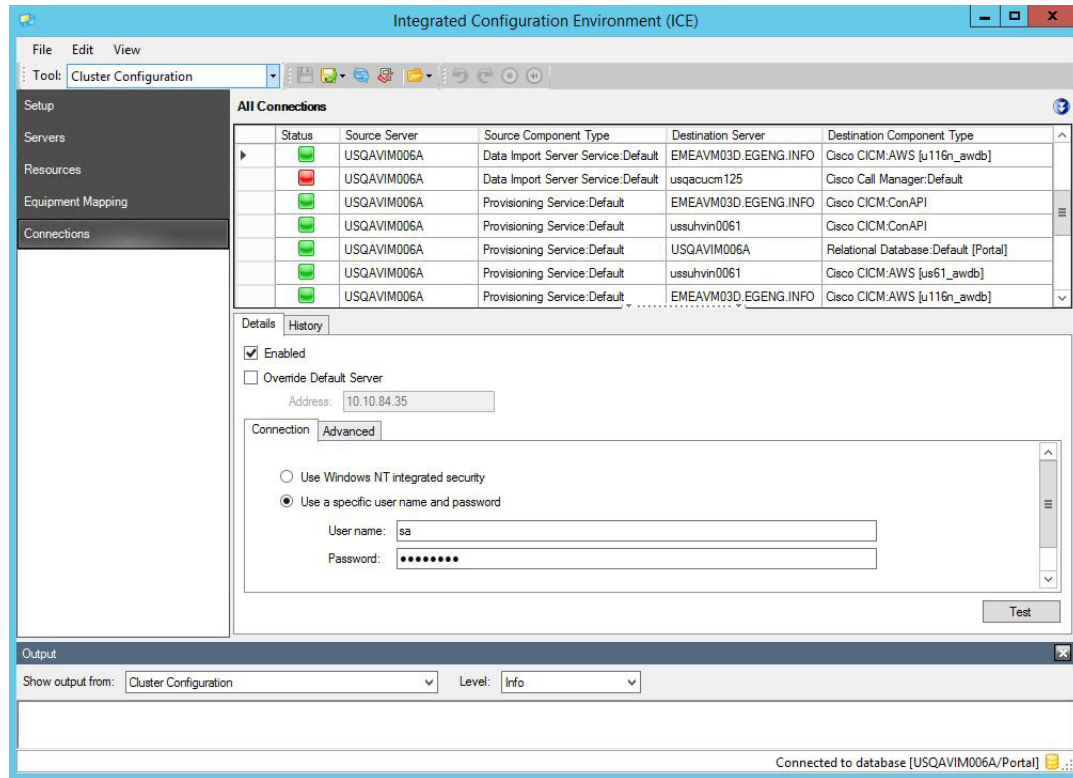
If you want to use the **Customer Resource Mapping** option, you are not able to configure this until you have imported the customer resources you want to use to define the mappings.

In this case, for the first import, do not select the **Default Import Location** option, as once you have selected this, the items from the remote equipment are imported to that location and cannot be re-imported. Instead, for the first import, do not specify any import location, so everything is imported into the **/Unallocated** folder. Once the customer resources have been imported, you can specify the customer resource mapping you require, and the items in the **/Unallocated** folder are moved to the required locations.

The **Customer Resource Mapping** is currently only valid for Cisco Unified CCE Resources. The list is populated with all the customer definitions available on the selected Cisco Unified CCE resource.

Connections Page




The Connections page within the Cluster Configuration tool enables all configured connections in the system to be edited and monitored.



Cluster Configuration Connections Page

The Connections page consists of a resizable top and bottom pane. The top pane is the connection status monitor and shows the status of all the connections configured in the open model. The bottom pane displays the details for the currently selected connection in the list view.

Each row in the connection status monitor has the following columns.

Column	Meaning
Status	An icon representing the status of the connection. The following options exist: <ul style="list-style-type: none"> ▶  Available ▶  Unavailable ▶  Disabled
Source Server	The name of the physical server that this connection is being established from.
Source Component Type	The display name for the physical resource component type that this connection is being established from.

Column	Meaning
Destination Server	The name of the physical server that this connection is being established to.
Destination Component Type	The display name for the physical resource component type that this connection is being established to.

Click the column headers in the connection status grid to sort the view by the selected column. Click on an entry in the grid (a source or destination server, or a source or destination component type) to go to the details for that item.

The row headers on the connection status grid may optionally show an **Alert** icon (🔴) if there is a potential problem with the connection. Hovering over the alert icon displays a tool tip explaining the reason for the alert. The most common cause of an alert being displayed is to indicate that the connection status has not been updated for more than 5 minutes. This usually indicates that the source service is not running or is failing to connect with the Unified CCMP database. The source service log files should be used to investigate the cause of the problem.

- ▶ To show the server details for a connection, hold down **Ctrl** and click on the connection.
- ▶ To maximize the status monitor and show the Details and History tabs, click on the **Expand** icon on the splitter bar.

Connection status is automatically refreshed from the database. By default, the status is refreshed every 5 seconds but this can be modified via the **Cluster Configuration** preferences (see section “[Cluster Configuration Preferences](#)” on page 21)

The Connections page includes a filter which enables you to filter by resource type, component type and server, for both the connection source and the connection destination. Click **Show Filter** (🔍) to expand the filter area if it is not currently shown.

Diagnostic Portal Support

The ICE Cluster Configuration tool enables you to access the diagnostic portal and view diagnostic logs for the Unified CVP, Unified CCE and Unified CCMP servers.

To view the logs for a server:

- ▶ Configure the diagnostic portal for the server (you only need to do this once).
- ▶ Select the required log and logging period to access the required logs.

Configuring the Diagnostic Portal

To configure the diagnostic portal for a server:

1. On the server you want to configure, identify a user name and password for an authorized user of the Diagnostic Framework. This user must be a trusted domain user in the **CONFIG** domain security group of the server being configured.
2. In the ICE Cluster Configuration tool, select the **Resources** tab.

3. Click on the server for which you want to configure the diagnostic portal.
4. In the right hand pane, select the **Components** tab.
5. Set the **Diagnostic Portal User Name** and **Diagnostic Portal Password** fields to the user name and password of the authorized user you identified above.
6. Select **File > Save** or click the **Save** button.



Note: For more information about the diagnostic portal see Serviceability Best Practices Guide for Cisco Unified ICM/Unified CCE & Unified CCH, Chapter 10, Unified ICM/Unified CCE Diagnostic Tools.

Accessing the Diagnostic Logs

To access a diagnostic log:

1. Right-click the server instance and from the context menu, select **Components**, then the component, then one of:
 - **View Logs to view the logs**
 - **View Trace Logs to view the trace logs**
2. The Diagnostic Logs window is shown. In the Diagnostic Logs window, select the type of log you want to view from the drop down list in the top left of the window.
3. Specify the **From Date** and **To Date** to filter the results by a date range, then click **Fetch Result** to get a list of all available logs of that type within the selected date range.
4. The bottom left pane may show the logs that match the filter, or may show servers or folders containing logs that match the filter. Double-click on the server or folder to view the contents of that item and drill down to the log files. When you locate the log file you want to view, double click on the log file to view the contents in the Raw Data tab of the right-hand pane. For CSV log files, you can also select the CSV tab of the right-hand pane to view the log file in CSV format.



Note: To view diagnostic logs, you must previously have configured the diagnostic portal for this server as described above.

3 Replication Manager

- ▶ [About Replication Manager](#)
- ▶ [Starting Replication Manager](#)
- ▶ [Configuring Replication](#)
- ▶ [Disabling Replication](#)
- ▶ [Monitoring Replication](#)
- ▶ [Identifying Replication Errors](#)
- ▶ [Performance Considerations](#)

About Replication Manager

The Unified CCMP Replication Manager enables you to manage SQL Server Replication between Unified CCMP databases and Microsoft Reporting Services Report Server databases.

The Replication Manager has two tabs:

- ▶ **Setup:** Used to configure and disable SQL Server replication between the Unified CCMP databases, and optionally, the Report Server databases.
- ▶ **Monitor:** Used to monitor general health of configured replication, at to start and stop replication agents.

The Replication Manager should typically be run on the Unified CCMP database publisher (side A) server. The user running the tool must be a Windows administrator on all the servers that take part in replication.



Note: To use the Replication Manager, the Unified CCMP databases and, optionally, the Microsoft Report Server databases must be configured as dual sided.

The Replication Manager Setup Tab

The Replication Manager Setup tab enables you to configure or disable SQL Server Replication. It shows the configured primary database and the distributor server properties.

The initial configuration is derived from the values set in ICE Cluster Configuration. If any of the values are modified, the configuration must be saved before replication setup can continue.

Unified CCMP Database Server Properties

This section shows the publisher and subscriber Unified CCMP databases. The following information is available:

- ▶ **Publisher:** The publisher database.
 - **Server Name:** The name of the Database Server. This is fixed and cannot be changed using the ICE Replication Manager.
 - **Catalog Name:** The name of the Unified CCMP database. It is recommended that the default value is used, but if the name is modified, then an Unified CCMP database with the new name must already exist on the corresponding database server.
- ▶ **Subscriber:** The subscriber database.
 - **Server Name:** The name of the Database Server. This is fixed and cannot be changed using the ICE Replication Manager.
 - **Catalog Name:** The name of the Unified CCMP database. It is recommended that the default value is used, but if the name is modified, then an Unified CCMP database with the new name must already exist on the corresponding database server.

Distributor Properties

This section shows the SQL Server Replication distributor properties. By default the distributor is created on the subscriber Unified CCMP Database Server. In most cases the default values are valid and should be used.

The following information is available:

- ▶ **Server Name:** The name of the subscriber server hosting the database as configured using ICE Cluster Configuration.
- ▶ **Catalog Name:** The name to be assigned to the distribution database. The recommended default is **distribution_portal**.
- ▶ **Override Distributor Admin Password:** Select to override the auto-generated replication password which is used to establish connectivity. The auto-generated password is 14 characters long, and contains alphanumeric characters (both upper and lower case) and a special character. If this does not meet the complexity requirements of the server then select this option and specify a password of your choice.



Note: This password is a one-off password used to set up replication. It is not stored and does not need to be recorded by the user.

- ▶ **Data Folder:** The folder path on the distributor server where the data file for the distribution database is created.



Note: If you are setting up replication after performing an upgrade, be particularly careful with the Data Folder path, as it may be different from the value used in previous versions. Make sure you use the path that was specified when the database was set up.

- ▶ **Log Folder:** The folder path on the distributor server where the transaction log file for the distribution database is created.
- ▶ **Distribution Share:** The distribution share folder where replication snapshot files are generated.






The Replication Manager Monitor Tab

The Monitor tab shows the replication status and information about the data that is being copied from the publisher to the subscriber. It enables you to monitor the general health of the replication. It can also be used to start and stop various replication agents.

Monitor Panes

The Monitor tab contains four panes:

- ▶ Publications (top left) lists the publisher servers and the publications on each publisher that need to be shared with the subscribers.
- ▶ Subscriptions and Agents (top right) shows the subscriptions to a publication and the replication agents associated with a publication. This pane has two tabs:
 - Subscriptions shows the subscriptions to the selected publication. Right-click on a subscription to start or stop the subscription.
 - Agents shows the replication agents associated with the selected publication. Right-click on a replication agent to start or stop the agent.
- ▶ Sessions (bottom left) shows all sessions for the selected publication and replication agent in the last 24 hours.

- ▶ Actions (bottom right) shows the activity for the selected session. The status icons are:
 -  **Unknown**
 -  **Running**
 -  **Completed**
 -  **Retry**
 -  **Error**

Information in the Monitor tab is refreshed every five seconds.

Starting Replication Manager

To start the Replication Manager:

1. Launch Integrated Configuration Environment (installed as part of Unified CCMP). In the Database Connection dialog box, set:
 - **Server Name:** Enter the name of the primary database server.
 - **Database Name:** Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this is **Portal**.
 - **Authentication:** Select **Windows Authentication**.
2. Click **OK**. The ICE Cluster Configuration tool starts by default.
3. In the **Tools** dropdown, select **Replication Manager**. The Replication Manager tool is displayed:
 - If SQL Server replication is not currently configured, the Replication Manager tool starts in the Setup tab (see section “[The Replication Manager Setup Tab](#)” on page 46)
 - If SQL Server replication is configured, the Replication Manager tool starts in the Monitor tab (see section “[The Replication Manager Monitor Tab](#)” on page 47)

Configuring Replication

To configure replication:

1. In the Replication Manager, select the Setup tab and click **Configure**. This process may take several minutes.
2. Once replication has been configured, the Replication Manager automatically switches to the Monitor tab, which enables you to monitor the replication process.

Disabling Replication

To disable replication:

1. In the Replication Manager, select the Setup tab and click **Disable**. This may take several minutes.
2. When replication has been disabled, a confirmation message is displayed.

Monitoring Replication

To monitor replication for a publication, in Replication Manager, select the **Monitor** tab and select a publication in the top left pane. The subscriptions and replication agents associated with the selected publication are listed in the top right pane in the respective tab.

The **Subscriptions** tab shows all the subscriptions to the selected publication. It helps answer the following questions

- ▶ Which subscriptions are slow?
 - This shows the latency of replication from publisher to the subscriber.
- ▶ Is the replication system healthy?
 - The grid shows status icons for warnings and error for subscriptions that require attention.

The **Agents** tab displays the agents that are used by the selected publication. This tab shows the following agents:

- ▶ The Snapshot Agent is shown for all publications
- ▶ The Log Reader Agent is shown for transactional publications Base and NonQueued.
- ▶ The Queue Reader Agent is shown for transactional publication Base only.

You can use the Monitor tab to start and stop the Subscriptions and Replication Agents. To start or stop, right-click on the selected subscription or agent and select **Start** or **Stop**.

You can view the session details for a Subscription or an Agent in the two bottom panes. Select the Subscription or Agent in the top right pane. The bottom left pane shows all the sessions for the selected Subscription or Agent in the last 24 hours. It shows the following details for each session:

- ▶ **Status:** The status of the session.
- ▶ **Start Time:** When the session was started.
- ▶ **End Time:** When the session stopped. This is set only for sessions that are not currently running.
- ▶ **Duration:** The total duration for each session.

The bottom right pane shows the SQL Server Replication actions performed for a replication session. To see the actions for a replication session, select the replication session in the bottom left pane.

Identifying Replication Errors

The Monitor helps to identify replication errors that have occurred in replication. If an error has occurred in a subscription or an agent, the respective subscription or agent status icon shows an error.

Select the subscription or agent that shows the error. Selecting the subscription or agent shows their sessions. If an error occurred during a session, the session shows an error icon. Select the session with the error to see the actions. The actions describe the nature of the error in the action message.

Performance Considerations

Each time the information in the Monitor tab refreshes, it requests data from the underlying replication system. These additional requests may sometimes affect the overall performance of SQL Server Replication, especially on busy systems. As a result, it is recommended that the Monitor should not be left running for long periods of time.



Failover Manager

- ▶ [About Failover Manager](#)
- ▶ [Preparing to Use the Failover Manager](#)
- ▶ [Starting the Failover Manager Tool](#)
- ▶ [Performing a Failover Operation](#)
- ▶ [Performing Provisioning Service Failover](#)
- ▶ [Performing Data Import Service Failover](#)

About Failover Manager

The Unified CCMP Failover Manager enables you to manually switch the Provisioning and Data Import services between two fully operational servers in a dual-sided Unified CCMP installation.



Caution: 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. If in doubt, please contact Cisco support before continuing.

Preparing to Use the Failover Manager

Before performing a failover for a service:

- ▶ Be aware that the service is unavailable during the failover, and that for a large database, the failover may take a significant period of time.
- ▶ Ensure that you have an up-to-date database backup.
- ▶ Ensure that you are logged in as a domain level user who has administrative rights on both servers, and also on the machine being used to run the ICE tool.
- ▶ Ensure that the firewalls on both servers and on the machine being used to run the ICE tool are configured as in the Network and Environment Configuration section of the *Installation and Configuration Guide for Cisco Unified Contact Center Management Portal*.



Caution: Before a failover is attempted, Replication Manager must be checked. Failover can only happen successfully if replication is all green.

Starting the Failover Manager Tool

To start the Failover Manager tool:

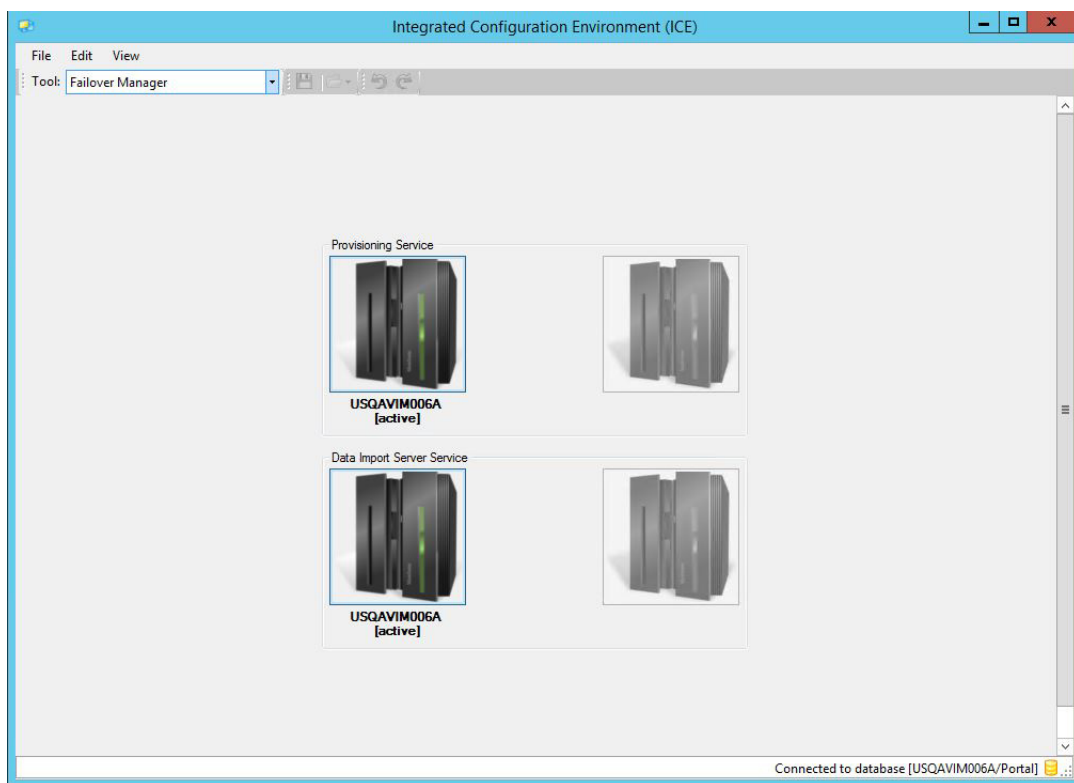
1. Launch Integrated Configuration Environment (installed as part of Unified CCMP). In the Database Connection dialog box, set the following:
 - **Server Name:** Enter the name of the primary database server.
 - **Database Name:** Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this is **Portal**.
 - **Authentication:** Select **Windows Authentication**.
2. Click **OK**. The ICE Cluster Configuration tool starts by default.

3. In the Tools dropdown, select **Failover Management**. The Failover Manager tool is displayed, showing:
 - The Unified CCMP service types that support failover.
 - The service that is currently active for each.
 - Where available, the currently inactive service that can be used for failover.

For each service type, the currently active service is shown as a depressed button, and identified by **[active]**. The inactive service is shown as a raised button that can be clicked to select it. If there is more than one instance of the Mediator service, there is also an extra dropdown to select the instance of the Mediator service to display.



Note: This display simply indicates the active and inactive services that have been configured in your Unified CCMP installation. It does not indicate the health of the services. Before performing a failover, you should make sure that both services are fully operational.



Failover Management ICE Tool

Performing a Failover Operation

To start a failover operation:

1. In the Failover Manager tool, identify the service to be switched.
2. Identify the service to be switched, and click on the raised button of the currently inactive service to display the **Manual Failover Wizard** confirmation dialog box.

3. If you want to restart the new active service when the failover completes (the default option), select the **Restart services when complete** check box. If you do not want to restart the new active service when the failover completes (for example, if you want to perform other maintenance at the same time), clear the check box.



Caution: Before continuing, make sure you really want to perform the failover at this time. The process may take some time to complete, and once it starts, it cannot be interrupted. During this time, neither the old active service nor the new active service is available.

4. If you are sure you want to start the failover, click **Next**. The failover process may take some time to complete. The **Manual Failover Wizard** dialog box shows the progress and status for each step. A green tick means that the step completed successfully and a red cross means that the step completed but there was an error which needs to be fixed before the failover can continue.
5. Once the wizard has finished, click **Finished** to return to the main Failover Manager screen.
6. Confirm that the old service has stopped and the new service is running as follows:
 - a. In ICE, select the Service Manager tool.
 - b. Verify that the old service has stopped. If not, select it and click **Stop Selected**.
 - c. If you selected the **Restart services when complete** option for the failover, verify that the new service has started, and, if not, select it and click **Start Selected**.
7. If the failover reported an error, then when the wizard finishes, neither the old service nor the new service is running. The error message helps you identify and fix the problem and retry the failover, or you can restart the original active service. Contact support if you need further help or advice.

Performing Provisioning Service Failover

Provisioning service failover has the following steps:

1. Stop the provisioning service on the server on which it is currently running.
2. Migrate the active token.
3. If requested, start the provisioning service on the new active server.

Performing Data Import Service Failover

Data import service failover has the following steps:

1. Stop the data import server service on the server on which it is currently running.
2. Migrate the active token.
3. If requested, start the data import server service on the new active server.



Service Manager

- ▶ [About Service Manager](#)
- ▶ [Starting Service Manager](#)
- ▶ [Starting Services](#)
- ▶ [Stopping Services](#)
- ▶ [Restarting Services](#)
- ▶ [Sorting Services](#)
- ▶ [Filtering Services](#)
- ▶ [Using the Shortcut Menu](#)

About Service Manager

The Service Manager enables you to monitor, start and stop Unified CCMP services from a central location.

Starting Service Manager



Note: To use Service Manager to start and stop services you need to be logged in to Windows as a domain user with permission to start and stop services.

To start the service manager tool:

1. Launch Integrated Configuration Environment (installed as part of Unified CCMP). In the Database Connection dialog box, set:
 - **Server Name:** Enter the name of the primary database server.
 - **Database Name:** Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this is Portal.
 - **Authentication:** Select **Windows Authentication**.
2. Click **OK**. The ICE Cluster Configuration tool starts by default.
3. In the **Tools** dropdown, select **Service Manager**. The Service Manager tool is displayed, showing a table of Unified CCMP services including the machine name they are installed on, the service name and the current status (Running, Starting, Stopping or Stopped).

Starting Services

Perform the following steps on the primary database server.

To start one or more Unified CCMP services:

1. In the Service Manager tool, click on the service or services you want to start. If you want to start all or most of the services, you can select the **All** check box, then, if required, click on any services you do not want to start. Select the **All** check box again to deselect all the services in the list.
2. Click **Start Selected**.
3. A dialog box opens, reporting the status of each service as it is started. Click **Close** when complete.
If a service is already started then no action is taken.

Stopping Services

Perform the following steps on the primary database server.

To stop one or more Unified CCMP services:

1. In the Service Manager tool, click anywhere on each service you want to stop. If you want to stop all or most of the services, click **Select/Deselect All**, then, if required, click on any services you do not want to stop. Click **Select/Deselect All** again to deselect all the services in the list.
2. Click **Stop Selected**.
3. A dialogue box opens, reporting the status of each service as it is stopped. Click **Close** when complete.

If a service is already stopped then no action is taken.

Restarting Services

Perform the following steps on the primary database server.

To stop and restart one or more Unified CCMP services:

1. In the Service Manager tool, click anywhere on each service you want to restart, to select the service. If you want to restart all or most of the services, click **Select All**, then, if required, click on any services you do not want to restart. Click **Deselect All** to deselect all the services in the list.
2. Click **Restart Selected**.
3. A dialog box opens, reporting the status of each service as it is stopped and restarted. Click **Close** when complete.

If a service is already stopped then it is just restarted.

Sorting Services

The Service Manager tool enables you to sort the Unified CCMP services by machine name, service name or current service status. Perform the following steps on the primary database server:

To sort services:

1. In the Service Manager tool, click the column heading of the column you want to sort on. The list of services is sorted in ascending order according to the contents of that column.
2. If you want to sort the services in descending order, click the column name again. The list of services is displayed in descending order.

Filtering Services

The Service Manager tool enables you to filter the list of services by machine name, service name or service group.


Setting Filters

To set a filter:

1. In the Service Manager tool, select the filter or filters you require:
 - To filter by machine name, start typing the machine name or part of the machine name into the text box. The list of services is updated as you type, to show only those that contain the letters you specify.
 - To filter by service name, select the arrow beside the text box to display the list of available service names, and select the service name you want to filter by.
 - To filter by service group, select the arrow beside the text box to display the list of available service names, and select the service group you want to filter by.
2. The list of services is filtered according to the filter or filters you specified.

Clearing a Filter

To clear a filter:

1. To clear all the filters, select the  icon beside the filter boxes (only shown if you have set some filters).
2. To clear an individual filter do one of the following:
 - To clear the filter for the machine name, delete the characters in the **Machine Name** text box.
 - To clear the filter for the service name or service group, select the blank entry from the drop down list.

Refreshing the Filtered List

- ▶ To refresh the list of services, but retain the current filters, click **Refresh**.

Reloading the List of Services

- ▶ To clear all filters and reload the servers and services from the database, click **Reload**.

Using the Shortcut Menu

Service Manager also has a shortcut menu. Right-click anywhere in the list of services to see a shortcut menu with the following options:

- ▶ **Select/Deselect All**
- ▶ **Start Selected**
- ▶ **Stop Selected**
- ▶ **Apply Filter**
- ▶ **Clear Filter**



System Properties Manager

- ▶ [About System Properties Manager](#)
- ▶ [Starting System Properties Manager](#)
- ▶ [Setting Global Properties](#)
- ▶ [Setting Local Properties](#)
- ▶ [Setting Resource Properties](#)
- ▶ [Setting Capacity Properties](#)

About System Properties Manager

The System Properties Manager enables you to view and set Unified CCMP system properties.

Starting System Properties Manager

To open the System Properties Manager tool, perform the following steps on the server where the properties need to be modified.

To start the system properties manager:

1. Launch Integrated Configuration Environment (installed as part of Unified CCMP). In the Database Connection dialog box, set:
 - **Server Name:** Enter the name of the primary database server.
 - **Database Name:** Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this is **Portal**.
 - **Authentication:** Select **Windows Authentication**.
2. Click **OK**. The ICE Cluster Configuration tool starts by default.
3. In the Tools dropdown, select System Properties Manager. The System Properties Manager tool is displayed, showing the Unified CCMP properties, grouped by property type and functionality.

When you first start the System Properties Manager from ICE, the display shows the Global properties. To see the other properties, click in the appropriate tab in the left-hand pane. The following sections describe the properties available in each tab.

Setting Global Properties

The Global Properties tab enables you to view and configure system wide items and items that affect multiple Unified CCMP components.

Active Directory Lookup Configuration

This group specifies configuration information for the Activity Directory. It contains the following properties:

- ▶ **Active Directory Context Type:** Specifies the type of store used to authenticate against. The default value is set to Domain.

For more information about the options and what they mean, see the Microsoft .NET documentation, <http://msdn.microsoft.com/en-us/library/system.directoryservices.accountmanagement.contexttype.aspx>.

- ▶ **Active Directory Password:** The password used by Active Directory.
- ▶ **Active Directory User Name:** The user name used by Active Directory.

Activity Monitor

This group specifies configuration information for the Activity Monitor. It contains the following properties:

- ▶ **Provisioning Warn Threshold:** The number of seconds after which an item or membership in the provisioning queue is shown in the middle (orange) band of the Activity Monitor.
- ▶ **Provisioning Max Threshold:** The number of seconds after which an item or membership in the provisioning queue is shown in the top (red) band of the Activity Monitor.

Code Lookup, Supported Equipment Types

This group specifies information about equipment types. It contains the following property:

- ▶ **Code Lookup and Supported Equipment Types:** The type of equipment that is used to import codes into the Unified CCMP database. Currently the only supported value is **CRT_CICM** (equipment type **Cisco CICM**).



Note: Contact support before changing this value.

Database Lock Configuration

This group specifies the timeout values used in the database for the importer and provisioning services. It contains the following properties:

- ▶ **Lock Importer Acquire Timeout:** The time that the importer waits to acquire a lock before timing out. The setting is entered in hh:mm:ss format.
- ▶ **Lock Importer Retry Rate:** The number of times the importer service tries to gain a lock on a database item before failing the item.
- ▶ **Lock Provisioning Acquire Timeout:** The time that the provisioning service waits to acquire a lock before timing out. The setting is entered in the format hh:mm:ss.
- ▶ **Lock Provisioning Retry Rate:** Controls the number of times the provisioning service attempts to gain a lock on a database item before failing the item.

Gadget Management

This group specifies the gadget management settings. It contains the following properties:

- ▶ **Default Welcome Gadget Id:** The GUID of the default gadget that is shown on the gadget canvas if no **App** is selected. Set the value to **00000000-0000-0000-0000-000000000000** for none. Do not change this value unless instructed to by support.
- ▶ **Gadgets Cache Expiration Period:** The time in seconds after which a cached gadget definition expires and is removed from the gadget cache. To disable the gadget cache during gadget development, set this to zero. For normal production use, this should be set to a non-zero value.

- ▶ **Gadget File Path:** The file path to a location on the web server where gadget files are located (used during gadget development only). Each gadget file name must match the name of the gadget it contains. If the gadget cache expiration period is zero, then Unified CCMP first looks for gadget files in this location and only load a gadget from the database if the gadget is not found here. For normal production use, this should be set to the empty string.

Importer State

This group specifies the import data settings. It contains the following properties:

- ▶ **Bow Wave Duration Hours:** The time period in hours relative to a cluster resource creation date that constitutes the bow wave period. The value is between 1 and 24.
- ▶ **Bow Wave Effective From:** The effective from date for dimensions created during a bow wave.
- ▶ **Last Cluster Update:** The date and time the cluster was last updated (read- only).
- ▶ **Last Mediator Model Update:** The date and time the Mediator model was last updated (read-only).
- ▶ **Default ETL Execution Update:** The interval for execution audit to be written for component execution.

Local Login Security

This group specifies the way that Unified CCMP logins are authenticated. This group contains the following properties:

- ▶ **Max Password Length:** The maximum number of characters allowed in a password.
- ▶ **Min Password Length:** The minimum number of characters allowed in a password.
- ▶ **Minimum Password Lifetime:** The minimum number of days that a password can be used for, before it is possible to change it.
- ▶ **Password Expiry:** The number of days before a password expires and must be changed, measured from the date that the password was last changed.
- ▶ **Password Expiry Warning:** The number of days before which to notify the user of password expiry.
- ▶ **Password Format:** The required password format. This field can also be set in the web application using **Settings > Security Settings > Password Format**. If one of predefined password formats (**Low Security**, **Medium Security**, **Medium/High Security** or **High Security**) is chosen in the web application, this field is automatically populated with the corresponding expression. This field is a .NET regular expression, except that the expression `{MIN_MAX}` can also be used to specify that the password length must lie between the values specified for **Min Password Length** and **Max Password Length**. For example, if Min Password Length is 8 and Max Password Length is 20, then `{MIN_MAX}` is equivalent to `{8,20}` in the .NET regular expression syntax.
- ▶ **Password Hash Algorithm:** Specifies the algorithm for encoding user passwords. To change the encoding of existing passwords, in the web application User Manager tool, set **User must change password at next login** for each user. The default is set to **SHA256**.
- ▶ **Password History:** The number of previous passwords that are saved and cannot be reused when a user password is changed.

- ▶ **Password Reuse Time:** The minimum number of days that must elapse before a previous password can be reused.
- ▶ **User Lockout:** The number of failed login attempts that a user is allowed before their account is locked.

Login Authentication Configuration

This group specifies the way that Unified CCMP logins are authenticated. It contains the following properties:

- ▶ **Adfs Metadata Url:** The Active Directory Federation Services metadata URL.
- ▶ **Azure Ad Client Id:** The Azure AD Application (client)ID for this application. If Azure AD is enabled, this ID is required.
- ▶ **Azure Ad Tenant Id:** The Azure AD Application (Tenant ID) for this application. Leave blank for multiple tenants.
- ▶ **Override Idle Timeout Exception:** When set to true, all idle user sessions will be timed out regardless of the application page they are on.
- ▶ **Credential Cache Expiration Period:** Specifies the time in seconds that the user's login is cached before being re-authenticated. This re-authentication is internal, and not visible to the user. Choose a longer cache expiry to reduce the traffic between the Unified CCMP Web/App server and the authenticating server.
- ▶ **Credential Cache Expiration Type:** Specifies the way in which the expiry period for re-authentications is determined. One of:
 - **Absolute Expiry:** The expiry period for re-authentication is measured from the last authentication, if the user has been active on the system since that time.
 - **Sliding Expiry:** The expiry period for re-authentication is measured from the last time the user was active on the system, or from the last re- authentication, if that was later.
- ▶ **Disable Inactive User Accounts Time Period:** Disable all non-system users that have not logged into the application for a set time period. Default is set to **30** days.
- ▶ **Enabled Login Types:** Specifies which authentication modes can be used by the user to login to the system. Multiple authentications can be used for the same user. The authentications modes supported are:
 - **Local**
 - **Windows**
 - **ADFS**
 - **Azure Active Directory (AD) Logins (azuread)**
- ▶ **Ext Auto Create User:** Creates a user for logins that were successfully authenticated against an external provider. One of **True** or **False**.
- ▶ **External Signout:** When you logout from the web application, you are also logged out of the identity provider. One of **True** or **False**. Defaults to **True**.
- ▶ **Override Idle Timeout Exceptions:** When set to **True**, all idle user sessions are timed out, regardless of the application page the users are viewing.

Media Upload

This group specifies the default behavior for uploading media. This group contains the following properties:

- ▶ **Media File Accepted Formats:** A comma separated list of file extensions that are valid for media files.
- ▶ **Media Share:** The network share name where WAV files uploaded through the Unified CCMP user interface is placed for replication to the CVP Media Server.

Miscellaneous

This group specifies some miscellaneous properties. It contains the following properties:

- ▶ **Additional White listed Origins:** A comma-separated list of whitelisted origins for Cross-Origin Resource Sharing (CORS), e.g `https://www.domain1.com, https://doamin2.co.uk`. The System Url is automatically whitelisted.
- ▶ **Agent Description Field Mandatory:** Whether the agent description field is mandatory when agents are created and edited. One of True or False.
- ▶ **Agent Description Format:** A regular expression defining the characters that are not allowed in the agent description field. Special characters must be escaped. For example, if you wanted to exclude the characters `z`, `&`, and `*`, you would enter `[z\&*]`.
- ▶ **Delete Person With Last Agent Member:** Determines if the associated person dimension is deleted when the last agent member is deleted.
- ▶ **Display Purge Button Stuck Seconds:** The number of seconds to wait before determining that an item in synchronizing or pending state is blocked. Once this time has been exceeded a purge button is displayed in the web application.
- ▶ **Menu Items:** Custom applications can be added to the menu bar by the inclusion of a display name and URL. Items separated by a semi colon.
- ▶ **Product Name:** The name of the product to display in the user interface, allowing organizations to personalize the product.
- ▶ **Prov Agent State Trace Enabled:** Determines whether Resource Manager users can enable the **ICM State Trace** feature on agents. ICM State Trace provides enhanced logging information when individual agents move from one state to another.
- ▶ **Query Parameter Boundary:** The maximum number of parameters in an SQL query before a sub query is generated.
- ▶ **Show Fiscal Dates In Parameter Bar:** Determines if custom fiscal dates are available for selection in the reporting parameter bar.
- ▶ **Show Only Reporting Timezones:** Determines whether only timezones supported for reporting re displayed in the web application, rather than all timezones.
- ▶ **Show Only UI Translation Cultures:** Determines whether only cultures which have a UI translation are displayed in the web application rather than all cultures.



Note: Non UI cultures are not fully supported. All unrecognized cultures default the date format to en-US.

- ▶ **Supported Languages:** The culture codes for the languages supported by the installation. Click the dropdown list to see and select the supported languages.
- ▶ **Supported Peripheral Types:** The peripheral types that can be associated with resources such as agents. Click the drop-down list to see and select the supported peripheral types.
- ▶ **Use Domain Sharding:** Determines if the web application will use domain sharding to separate web request sub-domains for improved responsiveness.
- ▶ **Web Server Debug Info Disclosure:** Whether server and culture information is shown in the menu bar of the web application. One of **True** or **False**.

Other Security

This group specifies other security options. It contains the following properties:

- ▶ **Enable User Copy:** Determines whether the user copy feature is available in the Unified CCMP web application. One of **True** or **False**.
- ▶ **Inherit Permissions Default:** Determines whether the **Inherit Permissions** check box is selected by default when a new folder is created. One of **True** or **False**.
- ▶ **Push Policy Changes to Child:** Determines whether the **Change Permissions for Subfolders** check box in Security Manager is selected by default when the user selects **Change Permissions**. One of **True** or **False**.

Partitioning State

This group specifies database partitioning options. This group contains the following properties:

- ▶ **Last Partition Metadata Change:** The date and time that the partition metadata was last updated (read-only).
- ▶ **Dimension Purge retention Period (Days):** Minimum retention period before dimensions are purged after Fact data retention period has been breached. Only used when a value cannot be automatically calculated from existing data. Warning: Improper use of this property can cause permanent removal of dimensions and corruption of the parameter sets. Use with care.
- ▶ **Report Schedule History Purge Retention (Days):** The number of days for which the completed report schedule histories should be kept in the database.
 - **Report Schedule Purge Retention (Days):** The number of days for which the completed report schedule should be kept in the database.
 - **NTLM**
 - **Kerberos**
 - **Negotiate**

System Limits

This group contains the following properties:

- ▶ **Max Dimension Associated Items:** The maximum number of associated items that can be listed for a dimension in the web application.

- ▶ **Max Dimension Drop Down List Items:** The maximum number of dimension items that can be shown in a drop-down list in the web application before the list is disabled.

User Provisioning

This group specifies the default behavior when creating users. It contains the following properties:

- ▶ **Create Advanced Users Groups:** Determines if an advanced users group is created when a folder is set to not inherit permissions. One of **True** or **False**.
- ▶ **Create Basic Users Groups:** Determines if a basic users group is created when a folder is set to not inherit permissions. One of **True** or **False**.
- ▶ **Create Supervisor Users Groups:** Determines if a supervisor users group is created when a folder is set to not inherit permissions. One of **True** or **False**.
- ▶ **Default Home Folder Role:** The role that is automatically associated with a user on their home folder when the home folder is created.
- ▶ **Default Tenant Administrators Global Role:** The global role that is automatically associated with the Administrators group when a new Tenant or policy root folder is created.
- ▶ **Default Tenant Administrators Role:** The role that is automatically associated with the Administrators group when a new Tenant or policy root folder is created.
- ▶ **Default Tenant Supervisors Global Role:** The global role that is automatically associated with the Supervisors group when a new Tenant or policy root folder is created.
- ▶ **Default Tenant Supervisors Role:** The role that is automatically associated with the Supervisors group when a new Tenant or policy root folder is created.
- ▶ **Default Tenant Users Global Role:** Specifies the global role that is automatically associated with the Users group when a new Tenant or policy root folder is created.
- ▶ **Default Tenant Users Role:** Specifies the role that is automatically associated with the Users group when a new Tenant or policy root folder is created.
- ▶ **Home Folder Suffix:** The suffix that is appended to the username when a home folder is created for a user.

Setting Local Properties

The Local Properties tab enables you to view information from the local machine.

Checksum

This group displays database validity information. It contains the following property:

- ▶ **Is Database Valid:** The value determining whether or not the database is valid. (read-only).

Partitioning State

This group specifies partition table information. It contains the following property:

- ▶ **Last Partition Tables Refresh:** The date and time of the last partition table refresh (read-only).

Versioning Group

This group displays the following version numbers. It contains the following properties:

- ▶ **Build Version:** The build cycle that the installation was taken from (read-only).
- ▶ **Schema Version:** The version of the database schema being used (read-only).

Setting Resource Properties

The Resource Properties tab enables you to view and configure the way that resources are handled in Unified CCMP.

Resource Items

This group lists each resource item. Each resource item has the following properties:

- ▶ **TaxonomyEnabled:** Determines whether resources of this type are available to the taxonomy (hierarchy) feature of Unified CCMP.

Resource Members

This group lists each resource membership. Each resource membership has the following properties:

- ▶ **TaxonomyEnabled:** Always **False** for resource memberships.

Setting Capacity Properties

The Capacity Properties tab enables you to view and configure the capacity rules for the remote equipment. A capacity rule may apply to:

- ▶ All equipment of a specified type in the cluster, or only to a specific equipment instance.
- ▶ All tenants in the cluster, or only to a specific tenant.

The properties of the capacity rules are determined by the remote equipment. The properties are grouped by capacity rule. Each capacity rule has the following properties:

- ▶ **CapacityId:** The database primary key of the capacity rule (read-only).
- ▶ **ItemType:** The resource type that the capacity rule applies to (read-only).

- ▶ **MemberType:** The membership that the capacity rule applies to, or **<None>** (read-only).
- ▶ **ViaMemberType:** The additional membership that the capacity rule applies to, or **<None>** (read-only).
- ▶ **Description:** The description of this capacity rule (read-only).
- ▶ **MaxCapacity:** The maximum number of resources or memberships allowed under this capacity rule. This value can be edited if the **System** property is **False**, or if the **ClusterInstance** property is **<All>**. Otherwise this value is read- only.
- ▶ **ClusterType:** The cluster type of the remote equipment that the capacity rule applies to (read-only).
- ▶ **ClusterInstance:** The remote equipment that the capacity rule applies to (read- only). One of:
 - **<All>:** if the capacity rule applies to all instances of that equipment type
 - The specific cluster name of the remote equipment, if the capacity rule only applies to a single instance of that equipment type.
- ▶ **TenantName:** The tenant that the capacity rule applies to (read-only). One of:
 - **<All>:** If the capacity rule applies to all tenants on the specified equipment
 - The specific tenant name, if the capacity rule only applies to a single tenant on the specified equipment.
- ▶ **CreationDate:** The date that this capacity rule was created (read-only).
- ▶ **ModifiedDate:** The date that this capacity rule was last modified (read-only).
- ▶ **System:** Determines whether this the capacity rule is a default system value, or whether it was added as a customization (read-only). One of:
 - **True:** The rule is a default system value.
 - **False:** The rule is a customization.
- ▶ **Enabled:** Determines whether this capacity rule should be considered when creating a resource or membership. One of **True** or **False**.



Custom Dimension Editor

- ▶ [About the Custom Dimension Editor](#)
- ▶ [Starting the Custom Dimension Editor](#)
- ▶ [Adding a Custom Dimension Item](#)
- ▶ [Editing a Custom Dimension Item](#)
- ▶ [Deleting a Custom Dimension Item](#)
- ▶ [Moving a Custom Dimension Item](#)

About the Custom Dimension Editor

The ICE Custom Dimension Editor enables you to create and edit custom dimensions.

Custom Dimensions

Custom dimensions are user-defined dimensions that store user data in Unified CCMP. This data can be exported from the database, used in custom reports and also accessed programmatically using the Unified CCMP Web Services APIs. Each item in a custom dimension can have free-format attributes, defined as name-value pairs.

Unified CCMP provides ten custom dimensions, **Custom0**, **Custom1**, **Custom2**, . . . **Custom9**. Each custom dimension can be used to store any number of items, and each item can have any number of custom attributes. Each item in a custom dimension can have the same attributes, or different items can have different attributes, depending on the requirements. The Custom Dimension Editor does not check the attribute names or content, so it is up to the user to enforce any rules that apply.

Starting the Custom Dimension Editor

To start the ICE Custom Dimension Editor:

1. Launch Integrated Configuration Environment (installed as part of Unified CCMP). In the Database Connection dialog box, set the following:
 - **Server Name:** Enter the name of the primary database server.
 - **Database Name:** Enter the name of the Unified CCMP database that was installed when setting up the Database Component. If you accepted the default value, this will be **Portal**.
 - **Authentication:** Select **Windows Authentication**.
2. Click **OK**. The ICE Cluster Configuration tool starts by default.
3. In the Tools dropdown, select **Custom Dimension Editor**. The Custom Dimension Editor is displayed, showing **Custom0** to **Custom9** tabs and a grid listing the custom dimension items.

Adding a Custom Dimension Item

To add a custom dimension item:

1. Start the ICE Custom Dimension Editor (see section [“Starting the Custom Dimension Editor”](#) on page 71).
2. Click the custom dimension corresponding to the item you want to add. For example, to add a new item to Custom2, click the Custom2 tab.
3. In the grid, enter a name for the custom dimension item, and optionally, a description.
4. To add attributes, do the following:

- a. In the attribute column, click **Add** (shown as **Edit** if the custom dimension item already has one or more attributes).
- b. In the attributes dialog box, in the blank row, enter the name of the attribute and the required value. All values are stored as strings.
- c. Add additional attribute rows as required. When you have finished adding attributes, click **OK** to return to the Custom Dimension Editor.



Note: A custom dimension item cannot have two attributes with the same name. Unified CCMP does not carry out any other validation on the attribute names or values, so if you require specific attributes to be present, or for attributes to have a specific range of values, you must enforce this yourself.

5. To save and action your changes, either click the **Save** button in the toolbar or select **File > Save** from the menu. The custom dimension item is created in the **/Shared** folder in the Unified CCMP folder tree.

Editing a Custom Dimension Item

To edit a custom dimension item:

1. Start the ICE Custom Dimension Editor (see section [“Starting the Custom Dimension Editor” on page 71](#)).
2. Click the custom dimension tab that contains the item you want to edit.
3. In the grid, locate the item you want to edit.
 - You can change the name or description of a custom dimension item directly in the grid.
 - To edit the attributes, click **Edit** beside the item (or **Add** if the item has no attributes yet) then make the required changes to the attributes.
 - You can change the name or value of an attribute directly in the grid.
 - To add an attribute, in the blank row, enter the name of the attribute and the required value. All values are stored as strings.
 - To delete an attribute, select the attribute row you want to delete, then press **Delete**. You can select multiple rows to delete multiple attributes.
4. When you have finished, click **OK** to return to the Custom Dimension Editor.
5. To save and action your changes, either click the **Save** button in the toolbar or select **File > Save** from the menu.

Deleting a Custom Dimension Item

To delete a custom dimension item:

1. Start the ICE Custom Dimension Editor (see section [“Starting the Custom Dimension Editor” on page 71](#)).
2. Click the custom dimension tab that contains the item you want to delete.

3. In the grid, select the check box beside the item or items you want to delete. You can click **Select All** to select all items in the grid, or **Select None** to clear all the selections you have made in the grid.
4. When you have selected the item or items you want to delete, click **Delete Selected**.
5. To save and action your changes, either click the **Save** button in the tool bar or select **File > Save** from the menu.



Tip: You can also use the classic Resource Manager in the Unified CCMP web application to delete custom dimension items.

Moving a Custom Dimension Item

The Custom Dimension Editor creates all custom dimension items in the **/Shared** folder. You can use the classic Resource Manager in the Web UI to move custom dimension items to other folders if required. See the *Unified CCMP User Guide* or the online help for more information.

The Custom Dimension Editor does not show the folder path of an item, and can only create items in the **/Shared** folder. But if the item has been moved, the new location is retained when the item is edited.



ICE Diagnostic Support

- ▶ [Diagnostic Features](#)
- ▶ [Installing the Cisco Diagnostic Portal](#)
- ▶ [Configuring ICE Integration with the Diagnostic Portal](#)
- ▶ [Viewing Logs](#)

Diagnostic Features

ICE provides two features to help you view and collect status information and log files from the servers in the Unified CCMP cluster.

- ▶ ICE supports integration with Cisco's Diagnostic Portal, and provides a simple, central way to view diagnostic information from any server in the Unified CCMP cluster.
- ▶ ICE provides a wizard that enables you to collect log files from all the servers in the cluster and package them into a single zip file that can be set to your vendor support in case of problems.

Before you can use the diagnostic support features provided in ICE, you need to

- ▶ Install the Cisco Diagnostic Portal on each physical Unified CCMP servers if not already installed.
- ▶ Configure ICE integration with the Diagnostic Portal on each physical Unified CCMP server. For more information, see [“Configuring ICE Integration with the Diagnostic Portal” on page 75](#).

Installing the Cisco Diagnostic Portal

Perform this step for each physical Unified CCMP server in the product cluster. For example, if you have a dual-sided deployment, and a two tier installation, with separate Database and Web/Application servers, you should install the Cisco Diagnostic Portal on the Side A Database Server, the Side A Web/Application server, the Side B Database Server and the Side B Web/Application server.

Install the Diagnostic Portal as described in the *Installation and Configuration Guide for Cisco Unified Contact Center Management Portal*.

Configuring ICE Integration with the Diagnostic Portal

Use ICE to perform this step for each physical server in the product cluster. When you configure ICE integration with the Diagnostic Portal for one ICE server resource on a physical server, the other ICE server resources are automatically updated to use the same values.

For example, if you have a single-sided deployment, with an all-in-one server running both the Database and Web/Application components, a Unified CCE server and an ICM server, you need to configure ICE integration with the Diagnostic Portal on:

- ▶ The Unified CCMP Database Server or the Unified CCMP Web/Application server (the configuration automatically is propagated to the other one)
- ▶ The Unified CCE server
- ▶ The ICM server

To configure ICE for use with the Diagnostic Portal on a physical server:

1. Identify a Windows user for ICE to use to access the Diagnostic Portal. If you have a single-sided all-in-one deployment, then you can use the local wsmadmin user that was created when you installed the Diagnostic Portal. Otherwise you need to create a domain user.
2. Select **Start > Computers > Manage**, select **System Tools > Local Users and Groups > Groups** to view the available security groups.
3. Add the required user to the Diagnostic Framework Users Security group. The name of this group is different for each type of server, but always ends in **DiagnosticFrameworkUsers**. For example, on a Unified CCE server, the group is called **ICMDiagnosticFrameworkUsers**.
4. In ICE, in the Resources tab, select a logical server on this physical server, click the **Component** tab for the resource and set the following:
 - **Diagnostic Portal User Name:** the required user name. If you are using a domain user you need to specify the user name in the format **<username>@<domainname>**. where **<username>** is the Windows user name and **<domainname>** is the fully qualified Windows domain name, for example, **dp_user1@testdomain.local**.
 - **Diagnostic Portal Password:** the password for the specified user.
 - **Diagnostic Portal Service URL.**

These details are automatically propagated to any other servers located on the same physical server.

Repeat for the other physical servers in the system.

Viewing Logs

To view a log or trace log:

1. Open ICE and select the Cluster Configuration tool.
2. Click **Resources** to view the logical server resources in the Unified CCMP cluster.
3. Right click on the logical server resource for which you want to view the logs, and select **Components**, then select the required component. Finally select **View Logs** or **View Trace Logs** to see the selected log information.