



# Administration Manual for Cisco Unified Contact Center Management Portal

**Release 8.5(2)**

**July 2011**

**Corporate 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: 408 526-4100



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at <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. (1005R)

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

Copyright 2011 Cisco Systems, Inc. All rights reserved.

# Contents

Purpose .....	v
Audience .....	v
Organization .....	v
Related Documentation.....	vi
Product Naming Conventions .....	vii
Conventions .....	viii
Obtaining Documentation and Submitting a Service Request.....	ix
Documentation Feedback .....	ix
<b>1. Unified Contact Center Management Portal .....</b>	<b>1</b>
<b>2. Web Server .....</b>	<b>3</b>
Import a Tenant from Unified Contact Center Enterprise.....	3
How does it work? .....	3
Portal Users.....	3
Host Administrator First Steps .....	3
Configuring Imported Resource Data.....	4
Single Sign-On .....	5
Administrator Account Setup .....	5
Configuring Management Portal Authentication .....	5
Managing Users with Single Sign-On .....	7
Creating a Tenant Administrator .....	7
Assigning Tenant Administrator Permissions .....	7
Using the Agent Password Reset Utility.....	8
Password Complexity Rules .....	8
Unified CCE Password Compliancy.....	8
<b>3. System Provisioning.....</b>	<b>9</b>
Security Management .....	9
System Management .....	9
<b>4. Bulk Upload .....</b>	<b>11</b>
Member Attributes .....	11
Editing CSV Files .....	11
Template Descriptions.....	11
Common Template Column Names .....	11
Agent Template.....	13
Folders Template .....	14
Agent Desktop Template .....	15
Agent Team Template .....	15
Enterprise Skill Group Template .....	15
Skill Group Template .....	16
User Variable Template .....	17

Using the Bulk Upload Tool.....	17
Reasons for Upload Failure .....	18
<b>5. Audit Trails .....</b>	<b>19</b>
Audit Histories .....	19
Audit Reports.....	19
Setting Up Audit Reporting .....	19
Parameter Sets .....	19
Viewing an Audit Report .....	20
<b>6. System Architecture .....</b>	<b>21</b>
Web Application .....	21
Application Server .....	22
Reporting Services .....	22
Data Import Server .....	22
Provisioning Server .....	22
Agent Self Re-Skilling and the Provisioning Service .....	23
Resource States .....	23
State Descriptions .....	24
Synchronize .....	24
Ready.....	24
Error .....	24
Delete Pending .....	25
Delete Confirmed .....	25
User Interface.....	25
Database Codes.....	26
Memberships.....	26
State Machine Scenarios .....	27
<b>7. System Operations.....</b>	<b>29</b>
Service Restart Configuration .....	29
Database Backup and Recovery.....	29
Manual Provisioning/Importer Failover.....	30
Changing the Active Provisioning Server .....	30
Changing the Active Resource Import Server .....	31
<b>8. Connection Monitoring .....</b>	<b>32</b>
Performance Counters .....	32
CCMP Data Pipeline Object.....	32
CCMP Application Datasources Object.....	33
CCMP Application Monitoring Object .....	33
CCMP Application Server Object.....	33
<b>Index .....</b>	<b>34</b>

# Preface

## Purpose

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

## Audience

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

## Organization

The following table describes the information contained in each chapter of this guide.

Chapter	Description
Chapter 1, “Unified Contact Center Management Portal” Intended Audience: all audiences	Provides information on the components that make up Unified CCMP and the configuration that needs to be done for each.
Chapter 2, “Web Server” Intended Audience: contact center/system administrators, business users, and supervisors	Explains how to set up the essential users and equipment within the Web Server so that tenant users can use it to view reports and perform administrative tasks upon their own resources.
Chapter 3, “System Provisioning” Intended Audience: System administrators	Introduces system security and system management and explains where to find further information.
Chapter 4, “Bulk Upload” Intended Audience: System administrators	Details the process required to bulk upload dimension data into Unified CCMP, the templates used to do so and details on how to understand any upload failure.
Chapter 5, “Audit Trails” Intended Audience: System administrators	Describes the audit histories of individual items and the audit report used to measure actions taken upon entities in Unified CCMP.
Chapter 6, "System Architecture" Intended Audience: System administrators	Describes how the system operates, including system architecture, possible resource states and the effects events have on these states.
Chapter 7, "System Operations" Intended Audience: System administrators	Describes best practices within Unified CCMP system, and the management of the Database Servers.

## 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 Management Portal, Cisco Unified Customer Voice Portal (CVP), Cisco Unified IP IVR, Cisco Unified Intelligence Center, and Cisco Support Tools.
- For documentation for these Cisco Unified Contact Center Products, go to <http://www.cisco.com/cisco/web/psa/default.html>, click **Voice and Unified Communications**, then click **Customer Contact**, then click **Cisco Unified Contact Center Products** or **Cisco Unified Voice Self-Service Products**, then click the product/option you are interested in.
- For troubleshooting tips for these Cisco Unified Contact Center Products, go to <http://docwiki.cisco.com/wiki/Category:Troubleshooting>, then click the product/option you are interested in.
- Documentation for Cisco Unified Communications Manager is accessible from: <http://www.cisco.com/cisco/web/psa/default.html>.
- Technical Support documentation and tools are accessible from: <http://www.cisco.com/en/US/support/index.html>.
- The Product Alert tool is accessible from (login 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 at (login required): [http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/prod\\_bulletins\\_list.html](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 at the bottom of the following page: [http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod\\_technical\\_reference\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html).

## 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 System IPCC Enterprise Edition	Cisco Unified System Contact Center Enterprise	Unified SCCE  <b>Note:</b> Cisco Unified System Contact Center Enterprise (Unified SCCE) is supported in 8.5(2); however, there is not a separate 8.5(2) version. If you request features that are in 8.5(2), you must migrate to the Unified ICM/CCE/CCH software. Full migration information is documented in the <i>Upgrade Guide for Cisco Unified ICM/Contact Center Enterprise &amp; Hosted</i> .
Cisco IPCC Hosted Edition	Cisco Unified Contact Center Hosted	Unified CCH
Cisco Intelligent Contact Management (ICM) Enterprise Edition	Cisco Unified Intelligent Contact Management (ICM) Enterprise	Unified ICM
Cisco Intelligent Contact Management (ICM) Hosted Edition	Cisco Unified Intelligent Contact Management (ICM) Hosted	
Cisco CallManager/Cisco Unified CallManager	Cisco Unified Communications Manager	Unified CM

## Conventions

This manual uses the following conventions:

Convention	Description
<b>boldface font</b>	<p>Boldface font is used to indicate commands, such as entries, keys, buttons, folders and submenu names. For example:</p> <ul style="list-style-type: none"><li>• Chose <b>Edit &gt; Find</b>.</li><li>• Click <b>Finish</b></li></ul>
<i>italic font</i>	<p>Italic font is used to indicate the following:</p> <ul style="list-style-type: none"><li>• To introduce a new term; for example: A <i>skill group</i> is a collection of agents who share similar skills.</li><li>• For emphasis; for example: <i>Do not</i> use the numerical naming convention.</li><li>• A syntax value that the user must replace; for example: IF (<i>condition, true-value, false-value</i>)</li><li>• A book title; for example: Refer to the <i>Cisco CRS Installation Guide</i></li></ul>
window font	<p>Window font, such as Courier, is used for the following:</p> <ul style="list-style-type: none"><li>• Text as it appears in code or that the window displays: for example: <code>&lt;html&gt;&lt;title&gt;Cisco Systems, Inc. &lt;/title&gt;&lt;/html&gt;</code></li><li>• Navigational text when selecting menu options; for example <b>ICM Configuration Manager &gt; Tools &gt; Explorer Tools &gt; Agent Explorer</b></li></ul>
< >	<p>Angle brackets are used to indicate the following:</p> <ul style="list-style-type: none"><li>• For arguments where the context does not allow italic, such as ASCII output</li><li>• A character string that the user enters, but does not appear on the window such as a password</li></ul>

## Obtaining Documentation and Submitting a Service Request

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

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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

## Documentation Feedback

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

[mailto:ccbu\\_docfeedback@cisco.com](mailto:ccbu_docfeedback@cisco.com)

We appreciate your comments.



# 1. Unified Contact Center Management Portal

Unified CCMP is a suite of server components that simplify the operations and procedures for performing basic administrative functions such as managing agents and equipment, and provide a common, web-based user interface within the entire Cisco Unified Contact Center Hosted and Enterprise Editions product set.

Unified CCMP consists of five components:

- **Database server** component utilizes an application called the Importer to import enterprise data from different data sources into a Microsoft SQL Server management information database.
- **Application server** component manages security and failover by ensuring that users can view only specific folders and folder content as defined by their security login credentials. This component verifies that a user is valid and then loads the system configuration that applies to that user. It also manages failover, so if one database server fails, the application can automatically retrieve the required data from an alternative database server.
- **Web server** component provides a user interface to the platform that allows users to interact with report data as well as to perform administrative functions.
- **Data Import server** component, an Extract, Transform and Load (ETL) server for data warehouses, is designed to import resource data (dimensions) such as agents, peripherals and skill groups.
- **Provisioning Server** component provides the mechanism for changes to be committed to the Cisco Unified Contact Center platform. This service constantly monitors changes from Unified CCMP and makes those related changes to the remote systems to which they belong.

When these components are installed on more than one machine, the Data Import, Provisioning Server and Database components are typically installed on the Database Server. The Application and Web components are installed on the Web Application Server.



## 2. Web Server

The Unified CCMP web component is a browser-based management application designed for use by contact center/system administrators, business users, and supervisors. The host administrator does not administrate the web component server on a day-to-day basis, but must set up a tenant administrator user to do so, as well as a tenant folder in which to put all the tenant's resources.

### Import a Tenant from Unified Contact Center Enterprise

All tenant data in the Unified CCMP platform is derived from imported customer definition data on the Unified Contact Center Enterprise (Unified CCE). All changes to the customer (tenant) data are performed using Cisco's Configuration Manager tool.

### How does it work?

Unified CCMP maintains a complete data model of the contact center equipment to which it is connected and periodically synchronized. Unified CCMP data model and synchronization activity allow for items to be provisioned either through Unified CCMP's Web interface or from the standard equipment specific user interfaces.

### Portal Users

The Portal user types on the Web component server are as follows:

- **Host administrator** is responsible for the whole platform and therefore has a view across all equipment and resources.
- **Tenant administrator** is responsible for those components of the system assigned to the tenant by the host administrator.
- **Tenant user** has access only to the resources and tools assigned by the tenant administrator. Using user groups and roles, the tenant administrator can create several sub-classes of tenant to achieve their business requirements. For example, one type of user might only be able to add information notices.

On a new system, the host and tenant administrators perform their respective tasks before the tenant user is given access to the system. These tasks are detailed below.

### Host Administrator First Steps

The Host administrator is responsible for:

- Creating a tenant, see Creating a Tenant Administrator on page 6.
- Ensuring that the tenant equipment (peripherals) is correctly located in the tenant folder.
- Creating an administrator user for each tenant.
- Adding them to the administrators group for the tenant and assigning any specific roles.

## Configuring Imported Resource Data

After the initial data import, resources imported from Cisco Unified Communications Manager (Unified CM) that are associated with specific tenants are stored in those tenant folders. When multiple tenants share a Unified CM, resources are put in the Unallocated folder and the administrator must place them in the appropriate folder. Put resources associated with more than one tenant, such as phone types and button templates, in a subfolder of the Shared folder that is set to be readable only by users from those tenants. For more information on how to manage security in the Management Portal, refer the *User Manual for Cisco Unified Contact Center Management Portal*.

**Caution:** Resources **cannot** be moved out of tenant folders unless they relate to customer instances defined in the same Unified CCE.

### Note

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

### To view the prefixes in the system that apply to tenant folder data:

1. In the Management Portal window click **Tools**. The **Tools** page displays.
2. Click **System Manager**. The **System Manager** page displays.
3. Select the **Root** folder from the folder tree and click the **Tenant** link from the summary section. The tenant folders in the system display as a list.
4. Click the name of the tenant to display the **Tenant Edit** section page.
5. Click the **Prefixes** tab. The prefixes associated with the selected tenant display as a list.

### To create a prefix (add a prefix to a system folder):

1. Click **Add**. A new row is added to the prefix table prompting for the following information:
2. In the **Prefix** field, enter the prefix.
3. From the **Type** drop-down, select the system resource type to which the prefix is to be applied, there are over thirty options to select from including:
  - Agent
  - Call Type
  - Routing Script
  - SkillGroup
4. In the **Priority** field, enter a unique numerical value (0 - 9999).
5. Check the **Enabled** flag.
6. Select the **Path** of the folder to which items will be moved.
7. Click the **...** button located to the right of the new row.

### To edit a prefix:

Click the **properties** icon next to the prefix name.

### To delete a prefix:

Click the **red cross** displayed next to the prefix you want to delete.

## Single Sign-On

By default, it is necessary for users to log in to the Portal every time they connect. The Portal can, however, be configured to use Single Sign-On (SSO), which allows users to connect without logging in by linking their Portal user accounts with their Windows user accounts.

**Note** Users cannot log in via SSO over a proxy connection.

**Caution** Setting up SSO will disable any existing Portal user accounts that are not in domain login format. You will need to set up new Portal user accounts for all existing users.

## Administrator Account Setup

**Warning** It is vital that a new administrator account be set up correctly, as the existing administrator account will be disabled when SSO is configured.

1. Log in to the Portal as 'administrator'.
2. In the **User Manager**, create a user account to be the new administrator account. The login name must be of the form <DOMAIN>\<your domain login>; for example CCMPDOM\jsmith. The password must conform to the password security specified in System Settings, but will never be used.
3. Click on the new user and open the **Groups** tab.
4. Click **Add to Group**.
5. Check the check box of the **Administrators** group.
6. Close and save.

You may now proceed to configure SSO for the Management Portal.

## Configuring Management Portal Authentication

1. From the location where you installed Unified CCMP (this will normally be **C:\Program Files \Management Portal**), navigate to the **Application Server** folder.

2. Open the XML file **Exony.Reporting.Application.Server.exe.config**.

**Note** Some text editors, such as Wordpad, will not save an XML file correctly, which will cause problems with the Management Portal. Always back up the config file before making changes.

3. Locate the section:

```
<Exony.Reporting.Application.Security.Security>
  <setting name="Authentication" serializeAs="String">
    value>Portal</value><!--SSO|Portal-->
  </setting>
```

```
</Exony.Reporting.Application.Security.Security>
```

and change Portal to SSO

```
<Exony.Reporting.Application.Security.Security>
  <setting name="Authentication" serializeAs="String">
```

```
<value>SSO</value><!--SSO|Portal-->
</setting>
</Exony.Reporting.Application.Security.Security>
```

4. Save and close.
5. Run **services.msc** and restart Unified CCMP **Application Server** service.
6. Open **Internet Information Services (IIS) Manager** and select **Web Sites > Default Web Site**.
7. Expand Portal virtual directory and locate the file `post_logon.aspx`. Right-click `post_logon.aspx` and select **Properties**.
8. In the **Directory Security** tab:
  - **Edit...** Authentication and access control
  - Ensure that only **Integrated Windows authentication** is checked. Uncheck any other options, particularly **Enable anonymous access** (normally found at the top of the window), and click **OK**.
9. In the **Custom Errors** tab:
  - Select each 401 error in turn and click **Edit**.
  - Ensure the **Message type:** is **File**.
  - Ensure the **File:** is set to the Portal **redirect401.htm** file which is by default found at **C:\Program Files \Management Portal\Web\redirect401.htm**.
10. Click **OK** to close the **Edit Custom Error Properties** window. Leave IIS open, as you will need to restart it when you have finished configuring SSO.
11. From the location where you installed Unified CCMP (this will normally be **C:\Program Files\Management Portal**), right-click on the **Web** folder and click **Properties**.
12. In the **Security** tab, click **Advanced** and ensure that the **Allow inheritable permissions from the parent to propagate to this object and all child objects option is checked**.
13. Give **Read** and **Read & Execute** properties on the Web directory to all domain users who must have access to the Management Portal.

**Note** You can create a Portal Users group, so future Portal users can be added to avoid repeatedly performing this step.
14. Click **OK** to close the **Advanced Security Settings** and **Web Properties** windows.
15. Double-click on the **Web** folder and open the **web.config** file.
16. Locate the section:

```
<setting name="AuthenticationProvider" serializeAs="String">
  <value>Portal</value><!--SingleSignOn|Portal-->
and change Portal to SingleSignOn:
<setting name="AuthenticationProvider" serializeAs="String">
  <value>SingleSignOn</value><!--SingleSignOn|Portal-->
```

17. In IIS, right-click on the current machine and select **All Tasks > Restart IIS...**

You will now be able to access Unified CCMP from your domain account without logging in.

## Managing Users with Single Sign-On

Once SSO has been set up, all Portal users must be given a Portal login in the form <DOMAIN>\<Windows domain login>. This means that previously-existing Portal user accounts must be recreated in the new format before any users can sign in.

Each time a new user is given a Portal account, that user must either be given **Read** and **Read & Execute** properties on the Web directory as described above, or added to a user group that has those permissions.

Each new user will also need to add the Portal to their list of trusted sites in Internet Explorer.

## Creating a Tenant Administrator

1. Click on the **Tools** link at the top right of the web page to display the **Tools** page.
2. Click on **User Manager**, and the **User Manager** page displays.
3. Select the tenant folder and click **New**.
4. Fill in the following fields:
  - **User Name** field enter the name as it will appear in the system for the new user
  - **Password** field enter the password for the new user
  - **Confirm Password** field re-enter the selected password
  - **First Name** and **Last Name** fields enter the user's details
  - **Email** field enter the email address of the new user
  - **Description** field enter any explanatory text, if required
5. Select the **Advanced Mode** check box and any of the following check boxes, if applicable:
  - **Enabled** check box to ensure that the user is live in the system. If unchecked the new user is saved in the system but cannot access it
  - **User must change password at next Logon** check box to prompt the new user to change their password after their first login
  - **Password Never Expires** check box to assign the password to the new user indefinitely
  - **User cannot change password** check box to prevent the new user from being able to change their password

**Note** Only the User Name, Password and Confirm Password fields are required.
6. Click **OK**.

## Assigning Tenant Administrator Permissions

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

1. Click on the administrator user from the **User Manager** to display the **Edit User** page.
2. Click on the **Groups** tab to show the available groups.

3. Select the group <tenant> Administrators and save the user. The user's permissions are updated so that they can manage users, folders, information notices and folder security within the tenant folder.

## Using the Agent Password Reset Utility

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

This page is reached by navigating to the URL: *http://<CCMP Server>/Portal/agent\_manage\_password.aspx*. You do not need to have a Portal user account to use the Change Your Agent Password page.

### To change a password:

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

**Note** Password changes are subject to a small time delay while they are committed to the Cisco Unified Intelligent Communications Manager.

## Password Complexity Rules

Passwords for agents must conform to the password complexity rules defined in the Cisco Unified Communications Management Portal.

The following settings can be configured:

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

For more information about changing the password complexity rules in Cisco Unified Communications Management Portal, please refer to the section on Security Settings located in the *User Manual for Cisco Unified Communications Management Portal*.

## Unified CCE Password Compliancy

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

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

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

# 3. System Provisioning

All system and security management for Unified CCMP is performed through the web interface. For details on how to use the web interface, refer to the *User Manual for Cisco Unified Contact Center Management Portal*. Most system and security management after the initial setup is performed by individual tenant administrators.

## Security Management

Security Management can be thought of as the process of determining which users can perform which actions in which folders. This involves creating and managing the following entities:

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

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

Security is explained in more detail in the *Security Management* chapter of the *User Manual for Cisco Unified Contact Center Management Portal*.

## System Management

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



## 4. Bulk Upload

The Bulk Upload tool is used to import hundreds of resource items into Unified CCMP. It is used to generate dimensions, such as an Agent or a Skill-Group, by filling in dimension attributes using the standard CSV format.

All CSV files require headers that dictate where each value goes. To facilitate this, Unified CCMP uses CSV templates. There is a template for every dimension type; for example, one for Agents, one for Skill-Groups, and so forth.

**Note** Templates do not inform you of the value type allowed in the field, for example, numeric values.

### Member Attributes

Member attributes, such as Peripheral Member or Desk Setting Member, can always be removed from the CSV file completely. This means the relationship will never be set in any row in the CSV file. Alternatively, you can leave this field blank so there will be no relationship for that particular row.

### Editing CSV Files

You can use Notepad or any other text-based editor to edit CSV files. Excel also offers support for CSV files, so you can edit these in a familiar environment while maintaining the integrity of the CSV format.

**Note** There are a few known issues with Excel and the CSV format. If the CSV is corrupt after editing it in Excel, edit the file in a standard text editor, such as Notepad, and check the file for missing commas.

### Template Descriptions

This section lists each template and describes the purpose of the columns included in each template.

### Common Template Column Names

The column names shown in the next table appear in *every* template file. The **Column Name** is the heading entry at the top of each column of the CSV file. Brief descriptions of the other columns that appear in these tables are as follows:

- **Data Type** See Data Types on page 12, for a description of the data types that can be entered.
- **Column Required?** This column states whether you can remove this column from the table.
- **Column Description** This column describes what this field is for and any special requirements.

## Data Types

The following data types are used:

- **SNC** indicates Standard Naming Convention and is the **same as the UI allows in the name** fields on the provisioning pages. That is, alphanumeric characters, no exclamation mark or hyphens, and so on
- **BOOLEAN** indicates one of the following values:
  - TRUE
  - FALSE
  - Empty field. Leaving these fields empty defaults the field to FALSE.
- **Y/N** is similar to Boolean however it can only contain the values Y or N.
- **Date** format is the universal date format <Year>-<Month>-<Day> for example 2006-08-30.
- Any Data Type marked with a hyphen (-) means that there are no constraints on what you can put in the field (except for the constraints imposed by the native CSV format).

## Incorrect Data Type Entry

It is essential that the values in the template are of a valid data type. If an incorrect data type has been entered an error will be produced.

For example, if an alphabetic data type has been used instead of a numeric one the following error displays:

```
System.InvalidCastException: The Peripheral Number is not numeric
```

Column Name	Data Type	Column Required?	Column Description
Path	Path	No	Describes where in the Tree the dimension will be created. If you wish to supply the path in the Bulk Upload screen, you must remove this column. <b>Note</b> If you leave the column present and do not set a value, it will attempt to upload into the Root directory, which is valid for items such as folders, but not for resources such as Agent or Skill Group. Removing the column allows you to control the path via the Bulk Upload control screen.
Name	SNC	Yes	The name of the dimension in the Portal. This must be unique and will never be provisioned. <b>Note</b> an entry is required in this field
Description	-	Yes	Describes the dimension being created. This never gets provisioned. <b>Note</b> this field can be left blank
Enterprise Name	SNC	Yes	The name for the dimension being created. This does get provisioned and <b>cannot</b> be omitted. <b>Note</b> if you leave this field blank an Enterprise name is generated for you.

Column Name	Data Type	Column Required?	Column Description
Effective From	Date	No	The date from which the dimension is active from (default is today). <b>Note</b> an entry is required in this field if you do not delete the column, it must be in the format <Year>-<Month>-<Day>
Effective To	Date	No	The date from which the dimension is inactive (default is today). <b>Note</b> an entry is required in this field if you do not delete the column, it must be in the format <Year>-<Month>-<Day>

## Agent Template

For further information about the Data Type column in the table below, refer to **Data Types** section on page 12.

Column Name	Data Type	Column Required?	Description
Peripheral Member	Enterprise Name	Yes	The Peripheral where the Agent is assigned. <b>Note</b> an entry is required in this field
Desk Setting Member	Enterprise Name	No	The Desktop this Agent will use. <b>Note</b> an entry is required in this field if you do not delete the column
Agent Team Member	Enterprise Name	No	The team where the Agent is assigned. The team must be on the same Peripheral otherwise provisioning will fail. This column may be subject to capacity limitations; for example, there may only be so many agents allowed in a team and that team has already reached its capacity. <b>Note</b> an entry is required in this field if you do not delete the column
Portal Login	-	No	This column is a placeholder for a pending feature. <b>Note</b> Remove it before uploading.
First Name	SNC	Yes	The first name of the agent. <b>Note</b> an entry is required in this field
Last Name	SNC	Yes	The last name of the agent. <b>Note</b> an entry is required in this field
Login Name	SNC	Yes	The peripheral login name for the agent. <b>Note</b> an entry is required in this field

Pass Phrase	Password	Yes	The peripheral login password for the agent. In this release the password length can be set to 0 (zero). If the password length is set to 0 the agent is not required to login to the peripheral. <b>Note</b> this field can be left blank
Supervisor	Boolean	No	Indicates whether the agent is a supervisor. This will not create a Portal user, and is a pending feature; however it enables you to bind this agent to a domain login name. <b>Note</b> an entry is not required in this field if you retain this column
Peripheral Number	Numeric	Yes	The service number as known at the peripheral, <b>Note</b> an entry is required in this field
Agent State Trace	Y/N	No	Indicates whether the software collects agent state trace data for the agent. <b>Note</b> an entry is not required in this field if you retain this column
Domain Login Name	NETBIOS Login Name	No - if Agent is not a supervisor	The login name for the domain user the agent is bound to. This is only relevant if the Supervisor field is set to TRUE. Example: DOMAIN\USERNAME
Domain User Name	NETBIOS Username	No - if Agent is not a supervisor	The username of the domain user; therefore the <i>Login-name</i> : DOMAIN\USERNAME, the Username is simply USERNAME.

## Folders Template

Column Name	Data Type	Column Required?	Description
Security	CSS Styled List	No	Allows you to set security on the folder you upload, an example is shown below <b>Note</b> an entry is not required in this field if you retain this column

### Agent Security Field Example

The following is a Dos-styled syntax example:

```
<USERORGROUENAME> : <ROLENAME> ; <USERORGROUENAME> : <ROLENAME> [ : <MULTIPLEROLENAME> ]
```

This is an example of what can be entered in the **Security** field in the agent CSV file.

```
// #1 a single user with a single role
Administrator: Tenant User
// #2 a single user with more than one role
Administrator: Tenant User: Tenant Supervisor
// #3 multiple users
Administrator: Tenant User: Tenant Supervisor; User1: Tenant User
```

Users are separated by semicolons, and the user and roles are separated by colons. This is very similar to the CSS syntax with the exception that a user or group can have multiple roles rather than one value.

### Agent Desktop Template

Column Name	Data Type	Column Required?	Description
Wrap up Incoming Mode	Numeric	Yes	Indicates whether the agent is allowed or required to enter wrap-up data after an inbound call. 0= Required 1 = Optional 2= Not allowed <b>Note</b> an entry is required in this field
Wrap up Outgoing Mode	Numeric	Yes	Indicates whether the agent is allowed or required to enter wrap-up data after an outbound call. 0= Required 1 = Optional 2= Not allowed <b>Note</b> an entry is required in this field
Wrap-up Time	Numeric	Yes	The amount of time in seconds (1-7200) allocated to an agent to wrap up the call <b>Note</b> an entry is required in this field
Remote Agent Type	Numeric	Yes	Even though this field is mandatory, it is only used in Unified CCE Release 7.2 or later, see Unified CCE documentation for more details. <b>Note</b> an entry is required in this field

### Agent Team Template

Column Name	Data Type	Column Required?	Description
Peripheral Member	Enterprise Name	Yes	Same as Agent Peripheral Member. <b>Note</b> an entry is required in this field
Dialed Number Member	Enterprise Name	No	The dialed number to use for this Agent team. <b>Note</b> an entry is not required in this field if you retain this column

### Enterprise Skill Group Template

This template does not contain any dimension specific columns.

## Skill Group Template

For further information about the Data Type column in the table below, refer to **Data Types** section on page 12.

Column Name	Data Type	Column Required?	Description
Peripheral Member	Enterprise Name	Yes	Same as Agent Peripheral Member. <b>Note</b> an entry is required in this field
Peripheral Number	Numeric	Yes	Same as Agent Peripheral Number. <b>Note</b> an entry is required in this field
Peripheral Name	SNC	No	The name of the Peripheral as it is known on the site. <b>Note</b> an entry is required in this field if you retain this column
Available Hold-Off Delay	Numeric	No	The value for this Skill Group instead of using the one associated with this peripheral. <b>Note</b> an entry is not required in this field if you retain this column
IPTA	Y/N	No	Indicates whether Unified CCE picks the agent. <b>Note</b> an entry is not required in this field if you retain this column
Service Level Threshold	Numeric	No	The service level threshold, in seconds, for the service level. If this field is negative, the value of the Service Level Threshold field in the Peripheral table is used. <b>Note</b> an entry is not required in this field if you retain this column
Service Level Type	Numeric	No	For Non-Unified CCE, indicates how the Unified CCE software calculates the service level for the service. See the Unified CCE documentation to determine value meanings. Valid Values are 0, 1, 2 or 3. <b>Note</b> an entry is not required in this field if you retain this column
Default Entry	Numeric	No	Normal entries are 0 (zero). Any records with a value greater than 0 are considered a default skill group for configuration purposes. Records having a value of 1 are used by OPC as the default target skill group. <b>Note</b> an entry is not required in this field if you retain this column

Column Name	Data Type	Column Required?	Description
Extension	Numeric	Yes	The extension number for the service (used by Lucent DEFINITY ECS). <b>Note</b> an entry is required in this field

## User Variable Template

This template does not contain any dimension specific columns.

## Using the Bulk Upload Tool

To use the Bulk Upload tool, perform the following:

1. Open the **System Management** page.
2. Select the required tenant.
3. Click **Upload** and then select the item types you want to bulk upload from the drop-down list. The **Bulk Upload Control** page displays.

**Note** This path will only be used if you have removed the **Path** column in the CSV file. This is not relevant for folders as the path option is not available.

4. Select a template for your chosen dimension. The template link is present in the horizontal toolbar near the top of the page. Once selected, a download box displays allowing you to save this CSV file to your machine.
5. Save the file.

Once saved, you can open it in the editor you require and begin entering your data or paste it from another source.

6. Return to the **Bulk Upload Control** page and make sure the path is set correctly.
7. Browse to the CSV file where you entered data.
8. Click **Upload**.

A progress bar at the bottom of the screen displays the upload progress.

**Note** Do NOT upload more than 500 items per CSV file.

If an error occurs, pause the upload and check why an item failed. For further information about why uploads fail, please see the **Reasons for Upload Failure** later in this document.

If the Bulk Upload tool encounters a problem that affects all rows and not just the current one, an alert box appears that describes the problem and returns you to the **Bulk Upload Control** page.

Once every row has been processed, a summary dialog appears showing how many rows failed and how many passed. Please note that this dialog does not supply the result of provisioning these items; it only provides the result of uploading the items into the Unified CCMP system.

## Reasons for Upload Failure

The table below details the causes as to why an upload can fail.

Exception Type	Reason
No Capacity Left	The capacity limit has been reached.
Enterprise Name Already Exists	The enterprise name already exists.
Login Name Already Exists	The peripheral login name already exists.
SQL Exception	The SQL error during upload, usually due to bad data.
Argument Exception	An attribute contains a bad value. It is usually an exception because you have an empty string in the <b>Path</b> column when attempting to upload items which cannot live in the <b>Root</b> folder.
Security Exception	You do not have security permissions to upload to here.
Format Exception	Invalid data in a column.
No Identity Available	Identity not available.

# 5. Audit Trails

Unified CCMP enables provisioning users to view the audit histories of individual items. Users with sufficient privileges can run an audit report on Unified CCMP platform itself.

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

## Audit Histories

Each individual resource has its own audit history, showing all the events that have occurred on that resource. This can be accessed from the History tab when examining the resource in the System Manager.

The Edit Filter link allows you to choose to view only those events which were successful, or those events which failed, or to select events that took place between certain dates.

Some events are links; click on these to open up a table showing details of the event.

Finally, by clicking the icon associated with certain events, you can switch to viewing the other item involved.

## Audit Reports

Use the Reporting tool to view audit reports.

## Setting Up Audit Reporting

Audit reports are uploaded as part of the installation and commissioning of the Management Portal. Before an audit report can be viewed, however, it is necessary to set up at least one *parameter set*.

## Parameter Sets

Parameter sets determine what data displays; for example, a report parameter that is a single tenant will produce a report that displays only data associated with that tenant. Parameter sets must not be confused with report parameters, which are set at the time of viewing the report and determine which parameter set is used and how the report is laid out.

To create a parameter set:

1. Click **Reports** to open the Reporting tool.
2. Select the **Parameter Sets** option. The Parameter Sets page displays.
3. Select a folder. All the parameter sets for the selected folder displays.
4. Click **New** to display the Create a new parameter set page.
5. Select the item type to view from the **Item type** drop-down list.
6. Click **Create Parameter Set**.
7. From the **Folders** tab, select the folder containing the resources, and choose whether you will be adding items in subfolders as well.

8. From the **Resources** tab, select the resources. You may choose to see resources only from the folder you have selected or from its sub folders also.
9. Click **Add** to add the specified resources to the parameter set.
10. You may also remove resources from the parameter set by checking them and clicking **Remove**.
11. Select the **Save As** option.
12. In the **Name** field enter a name for the new report (parameter set).
13. Click **OK**.

## Viewing an Audit Report

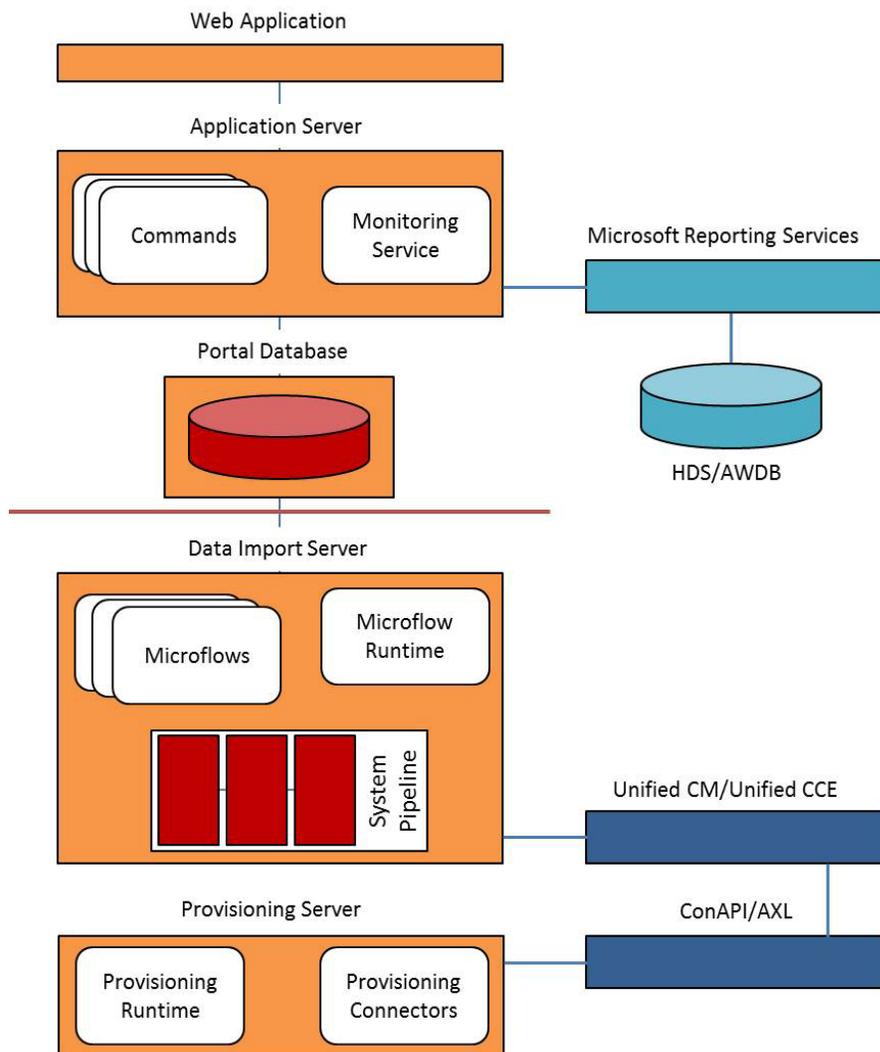
There are a number of audit reports available for use within the Management Portal. These are:

- **Audit Data Report** This report shows every provisioning change that has occurred within the system during the specified time period. This includes the name of the resource, the name of the user who made the edit, and whether the change was successful.
- **Daily Audit Summary** This summarizes the changes made to resources during the day, showing the percentage and total of successful and failed changes at different times for individual items.
- **Weekly Audit Summary** This summarizes the changes made to resources during the last week, showing the percentage and total of successful and failed changes on different days for individual items.
- **Monthly Audit Summary** This summarizes the changes made to resources during the last month, showing the percentage and total of successful and failed changes on different days for individual items.
- **Monitor Report** This shows the current state of the Portal's connections, essentially providing system monitoring (see Chapter 8) through the web interface.

More information on viewing reports is available in the *User Manual for Cisco Unified Contact Center Management Portal*.

# 6. System Architecture

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



## Web Application

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

The web application is hosted on the server by Microsoft Internet Information Services (IIS) and is suitable for lockdown in secure environments in line with the latest NSA Guidelines.

## Application Server

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

## Reporting Services

Unified CCMP utilizes **Microsoft Reporting Services** technology for generating audit reports. Microsoft Reporting Services is an integral part of SQL Server.

## Data Import Server

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

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

## Provisioning Server

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

The Unified CCMP Provisioning Service utilizes the Unified CCE ConAPI interface to commit changes to the Unified CCE.

Provisioning changes are managed via periodic cycles performed by the provisioning server. After a change has been committed by the ConAPI interface the Provisioning Server will wait a configurable period of time (5 seconds by default), before moving onto the next operation. This configurable throttle reduces the possibility of overloading Unified CCE during busy times. More information on configuring this setting are described in the Agent Self Re-Skilling and the Provisioning section.

The provisioning characteristics of this service are as follows:

- For Agent > Skill Group relationships, the provisioning server will batch together up to 100 requested operations into one request executed every provisioning cycle.

- For all other items (for example Agents, Agent Teams and so on), all items and relationships are treated as separate provisioning operation. These are executed one by one honouring the configured provisioning throttle between operation executions.
- By default this would mean that the creation of an Agent that is linked to 1 Agent Team and 2 Skill Groups would create the following provisioning operations:
  - Agent Creations
  - Agent > Agent Team relationship
  - Bulk Agent > Skill Group relationship

## Agent Self Re-Skilling and the Provisioning Service

The Agent Self Re-Skilling feature of Unified CCMP allows users the capability to re-skill themselves from the Unified CCMP interface. Because of the additional provisioning load generated on Unified CCE when enabling this feature, the provisioning throttle will automatically be configured to 30 seconds. This indicates that provisioning changes to Unified CCE will be made at a rate of one change every 30 seconds.

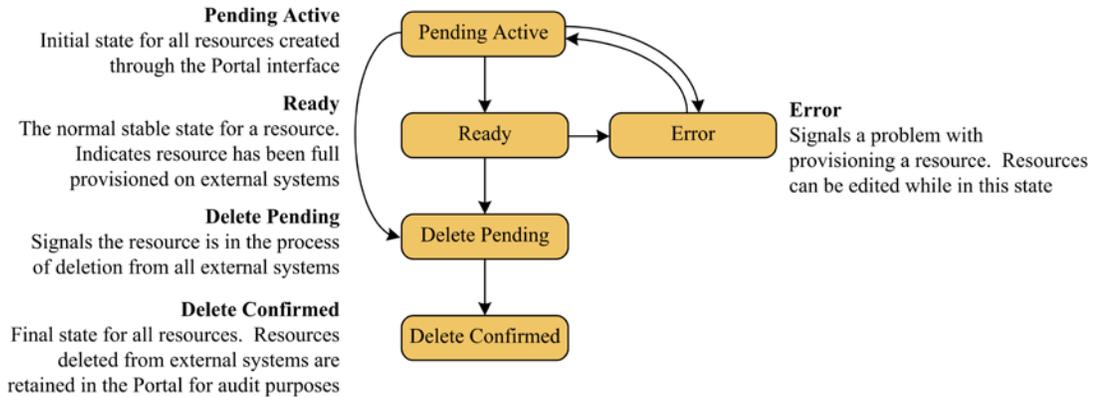
By default the Agent Self Re-Skilling feature is disabled. To enable this feature and the associated provisioning throttle, complete these steps:

1. Navigate to Unified CCMP Configuration Manager tool, click **Start > All Programs > Management Portal > Configuration Manager**.
2. Select the **Communication Servers** option and navigate to the **Unified ICM** tab.
3. Select the **Unified ICM** to which the Self Re-Skilling feature is to be enabled and press **edit**.
4. Select the **Self Skilling Enabled** check box.
5. Select **Yes** on the prompt asking if you are sure you want to enable Self Skilling.
6. Select **OK** to close the Unified ICM edit dialog.
7. Select **Save Changes** to make this change to the system.

This change may take up to 5 minutes to be reflected within Unified CCMP. After this period users will be able to access the Agent Self Re-Skilling interface and Unified CCE provisioning requests will be throttled to one every 30 seconds.

## Resource States

A resource is any kind of entity on the Unified Contact Center platform, for example agents, teams, skill groups and phones. All the resources in Unified CCMP participate in a *state machine*. A state machine is a collection of states which a resource will progress through during its lifetime. It is important to understand the state machine when trouble shooting problems in Unified CCMP. The states are shown below:



## State Descriptions

### Synchronize

**Synchronize** is the initial state for all dimension items created through Unified CCMP.

Each dimension type (agent, tenant, skill group and so forth) has a separate idempotent **Synchronize** microflow. (By *idempotent* it is meant that no matter how many times the microflow is launched, conflicts or errors will not be generated as a result). The role of the **Synchronize** microflow is to bring all externally controlled systems in line with Unified CCMP database.

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

### Ready

**Ready** is the normal state of a dimension item in Unified CCMP database. It indicates that the dimension item has been fully provisioned on all the external systems controlled by Unified CCMP.

If the user interface edits a dimension item then it is changed to the **Synchronize** state.

### Error

**Error** state signals that an error has occurred while provisioning a dimension item.

There are two methods to resolve the error state of a dimension item:

- Delete the dimension item either through Unified CCMP user interface, or in an external system. In both cases the state of the dimension item is changed to **Delete Pending**. Note that if the dimension item is deleted on an externally controlled system then it is the importer microflow that changes the dimension item to the **Delete Pending** state.
- Edit the dimension item in Unified CCMP user interface, which changes the state to **Synchronize**.

## Delete Pending

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

The **DELETED** flag and **EFFECTIVE\_TO** fields on the dimension item row in the **TB\_DIM\_ITEM** table must be set in the transition to this state. User interface operations are not allowed on a dimension item which is **Delete Pending** – editing in particular.

Each dimension type (agent, tenant, skill group and so forth) has a separate idempotent **Delete Pending** microflow. (By *idempotent* it is meant that no matter how many times the microflow is launched, conflicts or errors will not be generated as a result). The role of the **Delete Pending** microflow is to delete the item from all externally controlled systems. Once all the changes have been made, the dimension item is changed to the **Delete Confirmed** state.

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

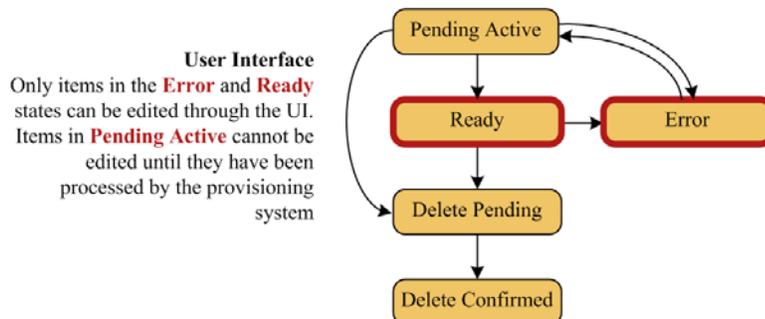
## Delete Confirmed

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

## User Interface

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

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



## Database Codes

The dimension state field in the **TB\_DIM\_ITEM** table uses the following codes:

Code	State	Description
R	Ready	Ready is the normal state of a dimension item in Unified CCMP database. It indicates that the dimension item has been fully provisioned on all externally controlled systems.
S	Synchronize	Synchronize is the initial state for all dimension items created through Unified CCMP.
P	Delete Pending	The Delete Pending state signals the dimension item is to be deleted from all externally controlled systems. The EFFECTIVE_TO and DELETED fields are also set in the TB_DIM_ITEM table.
D	Delete Confirmed	A dimension item transitions to the Delete Confirmed state once it has been deleted from all externally controlled systems.
E	Error	The Error state signals an error occurred provisioning a dimension item.

## Memberships

Memberships in Unified CCMP database also have effective dating and a status. The **Synchronize** microflows ensure that changes to memberships are reflected on any externally controlled system. The state of a dimension item shows whether it has been provisioned on all external systems (for example, whether an agent has been added to Unified CCE). The state also reflects whether all its memberships are up to date and fully provisioned. This approach easily indicates an item's state on the user interface.

## State Machine Scenarios

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

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

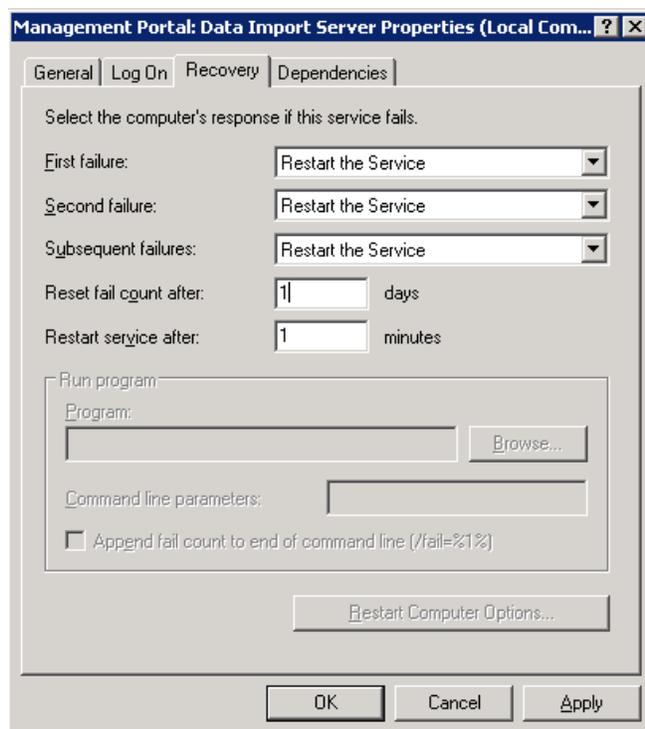


# 7. System Operations

## Service Restart Configuration

To configure the services for automatic restart on failure:

1. Click **Start > All Programs > Management Portal > Data Import Server**.
2. Select **Recovery** tab.
3. Select **Restart the Service** from the drop-down list for each failure type shown.



## Database Backup and Recovery

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

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

The Data Import Server is enabled through the **EnabledTime** attribute in the Data Import Server service configuration file (**DataPipelineService.exe.config**). In the example below, the Data Import Server processes microflows from 3:00 through to

2:00 (24 hour clock). This effectively disables the Data Import Server for an hour at 2am. Note that an import cycle could start just before 2:00 and so may still be running after 2:00.

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

## Manual Provisioning/Importer Failover

In a distributed deployment of Unified CCMP, there may be only one active import server and one active provisioning server. These resources usually reside on the same database server flagging that server as the active provisioning and import server.

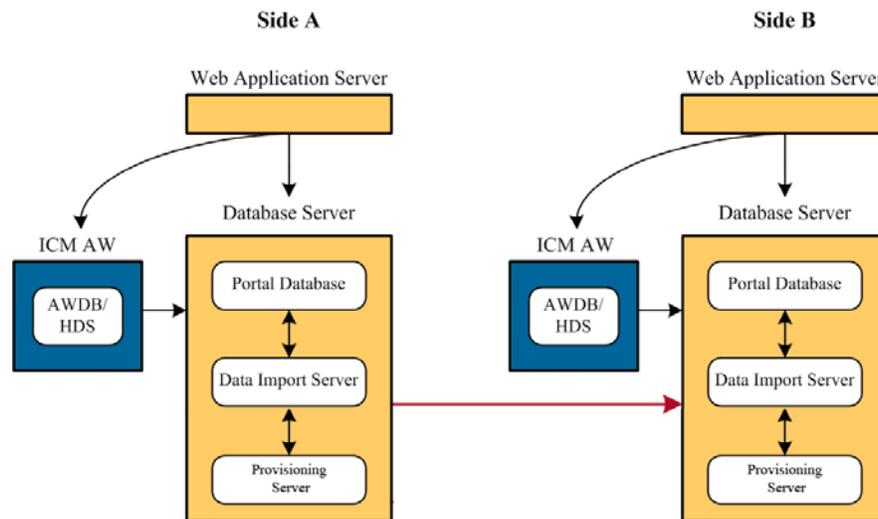
To identify the server that is currently the active provisioning server you can run the following query on either side of the system:

```
SELECT s.SERVER_NAME FROM TB_CLU_GROUP g
JOIN TB_CLU_SERVER s ON s.SERVER_ID = g.SERVER_ID
WHERE g.NAME = 'Provisioning' and g.type = 'F'
```

To identify the server that is currently the active import server you can run the following query on either side of the system:

```
SELECT DISTINCT s.SERVER_NAME FROM TB_CLU_GROUP g
JOIN TB_CLU_SERVER s ON s.SERVER_ID = g.SERVER_ID
WHERE g.NAME <> 'Provisioning' and g.type = 'F'
```

Changing the active import/provisioning server to an alternate side is a manual process. Within this set of steps, the active side is taken to mean the active importer/provisioning server **before** the switch (database A in the diagram below).



## Changing the Active Provisioning Server

1. Stop the UCCMP: Provisioning Server Service on both sides of the system.
2. On the active importer open **SQL Server Management Studio** and connect to Unified CCMP database.

3. Execute the following SQL script, specifying the name of the server to become the active provisioning server:

```
UPDATE TB_CLU_GROUP
SET SERVER_ID = (SELECT SERVER_ID FROM TB_CLU_SERVER
WHERE SERVER_NAME = '<ServerName>')
WHERE NAME = 'Provisioning' and type = 'F'
```

4. Restart the UCCMP: Provisioning Server Service on both sides of the system.

## Changing the Active Resource Import Server

1. Stop the UCCMP: Data Import Server Service on both sides of the system.
2. On the active importer open **SQL Server Management Studio** and connect to Unified CCMP database.
3. Execute the following SQL script, specifying the name of the server to become the active import server:

```
UPDATE TB_CLU_GROUP
SET SERVER_ID = (SELECT SERVER_ID FROM TB_CLU_SERVER
WHERE SERVER_NAME = '<ServerName>')
WHERE NAME <> 'Provisioning' and type = 'F'
```

4. Restart the UCCMP: Data Import Server Service on both sides of the system.

## 8. Connection Monitoring

The status of the connections used by Unified CCMP can be monitored using the Management Portal's Configuration Manager. Open it by clicking **Start > All Programs > Management Portal > Data Import Server > Configuration Manager**. Click the **Connection Manager** button and open the **Connections** tab.

From here, you can edit connection details and attempt to repair failing connections.

**Note** The monitor automatically refreshes every few seconds.

### Performance Counters

Unified CCMP integrates with Windows performance counters (accessed by running the **perfmon** command) to provide real time activity monitoring. Portal appears as up to five separate objects in **perfmon**, each with a number of associated performance counters.

The **perfmon** graph can combine many different performance counters. Furthermore, **perfmon** can be configured to trace specific counters at scheduled times of the day. These performance logs can then be exported to Excel for further analysis. **Perfmon** can also connect to remote computers, if necessary.

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

### CCMP Data Pipeline Object

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

## CCMP Application Datasources Object

Counter	Monitors
<CICM AWDB server>\Health	Current datasource health score
<OLAP server>\Health	Current datasource health score
<RDBMS server>\Health	Current datasource health score
<Reporting Services server>\Health	Current datasource health score

## CCMP Application Monitoring Object

Counter	Monitors
Connection Requests/Second	Connection requests processed per second
Connection Requests/Total	Total connection requests processed

## CCMP Application Server Object

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

# Index

- administrator
  - account, 5
  - host, 3
  - tenant, 7
- agent desktop templates, 15
- agent team templates, 15
- agent templates, 13
- application server, 1, 22
- audit history, **19**
- audit reports, 19, 22
  - viewing, 20
- audit trails, **19**
- authentication, 5
- bulk upload, 11
  - failure, **18**
  - tool, 17
- connection monitor, 33
- creating
  - prefixes, 4
  - tenant administrator, 7
- CSV files, 11
  - editing, 11
- data import server, 1, 22, 29
- data types, 12
- database
  - backup and recovery, 29
- database codes, 26
- database server, 1
- delete confirmed state, 25
- delete pending state, 25
- editing
  - CSV files, 11
- error state, 24
- folder templates, 14
- global templates, 11
- host administrator
  - responsibilities, 3
- Internet Information Services Manager (IIS), 21
- memberships, 26
- passwords
  - resetting, 8
  - rules, 8
- perfmon, 33
- performance counters, 33
- prefixes
  - creating, 4
  - deleting, 5
  - editing, 4
  - viewing, 4
- provisioning server, 1, 22, 30
- ready state, 24
- reporting services, 22
- resource states, 23
- restart, 29
- servers
  - application, 22
  - data import, 22, 29
  - provisioning, 22, 30
- single sign-on, 5
  - managing users with, 7
- skill group templates, 16
- SSO. *See* single sign-on
- state machine scenarios, 27
- states, 23
  - delete confirmed, 25
  - delete pending, 25
  - error, 24
  - ready, 24
  - state machine scenarios, 27
  - synchronize, 24
- synchronize state, 24

system manager, 9

templates, 11

- agent, 13

- agent desktop, 15

- agent team, 15

- folder, 14

- global, 11

- skill group, 16

tenant administrator, 3

tenant folder, 3, 4

tenants

- importing, 3

- tenant administrator, 3

- tenant administrators, 7

- tenant folder, 3, 4

user interface, 25

user types, 3

web application, 21

web server, 1, 3