Troubleshooting Guide for Cisco Unified Contact Center Management Portal

Release 7.2(1)

May 2007

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

TABLE OF CONTENTS

PREFACE

Purpose

This document explains how to adminstrate and provision the Unified Contact Center Management Portal platform.

Audience

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

Organization

Chapter 1, "Initial Checks"

Lists the initial checks to be made if experiencing problems with the Unified Contact Center Management Portal.

Chapter 2, “Operational Overview”

Describes how the system operates, including system architecture, possible resource states and the effects events have on these states.

Chapter 3, "System Operations"

Describes best practices within the Unified Contact Center Management Portal system and the actions to take in the event of problems with the server components.

Chapter 4, "Management Portal"

Describes how to troubleshoot problems that may arise when using the Unified Contact Center Management Portal to manage resources and security. A list of user-friendly error codes is included.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems

Attn: Customer Document Ordering

170 West Tasman Drive

San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.
Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- iQ Magazine is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

1. INITIAL CHECKS

Check that you have performed the following for all Unified Contact Center Management Portal servers in the deployment:

- Installed Windows Operating Systems and relevant service packs.
- Installed the pre-requisite applications required per component.
- Setup network connectivity.
- Installed the Unified Contact Center Management Portal software.
- Setup and run services.
- Installed virus checkers.
- Installed other third party software.
- Applied Windows hot fixes.

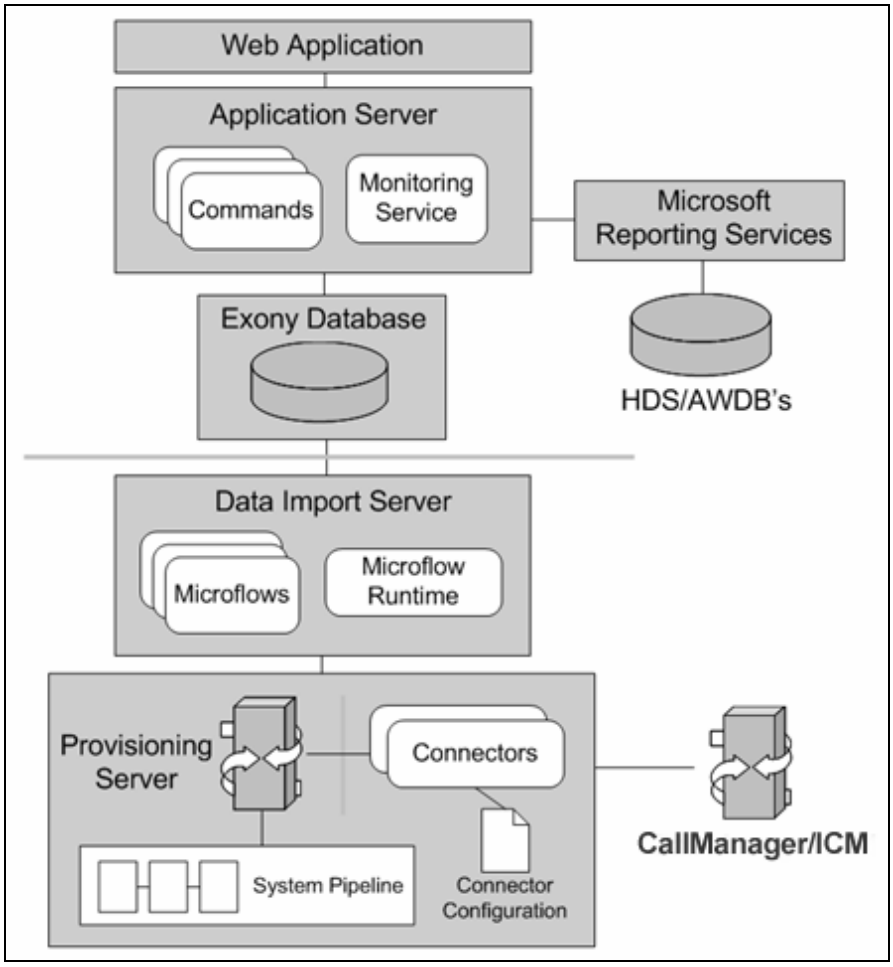
If there is a user related problem, check that you have performed the following for the client machine:

- Installed Windows Operating Systems and relevant service packs.
- Installed the correct client browser version.
- Applied the correct Internet Explorer security settings.
- Setup the connection to the HTTP/HTTPS server.
- Installed virus checkers.
- Installed other third party software.
- Applied Windows hot fixes.

The guide starts with a system overview to set a context for the troubleshooting cases.

2. OPERATIONAL OVERVIEW

The Unified Contact Center Management Portal 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 2000 database. The lower half of the system architecture is a process orchestration layer called the Data Import Server and a systems integration layer called the Provisioning Component.



Web Application

The user interface to the Unified Contact Center Management Portal is via a web application that is accessed by a web browser (Microsoft Internet Explorer). Access to the Unified Contact Center Management Portal application 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 define the system functions the user can access and perform.

The user interface is time-zone aware and connections to it are secured through HTTPS. The web application is hosted on the server by Microsoft Internet Information Services (IIS) and so is suitable for lockdown in secure environments.

Application Server

The Unified Contact Center Management Portal **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

The Unified Contact Center Management Portal utilizes **Microsoft Reporting Services** technology for generating reports. Microsoft Reporting Services is an integral part of SQL Server Enterprise Edition. The Unified Contact Center Management Portal provides a flexible reporting system in which reports are authored in the industry standard Report Definition Language (RDL).

Data Import Server

The **Data Import Server** component is an Extract, Transform and Load application for the Unified Contact Center Management Portal. The Data Import Server component imports the data used in the Unified Contact Center Management Portal. It is designed to handle high volume data (facts), such as call detail records as well as data which is changed irregularly (resources), such as agents, peripherals and skill groups.

The Data Import Server component is also responsible for monitoring changes in the Unified Contact Center Management Portal system and ensuring that those changes are updated onto the Cisco ICM and CallManager. The Data Import Server component orchestrates the creation, deletion and update of resources to the Cisco ICM and CallManager.

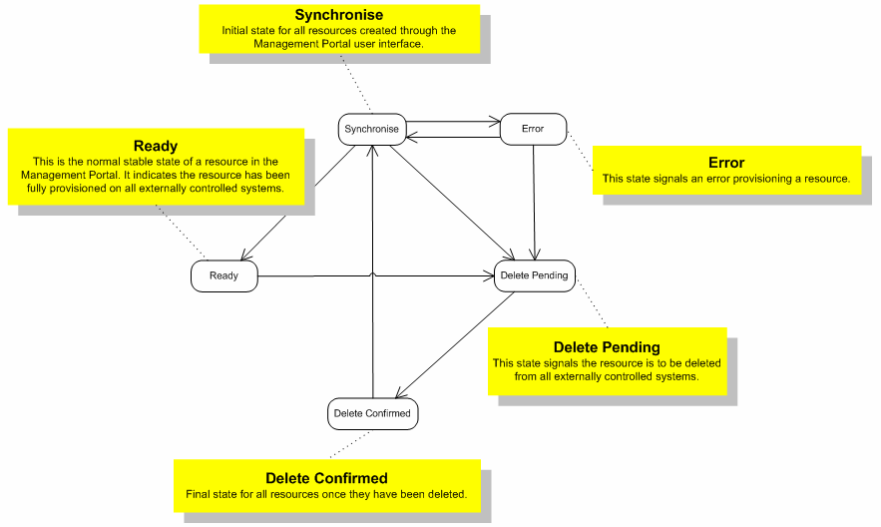
The **Microflow Runtime** is the heart of the Data Import Server component. It orchestrates systems without resorting to low level programming languages. The Microflow Runtime is a general purpose scripting environment and can be applied to a wide range of problems. The term *microflow* describes any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

The Management Portal Provisioning Server

The Unified Contact Center Management Portal **Provisioning Server** component provides the connections to remote systems such as the Cisco ICM and CallManager. Using the Provisioning Server component to access remote systems provides a tried and tested way to manage, monitor and secure system connections. The Unified Contact Center Management Portal Provisioning Server component provides many advanced features including connection management, fault tolerance and automatic failover between connected systems.

Resource States

A resource is any kind of entity on the Cisco ICM or CICM and CallManager, for example agents, teams, skill groups and phones. All the resources in the Unified Contact Center Management Portal 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 the Unified Contact Center Management Portal. The states are shown below:



State Descriptions

Synchronize

Synchronize is the initial state for all dimension items created through the Unified Contact Center Management Portal.

It is also the initial state for any dimension item that is created by the importer. This ensures that dimension items created on an external system, such as a CICM, are provisioned on all other systems controlled by the Unified Contact Center Management Portal**,** such as the CallManager.

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 the Unified Contact Center Management Portal 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 the Unified Contact Center Management Portal database acts as conflict master.

Ready

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

If the user interface edits a dimension item then it is changed to the **Synchronize** state. If an importer microflow updates a dimension item (perhaps the agent's name was changed on the source system) then it also changes to the **Synchronize** state.

Error

The **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. The first is to delete the dimension item either through the Unified Contact Center Management Portal 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.

The second is to edit the dimension item in the Unified Contact Center Management Portal 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. Once it has been changed to **Delete Confirmed** then the dimension item can be reactivated.

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 the Unified Contact Center Management Portal Provisioning component ConAPI (ICM) and CallManager connectors always check to see if the dimension item is valid before starting a delete operation (this ensures the **Delete Pending** microflow is idempotent. 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).

Delete Confirmed

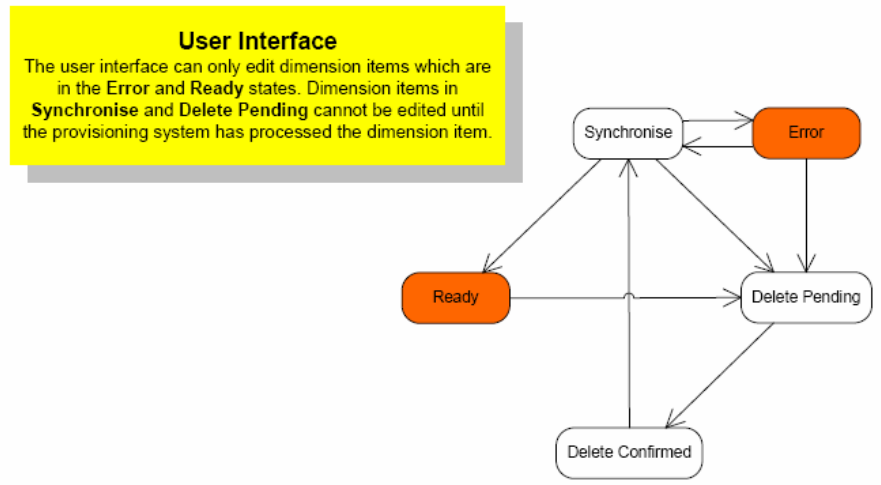
A dimension item changes to the **Delete Confirmed** state once it has been deleted from all externally controlled systems. The **Delete Pending** microflow runtime ensures all externally controlled systems are updated before the transition occurs. The microflow must also ensure any memberships are reset,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

The only action allowed in the **Delete Confirmed** state is to reactivate the dimension item (reactivating dimensions such as agents is a particularly powerful feature in the user interface) which returns it to the **Synchronize** state ready for provisioning. The **DELETED** flag and **EFFECTIVE_TO** fields on the dimension item row in the **TB_DIM_ITEM** table must also be reset as part of the reactivate transition.

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 provisioning 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 the Unified Contact Center Management Portal 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 Contact Center Management Portal.
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 the Unified Contact Center Management Portal 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 an ICM). The state also reflects whether all its

memberships are up to date and fully provisioned. This approach makes it easy in the user interface to show an item's state.

Example Synchronize Microflow

The following steps illustrate the function of a **Synchronize** microflow:

1. A new tenant is created through the Unified Contact Center Management Portal user interface. This creates a new row in the **TB_DIM_ITEM** table and the derived dimension table (for tenants this derived table is called **TB_DIM_TENANT)**.
2. The creation of a tenant also triggers the creation of a range of additional tenant specific entities in the Unified Contact Center Management Portal database. Examples include a tenant specific folder, and default tenant user / administrator groups. However, these additional entities are not central to explanation of this life cycle.
3. The state of the new tenant is **Synchronize**.
4. The provisioning system runs periodically. Each dimension type (agent, tenant, skill group and so forth) has its own **Synchronize** microflow. The tenant **Synchronize** microflow is run by the Unified Contact Center Management Portal Data Import component and picks up the new tenant through a SQL query against the Unified Contact Center Management Portal database.
5. The **Synchronize** microflow creates a new customer definition on the required ICM or CICM instance. The customer definition is created through the Gateway ConAPI connector. The resulting **CustomerDefinitionID** primary key allocated by ConAPI is stored in the **TB_DIM_ITEM_PKEY** table for that ICM/CICM instance's **CLUSTER_RESOURCE** identifier.
6. The **Synchronize** microflow then uses the Unified Contact Center Management Portal Provisioning component CallManager connector to create a new Calling Search Space. The microflow also creates a new dimension in the Unified Contact Center Management Portal **TB_DIM_CALLING_SEARCH_SPACE** table. The Calling Search Space's GUID is stored in the **TB_DIM_ITEM_PKEY** table for that CallManager's **CLUSTER_RESOURCE** identifier.
7. Route Partitions are then created in the CallManager. The microflow ensures new dimensions are added to the **TB_DIM_ROUTE_PARTITION** table as necessary. The Calling Search Space and Route Partitions are joined up in the CallManager and members are created in the Unified Contact Center Management Portal membership table: **TB_DIM_ROUTE_PARTITION_ CALLING_SEARCH_SPACE_MEMBER**

Note The Provisioning component connectors check to see if a resource already exists on an externally controlled system before attempting

to create it. This is not always possible but generally avoids duplicate resources after server crashes. If a resource already exists on an externally controlled system, then the Gateway connector just looks up and returns the primary key for that resource.

8. The tenant is now updated by the microflow to the **Ready** state.

State Machine Scenarios

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

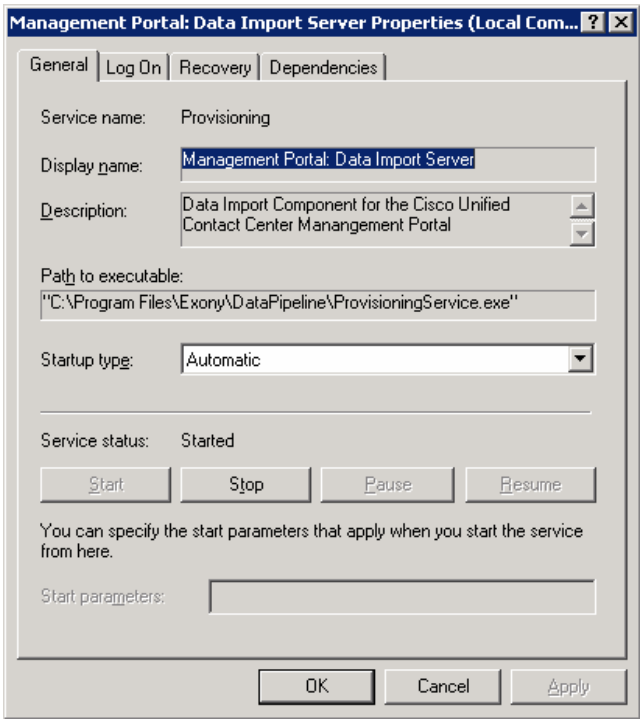
Scenario	Expected Result
Dimension item is created and provisioned (transitioning it to the **Ready** state). It is then deleted from one of the externally controlled systems.	Dimension item is transitioned to the **Delete Pending** state in the Unified Contact Center Management Portal.
Dimension item in the **Delete Pending** state is deleted from a different external system.	Dimension item is left in the **Delete Pending** state.
Dimension item in the **Delete Pending** state is reactivated on an externally controlled system.	Dimension item is left in the **Delete Pending** state and will be deleted on all externally controlled systems
Dimension item in the **Delete Confirmed** state is reactivated on an external system.	Dimension item is left in the **Delete Confirmed** state. Reactivation is only possible through the Unified Contact Center Management Portal system.
Dimension item fails to provision correctly; perhaps there is a network connectivity issue between the Unified Contact Center Management Portal and the CallManager.	Dimension item is transitioned to the **Error** state. Any systems it was correctly provisioned on are reflected in the Unified Contact Center Management Portal database. Details of the provisioning problem are available in the audit tables.
Dimension item fails to provision correctly and is then deleted in the Unified Contact Center Management Portal system.	Dimension item is transitioned to the **Delete Pending** state in the Unified Contact Center Management Portal.
Dimension item partially fails to provision correctly and is then deleted in an externally controlled system.	Dimension item is transitioned to the **Delete Pending** state in the Unified Contact Center Management Portal.

Dimension item in the **Error** state is deleted from an externally controlled system.	Dimension item is transitioned to the **Delete Pending** state in the Unified Contact Center Management Portal.
The Unified Contact Center Management Portal 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 **Synchronize**. The synchronization may take some time to run but ensures all externally controlled systems are in line with the Unified Contact Center Management Portal database. Any dimension items reactivated since the backup was taken have to be manually re-processed.
The Unified Contact Center Management Portal fact table importer creates a new dimension item.	Dimension item is created in the **Synchronize** state so that all externally controlled systems are brought in line.
Just prior to a server crash, a dimension item was created on an externally controlled system but was not updated in the Unified Contact Center Management Portal database.	The next time the **Synchronize** microflow runs, it brings back the existing primary key for the dimension item on the externally controlled system and updates its identity in the Unified Contact Center Management Portal database table **TB_DIM_ITEM_PKEY**.

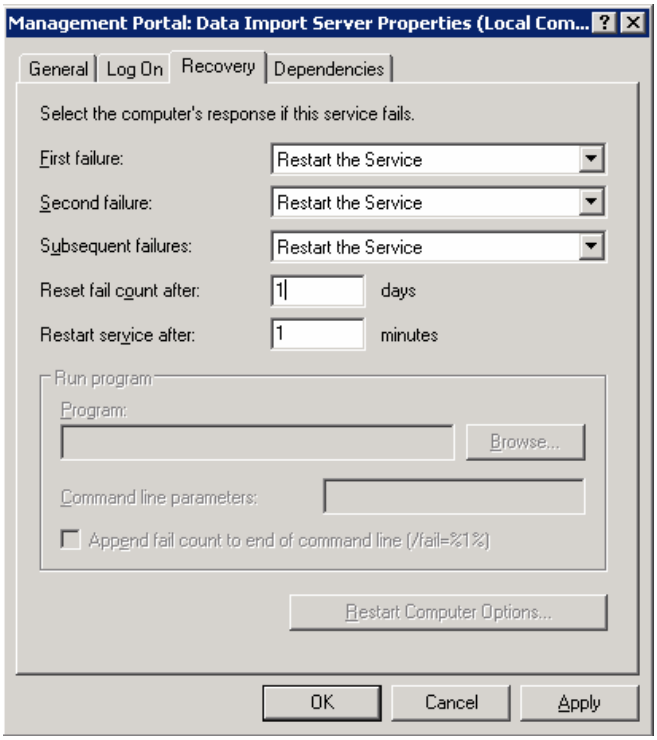
3. SYSTEM OPERATIONS

Service Restart Configuration

All the Unified Contact Center Management Portal services should be configured to restart automatically.



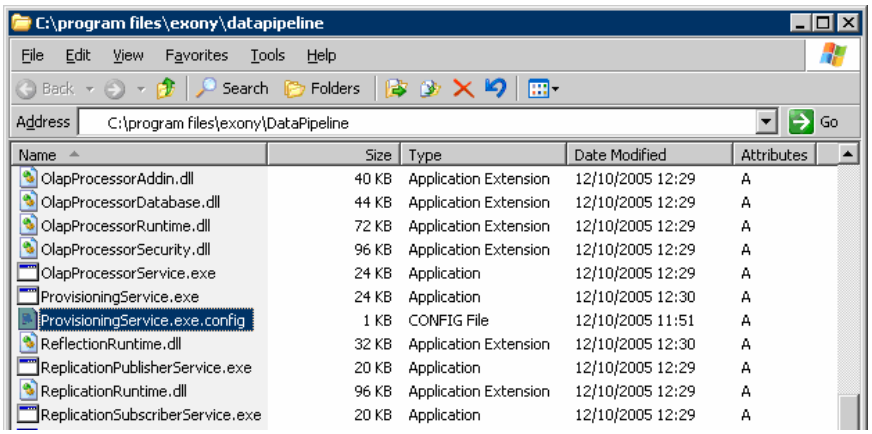
It is recommended to configure the services for automatic restart on failure.



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. It is not recommended to 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.



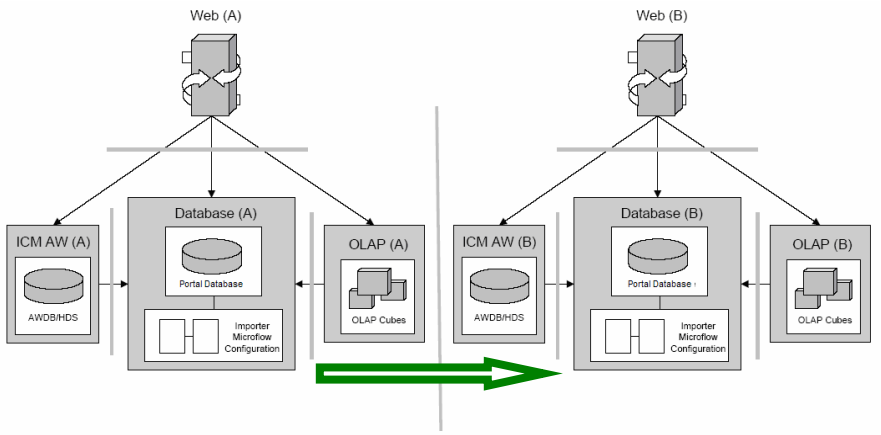
The Data Import Server is enabled through the **EnabledTime** attribute in the Data Import Server service configuration file (**ProvisioningService.exe.config**). In the example below, the Data Import Server processes microflows from 3:00 through to 2:00 (24 hour clock). This effectively disables the 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.

```
<configuration>
    <appSettings>
        <add key=”EnabledTime” value=”03:00-02:00” />
    </appSettings>
</configuration>
```

Changing the Active Importer Server

In a distributed deployment of the Unified Contact Center Management Portal, only one database server can be the active importer. Changing the active importer to an alternate side is a manual process. Within this set of steps, the active side is taken to mean the active importer/publisher **before** the switch (database **A** in the diagram below). If you need to check which machine is the current importer/publisher, the following SQL query returns the current active importer:

```
SELECT TOP 1 server.SERVER_NAME
FROM TB_CLU_GROUP grp
JOIN TB_CLU_SERVER server
ON server.SERVER_ID = grp.SERVER_ID
WHERE grp.SERVER_ID IS NOT NULL
```



1. On the active importer open SQL Server Query Analyzer and connect to the Unified Contact Center Management Portal database. Run the following query and paste the results into a text file. You will need these results to complete step five.

   SELECT GROUP_ID FROM TB_CLU_GROUP WHERE SERVER_ID IS NOT NULL

   The results should look something like:

   C617D006-8A1B-44F2-BB1B-592BA9FA3958

   98DC97B7-E519-41AF-893C-580D94ACEE4F

   17C25CA8-E257-4929-ABD8-1AB443534102

   F648492C-9AC1-4B89-98AD-9F5FBF20CC35

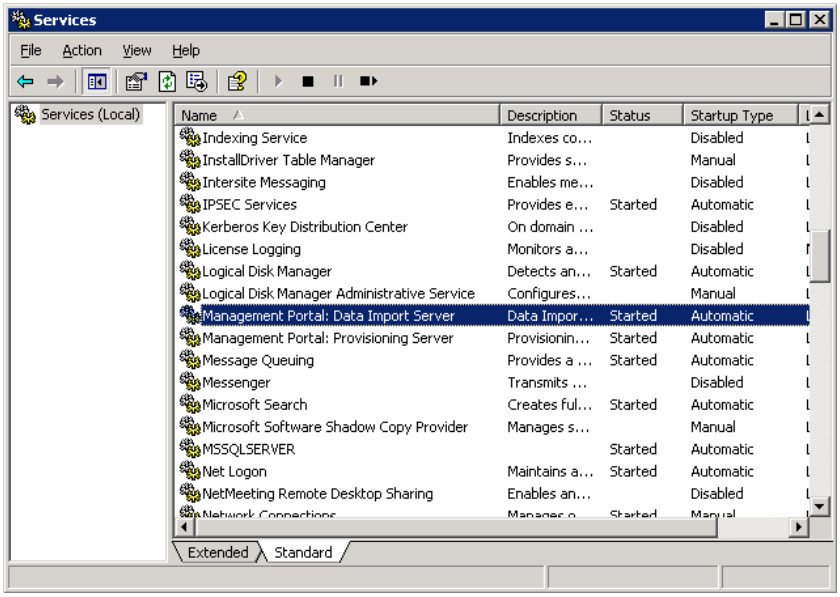
   D562A378-8EBE-4A41-9A34-E8B0F126CBA5

2. Then run the following SQL query:

   UPDATE TB_CLU_GROUP SET SERVER_ID = NULL

3. Before taking the Data Import component server down, wait for the current import cycle to complete and replication to complete synchronization. You need to wait until there are no folders in the **\IMPORTER\ToReplicate** folder on the publisher and **\IMPORTER\Replicated** on the subscriber. This indicates that the importer has finished its current cycle and replicated the facts on to the other side. Note that this may take a while during busy periods.

   At this stage the current database server is no longer the active importer. The Data Import Server continues to run after this update and completes the current import cycle but it will not begin a new import cycle.



Note that system stabilization cannot occur unless SQL Server and the Unified Contact Center Management Portal Replication services are running correctly. During the stabilization the Data Import Server and Replication services must both be left running on all servers.

4. Once the system has stabilized, stop the Data Import Server and the Unified Contact Center Management Portal Replication services on both sides. Open **Replication.xml** on the Publisher/active importer side and comment the following line:

   <Subscriber Name="RemoteSubscriber"
   Address="INACTIVE_SERVER_NAME " Port="7500"/>

This file can be found in the **Config** folder in the Data Import component server installation. Open the same file on the **inactive** side and modify the same line to point to the active server (you may need to uncomment the line).

<Subscriber Name="RemoteSubscriber"
Address="ACTIVE_SERVER_NAME" Port="7500"/>

5. Again, using SQL Query Analyzer run the following query against the Unified Contact Center Management Portal database (this can be done on either database server).

   SELECT SERVER_ID,SERVER_NAME FROM TB_CLU_SERVER

The results should look something like:

276824E5-F4BA-4E4C-A565-7F190A365EE1
XWEBTEST

43CA649D-F72B-49E3-B787-AC1966543617 10.10.10.10

3639C7E0-E059-4D04-B1AC-5336840664D2 10.10.10.11

Make a note of the **SERVER_ID** for the server you wish to set as the active importer. For example, **XWEBTEST** has a **SERVER_ID** of 276824E5-F4BA-4E4C-A565-7F190A365EE1. Using the **GROUP_ID** result set shown earlier and the **SERVER_ID** just obtained, adapt the following query.

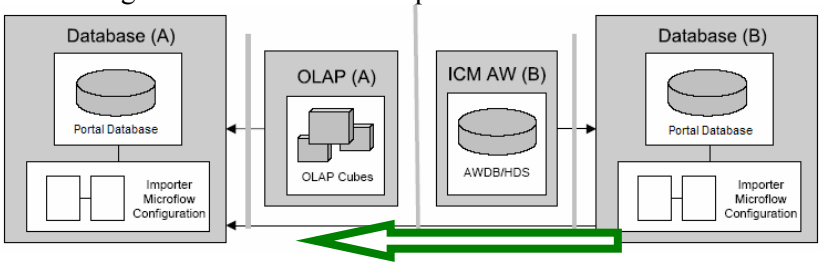
```
UPDATE TB_CLU_GROUP
SET SERVER_ID = '<NEW_ACTIVE_IMPORTER_SERVER_ID>'
WHERE GROUP_ID IN
('<GROUP_ID_FROM_EARLIER>',
'<GROUP_ID_FROM_ EARLIER >',
'<GROUP_ID_FROM_ EARLIER >',
'<GROUP_ID_FROM_ EARLIER >',
'<GROUP_ID_FROM_ EARLIER >')
```

Example using the **GROUP_ID** result set shown earlier:

```
UPDATE TB_CLU_GROUP
SET SERVER_ID = '7707C4EF-F58A-412C-9BA8-1A108409B379'
WHERE GROUP_ID IN
('C617D006-8A1B-44F2-BB1B-592BA9FA3958',
'98DC97B7-E519-41AF-893C-580D94ACEE4F',
'17C25CA8-E257-4929-ABD8-1AB443534102',
'F648492C-9AC1-4B89-98AD-9F5FBF20CC35',
'D562A378-8EBE-4A41-9A34-E8B0F126CBA5')
```

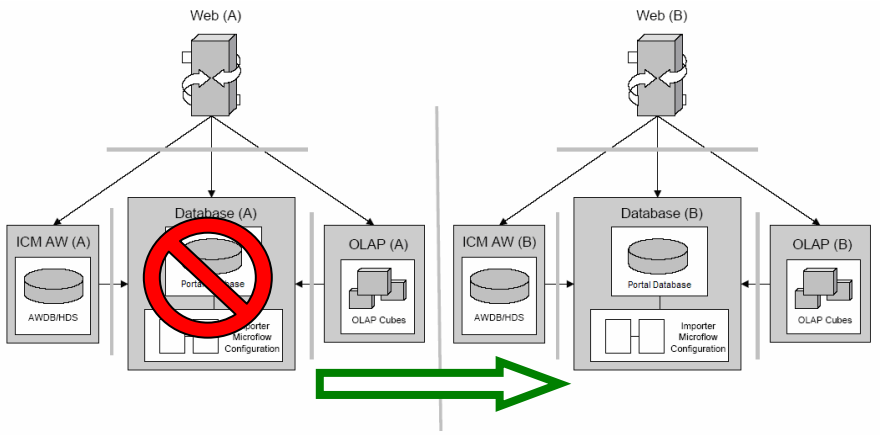
6. Start the Data Import Server service on both sides. Start the Unified Contact Center Management Portal Replication Subscriber and Publisher Service on both servers. The system will then start importing on the other side as normal. Assuming that the SQL Server and Unified Contact Center Management Portal Replication services have been configured correctly, the imported data should start being replicated.

The SQL Server Replication Monitor Manager can help verify this. The **Replicated** folder on the original server should also show data arriving from the new active importer.



Active Importer Server Crash

If a server crash or otherwise unrecoverable error occurs on the active importer then the other side needs to be brought into service as quickly as possible. The Data Import Server is designed to minimize the down time before importing can be restarted.



The following steps describe the actions to perform on the **inactive** side.

Turn off the Data Import Server and Management Portal Replication Subscriber - it is very important that these services shutdown properly otherwise the system may be in an inconsistent state. If either of these fails to shutdown properly then they should be restarted and allowed to run for at least ½ an hour. This should give them sufficient time to recover their state and rollback any inconsistencies.

Check the **TS_IMP_DIRECTORY_STATUS** table – this table contains one row for each replicated session directory. If there are any rows in this table which have a status other than **F** then the database state is inconsistent. The only recourse is to restart the Data Import Server to give it time to recover. After ½ an hour or so shutdown the Data Import Server service again. If there are still unfinished session directories then a double error has occurred in the platform – to correct this problem the database must be restored from backup before importing can proceed.

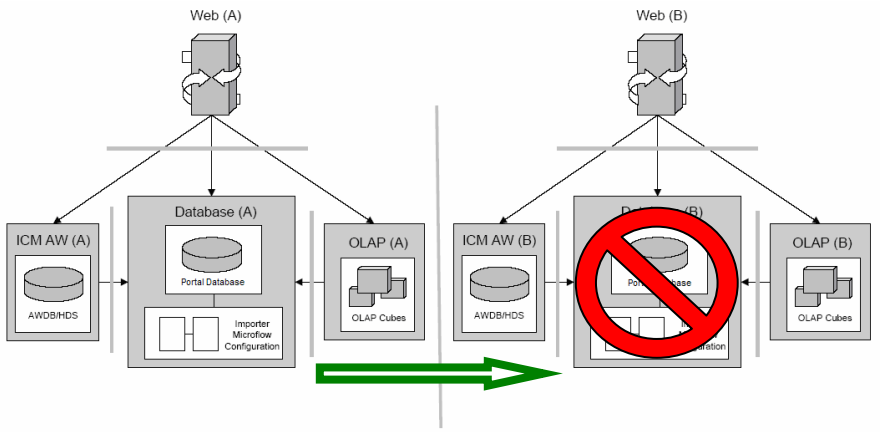
Assuming the services shutdown correctly and there were no unfinished session directories in the **TS_IMP_DIRECTORY_STATUS** table. The next step is to completely clear out the **Replicated** folder as it contains imported information from the crashed server and cannot be guaranteed. The data may also contain references to resources which will never arrive as the SQL Server replication link is down.

Finally, set the import token to active and restart the Data Import Server services. The process for restoring what was the active importer is described in the next section.

Inactive Importer Server Crash

Another failure mode to consider is a server crash which is not the active importer.

This scenario does not break import processing on the active importer. Data will continue to be imported on the active side and session directories will accumulate in the **ToReplicate** folder. These session directories cannot be replicated to the other side as it is unavailable so these will quite quickly use up available disk space.



The recommended approach is to re-configure **Replication.xml** on the active importer and remove the crashed server. All entries in the **ToReplicate** folder should then be deleted. This configuration change stops the disk filling up on the active importer.

```
<Replication>
  <Publisher PublisherId=”ReplicationPublisher” ChunkSize=”65536”
  Directory PollInterval=”1000” BroadcastPeriod=”10000”
  ToReplicateDirectory=”\Importer\ToReplicate”
  ReconnectionPeriod=”15000”>
    <LinkedServers>
      <Subscriber Name=”RemoteSubscriber” Address=”127.0.0.1”
      Port=”7500” />
    </LinkedServers>
  </Publisher>
  <Subscriber SubscriberId=”ReplicationSubscriber” Port=”7500”
  ReplicatedDirectory=”\IMPORTER\Replicated” />
</Replication>
```

Once the failed server has been fixed, the following steps should be taken:

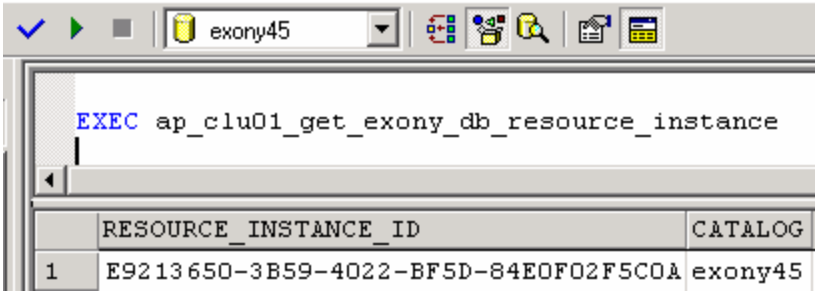
1. Switch off the Data Import Server and Unified Contact Center Management Portal Replication Publisher / Subscriber services.
2. Delete everything in the **ToReplicate** and **Replicated** folders on both servers.
3. Switch off SQL Replication between the two databases.
4. On the active importer take a snapshot of the SQL Server database and restore it on the failed side. At this point both databases contain identical data.
5. Bring up SQL Server replication between the two databases.

Each table imported by the importer has a tide mark. The tide mark is essentially a bookmark storing the location where everything has been imported up to. Everything after the tide mark has yet to be imported. The importer imports a chunk of available data from each file in turn and updates the tide mark afterwards. The tide marks are stored in a table called **TB_IMP_TIDEMARK** as shown below.

TABLE_NAME	RESOURCE_INSTANCE_ID	TIDEMARK1
t_Call_Type_Half_Hour	BDC53DEC-D06E-4994-BCDD-FA9CF2FE99C2	367220324999
t_Peripheral_Half_Hour	BDC53DEC-D06E-4994-BCDD-FA9CF2FE99C2	367220325013
t_Agent_State_Trace	BDC53DEC-D06E-4994-BCDD-FA9CF2FE99C2	371624343142
t_Route_Half_Hour	BDC53DEC-D06E-4994-BCDD-FA9CF2FE99C2	363235050788
t_Trunk_Group_Half_Hour	BDC53DEC-D06E-4994-BCDD-FA9CF2FE99C2	367220325039
t_Skill_Group_Half_Hour	BDC53DEC-D06E-4994-BCDD-FA9CF2FE99C2	363234054766

On the **failed** server the following changes must be made:

1. The tide marks in **TB_IMP_TIDEMARK** will be incorrect once the database has been restored on the failed side. So delete all rows from the table which contains the failed server's **RESOURCE_INSTANCE_ID**. On the failed server call **ap_clu01_get_exony_db_resource_instance** from SQL Server Query Analyzer to get its **RESOURCE_INSTANCE_ID**.



2. After deleting all the rows for the failed database server - duplicate each remaining row in the **TB_IMP_TIDEMARK** table. Each duplicated row must have its **RESOURCE_INSTANCE_ID** changed to the failed server identifier. By doing this it ensures that both servers have identical tide marks and so match the data in the fact tables and dimensions.

   The following SQL can be used to update **TB_IMP_TIDEMARK:**

```
CREATE TABLE #TEMP (RESOURCE_INSTANCE_ID
UNIQUEIDENTIFIER, CATALOG VARCHAR (50))

INSERT #TEMP
EXECUTE ap_clu01_get_exony_db_resource_instance


DECLARE @v_RESOURCE_INSTANCE_ID UNIQUEIDENTIFIER

SELECT @v_RESOURCE_INSTANCE_ID =
RESOURCE_INSTANCE_ID FROM #TEMP


DELETE FROM TB_IMP_TIDEMARK
WHERE RESOURCE_INSTANCE_ID =
@v_RESOURCE_INSTANCE_ID
```

```
INSERT TB_IMP_TIDEMARK (
   CLUSTER_RESOURCE_ID,
   TABLE_NAME,
   RESOURCE_INSTANCE_ID,
   TIDEMARK1,
   TIDEMARK2,
   TIDEMARK3,
   TIDEMARK4)
SELECT
   CLUSTER_RESOURCE_ID,
   TABLE_NAME,
   @v_RESOURCE_INSTANCE_ID,
   TIDEMARK1,
   TIDEMARK2,
   TIDEMARK3,
   TIDEMARK4,
FROM TB_IMP_TIDEMARK
```

Fact tables are not replicated through SQL Server but via the Unified Contact Center Management Portal Replication system. When importer session files are replicated from one side to another, they are bulk loaded by the Data Import Server into the database. As this process takes place, the Data Import Server logs its progress into a series of state tables in the database.

These importer state tables are replicated using standard SQL Server replication but are uniquely identified on each side via a **RESOURCE_INSTANCE_ID**. The system on each side uses these state tables to track the arrival of new data into the database fact tables for further processing.

TB_IMP_FCT_PARTITION is the base state table. This contains a definition of all the fact table partitions that have been created on each side. There are usually two identical rows in here, differentiated by **RESOURCE_INSTANCE_ID** (one for each side). This table links to **TB_IMP_FCT_PARTITION_TIDEMARK** and **TB_IMP_FCT_PARTITION_TIDEMARK_SLICE**.

Unfortunately, when one database is restored to another side, these state tables are no longer correct. As a result, data may exist in the fact partitions in the restored database that the system has no idea exists. The following steps recover the state tables on the **failed** database. It is very important that SQL Server replication is running while these steps are performed.

1. Delete all data from **TB_IMP_FCT_PARTITION** with the **RESOURCE_INSTANCE_ID** of the failed database. This should cascade delete data from all the other state tables.
2. All the data in the following tables must be duplicated using the failed database **RESOURCE_INSTANCE_ID**. This essentially matches the state tables with the actual data in the database fact tables.
   - **TB_IMP_FCT_PARTITION**
   - **TB_IMP_FCT_PARTITION_TIDEMARK**
   - **TB_IMP_FCT_PARTITION_TIDEMARK_SLICE**

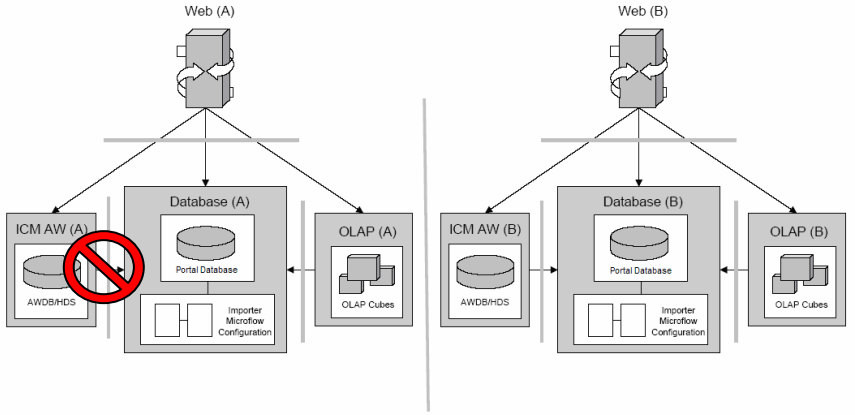
3. **Replication.xml** on the active importer can now be reset and the Data Import component server service along with the Unified Contact Center Management Portal Replication Publisher / Subscriber services can be restarted on both servers. The Data Import component server will start importing and replicating data to the other side as normal.

Recovery after No Disk Space Available

If there is no disk space for the importer it will continue trying and failing to import data until disk space is made available. However the importer should always reset the Unified Contact Center Management Portal database to a consistent state. Sometimes the importer cannot back out changes it has made to the database until disk space is made available (for example, disk space is often required by the SQL Server transaction log before changes are committed).

There are several places where running out of disk space can cause an import to fail. For example when the importer reloads a dimension cache, it saves it to a session file on disk. The same occurs when the importer is processing downloads from the Admin Workstation. It is therefore difficult to specify exactly where the importer will fail when there is no disk space left.

In all cases the importer should generate an exception (visible in the importer trace) and stop the current import. Once disk space is made available the importer should reset the database to a consistent state and start importing again.



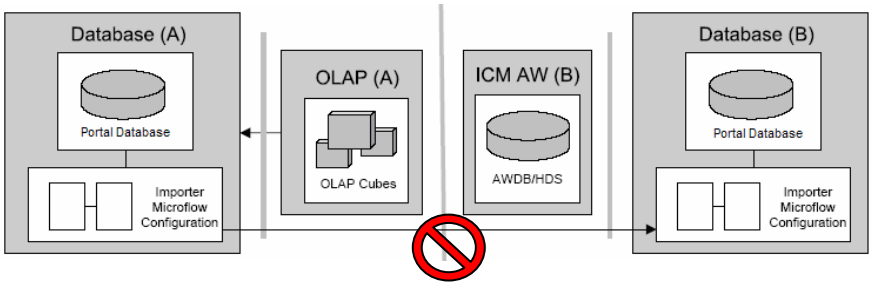
Network Disconnects in Replicated Environments

There are two types of replication connection between the database servers. The first is SQL Server replication which is used to replicate dimension, member and administration tables in the Unified Contact Center Management Portal database. The second connection is used by the Data Import Server to replicate high volume fact data between the systems.

If this connection is broken, both replication connections are expected to stop.

While the connection is down disk space will fill up on the active importer. This is because it is accumulating session files from the running importer which cannot be replicated to the other side. Once the connection is re-established the session files waiting to be replicated will be processed and data should not be lost as a result.

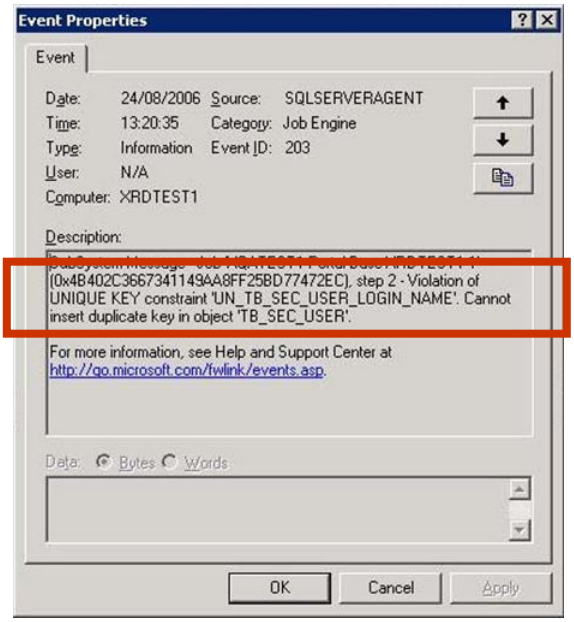
Once the connection is re-established both connections should start working again and catch up where they left off. For SQL Server replication this can be monitored through the Enterprise Manager Replication Monitor. Data Import Server replication can be monitored by opening Windows Explorer on the configured **ToReplicate** folder.



Replication Fails on Replication Restart

It sometimes happens that while replication is down, the same user is created on both the publisher and the subscriber. When replication is brought back up again, the presence of two records containing fields that must be unique (such as the login name) causes replication to fail.

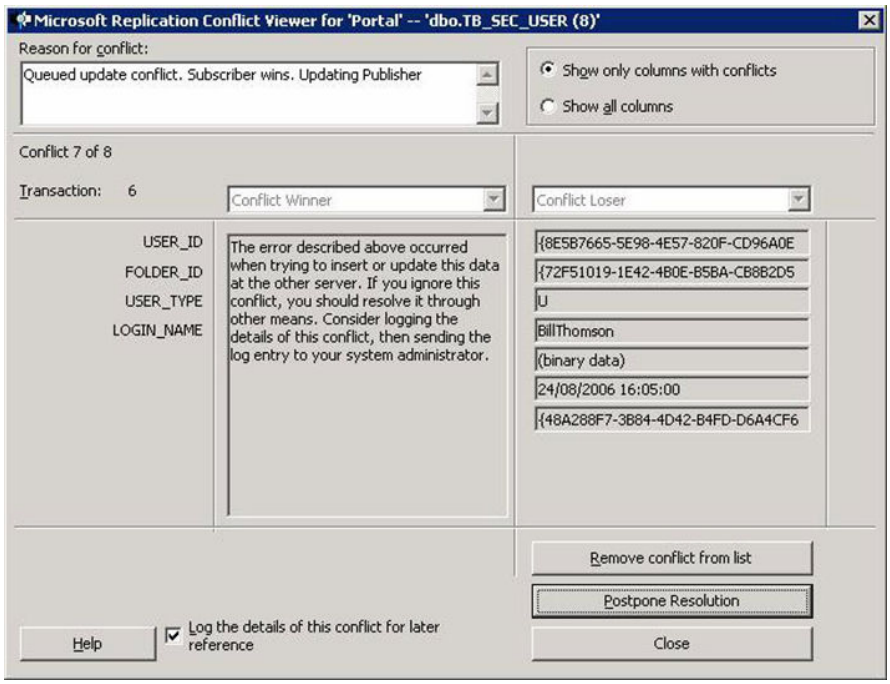
This problem can be confirmed by checking the event viewer for an event with a description that includes the phrase ‘violation of UNIQUE KEY constraint’.



To solve this problem, it is necessary to delete one of the duplicate records.

To find the record causing the problem:

1. Go to the subscriber database and expand the Portal database
2. Navigate to **Replication Monitor > Publishers > *Publisher Database Name*** and click on **Base:Portal** publication
3. In the left-hand window, right-click on the Distribution Agent for Base publication (this will be displayed **as *Subscriber Database Name*:Portal**)
4. Select **Agent History** and the Distribution Agent History window will open. This will give information about the error and the place where the conflict is occurring.
5. To find the record in the table where this error is occurring, right-click on the **Base:Portal** publication (**Replication Monitor > Publishers > *Publisher Database Name***) and click on **View Conflicts**. This will open the Replication Conflict Viewer window
6. Select the table that you suspect the conflict to be in and click **View**



7. Click on **Postpone Resolution** until you reach the place where you suspect the conflict is not resolved. In the above case it is the BillThomson LOGIN_NAME that is creating a conflict

You must then manually check on both sides for the duplicated record and delete one of them from the system. Once this is completed, the system will immediately replicate all records that were pending replication.

Domain Controller was Rebooted

Problems are occasionally seen after rebooting a domain controller. The solution is to reboot the Unified Contact Center Management Portal servers. If domain security policies do not allow cached account credentials then the domain controller must be available when the Management Portal servers restart (otherwise they will not be able to authenticate against the domain).

Taking a Cisco Admin Workstation Offline

No special action needs to be taken in this instance. While an Admin Workstation is offline the Unified Contact Center Management Portal will not be able to import any data from that system. It will however continue to import data from other Admin Workstations as normal.

Because the Admin Workstation is offline no provisioning actions will be completed for the tenant who has been allocated that Admin Workstation. This means that tenant's resources will remain in a synchronizing state forever. Once the Admin Workstation is back online the system automatically starts using it again.

Gateway Monitoring Web Page Shows Errors/Scripts Offline

This is typically because the remote system (ICM/CICM or CallManager) is not currently available. This may be because of a network disconnection or other service fault on the remote system. It is probably worth checking that the ICM or CICM is up and running correctly (in particular the CMS control in Configuration Tools).

Audit Report fails to Upload

Failure of the audit report to upload usually indicates that the Reports and ReportServer virtual directories are running under ASP.NET 2, rather than ASP.NET 1.1. In a dual sided system, the directories on both sides must be set to ASP.NET 1.1.

Information on how to change the version of .NET can be found in the Installation Guide, in the Web Server Component Installation section.

4. MANAGEMENT PORTAL

Resource Stays in Synchronizing State Forever?

This may be because the system has been unusually busy. The first check is in the history tab for the resource. This shows any activity taken by the system for that resource. If the system unsuccessfully attempted to make a change on the ICM/CICM or CallManager then that information is normally recorded in the audit history. If the audit history has not been updated then it may indicate that the Unified Contact Center Management Portal Provisioning Server is offline.

It is possible to manually run the microflows that synchronize the Management Portal with IPCC. To do this, from the Database Server:

1. Navigate to where the Management Portal has been installed (usually C:\Program Files\Management Portal)
2. Open the Data Import Server folder and run MicroExplorer.exe
3. In the Microflow Explorer window, browse to C:\Program Files\Management Portal\Data Import Server\Config\Microflows.xml
4. Select the Provision microflow
5. Click Run. The Microflow Runtime Debugger will open.
6. Click Run again. The Portal will synchronize

Caution: The Microflow Explorer should not be used to edit microflows.

Why is there No Data in My Report?

1. Open the parameter set and then click **Preview**. Check that there are resources listed as the Unified Contact Center Management Portal uses these to generate the report.
2. If the parameter set includes folders, check that these folders exist and that the user has the **Browse Dimensions** security privileges on them.
3. Check the parameters configured when viewing the report. Some reports have date ranges which can either be relative (for example, from last week, to today) or absolute (for example, from 2005-07-25, to 2005-12-31).

"Object reference not set to an instance of an object" When Running a Report

The Unified Contact Center Management Portal uses an internal indexing system to keep track of all resources in the system. This can take several minutes to load after the system starts. If the system has recently started up, wait five minutes and then try again.

Web Browser Displays “No connection could be made because the target machine actively refused it”

Check the Unified Contact Center Management Portal services are all up and running on the web component server.

Web Browser Displays “The page cannot be found”

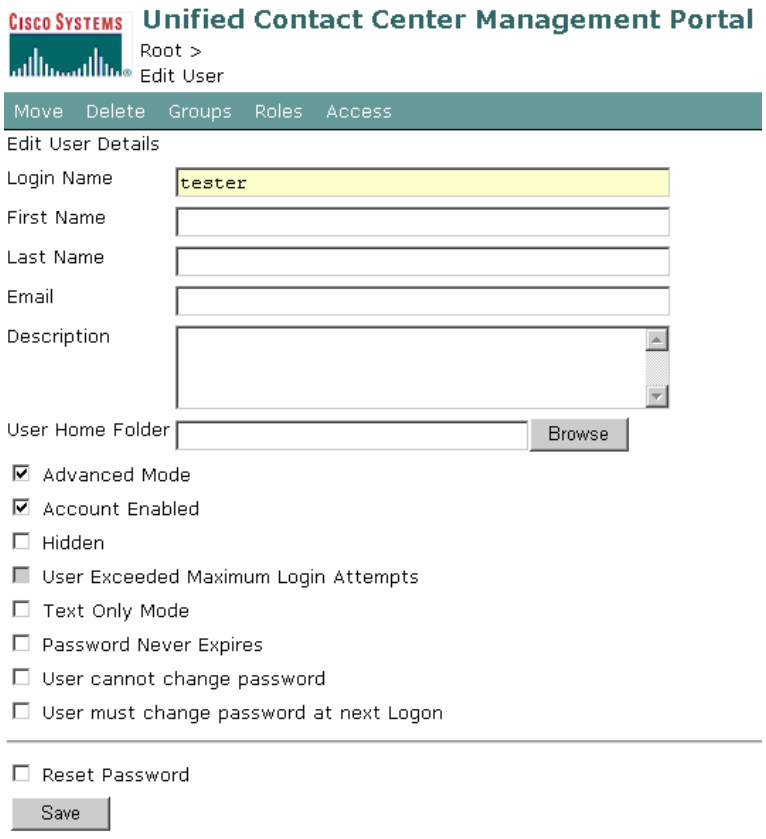
Check the URL in the web browser is correct (in particular the server name / IP address of the Unified Contact Center Management Portal server).

Can’t Print Reports

Printing requires the Microsoft Reporting Services ActiveX control to be downloaded to the client machine. The browser’s security settings might need to be modified to allow an ActiveX control download from the Management Portal web site.

How Do I Reset a User’s Password?

1. Login to the Unified Contact Center Management Portal as an *administrator*.
2. Navigate the **Security Manager** to the user resource.
3. Click the **Reset Password** check box at the bottom.
4. Click **User must change password at next login**.
5. Click **Save** to submit the changes into the system.



Basic User has no Agents or Skillgroups menu options

Check whether the user's home folder is one they have permission to manage resources in.

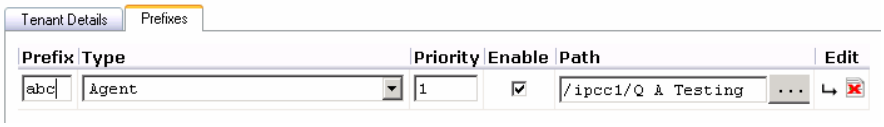
When moving users or changing their permissions it is a common error to neglect to change their home folder. In Basic Mode, a user is automatically set to work in the folder specified as their home folder, and if they do not have permission to manage dimensions in that folder they will not be able to access the **Agents** or **Skillgroups** menu options.

This is not a problem for Advanced Users because whereas Basic Mode presents a flat view, the tools available in Advanced Mode allow the user to change the folder in which they are working.

A Tenant's Resources are not being moved to the Correct Folder after Import

1. Login to the Unified Contact Center Management Portal as a *system administrator*.
2. In the **System Manager** navigate to the folder containing the tenant.
3. Click on the tenant and wait for the right hand pane to load.
4. Click the **Prefixes** table and edit the prefixes as appropriate.

5. Click **Save** to submit the changes into the system.



For Cisco ICM or CICM the prefix management works from the resource's enterprise name. So in the example rule above, if the agent's name begins with **abc** then it will automatically be moved to the folder **/ipcc1/QA Testing**. If more than one prefix rule is applicable then the rule with the lowest priority number is used.

Can't See Resources in System Manager?

This is probably because the user does not have **Browse Dimensions** security privileges. It is best practice to assign security permissions through security groups rather than to individual users. The Unified Contact Center Management Portal User Guide explains how to configure security users / groups and how to assign permissions to them.

Can't Provision Resources through System Manager?

The user probably needs a global provisioning security privilege, for example, Provision Agent. It is best practice to assign security permissions through security groups rather than to individual users. The Unified Contact Center Management Portal User Guide explains how to configure security users / groups and how to assign permissions to them.

When Creating New Item, Error Indicates Resource Already Exists

This indicates that the resource you are trying to create shares a field that must be unique, such as a Person's login name or a Dialed Number's number, with an existing resource.

If no duplicate resource appears to exist, this may indicate that the resource has been deleted. Deleted resources are marked as deleted but kept in the system for audit purposes, and so it is possible for a new resource to have a conflict with an old one. You can see deleted items within the system by checking the **Show Deleted Resources** checkbox in **Settings > User Settings**.

If a conflict exists you will not be able to create the new resource unless you change the conflicting detail.

Creating a Resource but can't see Related Resources in System Manager?

This is probably because the user does not have **Browse Dimensions** security privileges on the folders where the related resource is located. For

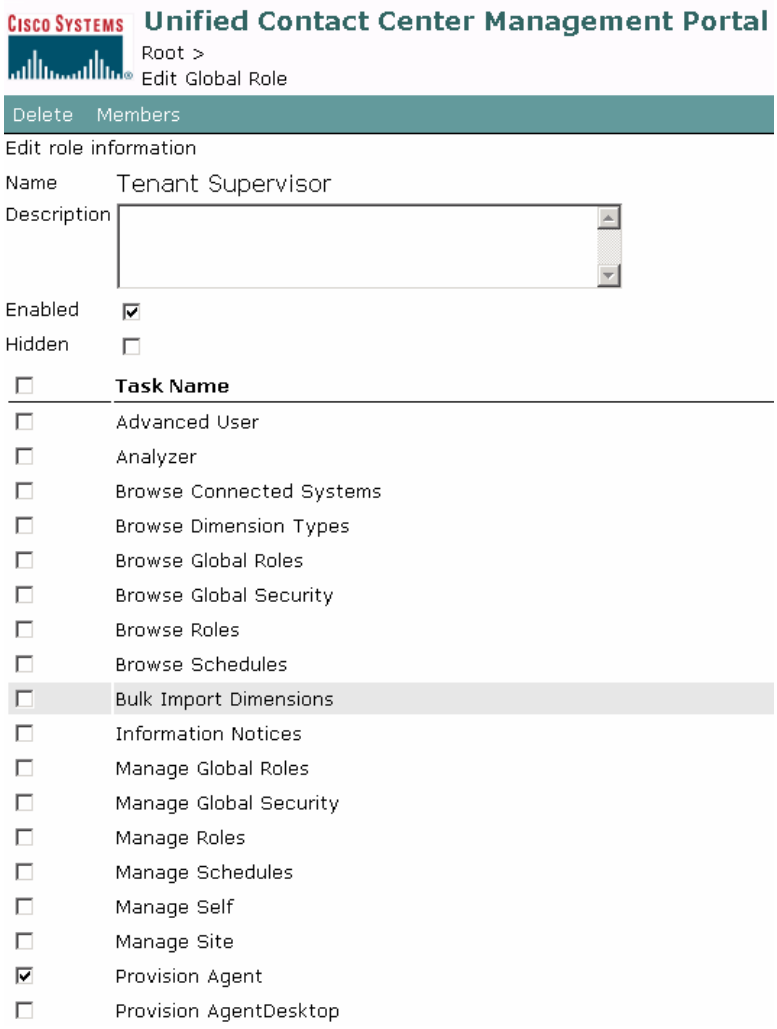
example, to add an agent to a skill group requires Browse Dimensions security privileges on the folder where the skill group is located. It is best practice to assign security permissions through security groups rather than to individual users. The Unified Contact Center Management Portal User Guide explains how to configure security users / groups and how to assign permissions to them.

Can't See Audit Reports in Management Portal?

This is probably because the user does not have **Browse Reports** security privileges to the folder where the audit report is located.

Can't Bulk Load Resources in System Manager?

This is probably because the user does not have the **Bulk Import Dimensions** security privilege. This security privilege is a global task and so is configured in a global role. A user must be granted the global role. The user must also be granted the provisioning global task to bulk upload particular resource types, for example Provision Agents.



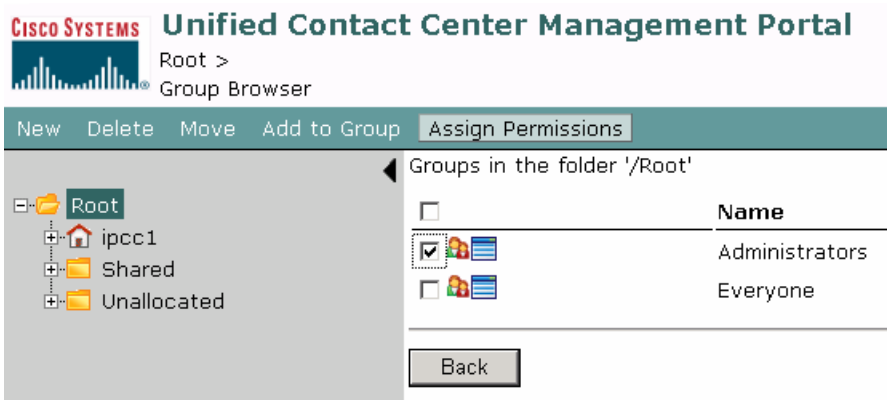
How Do I Assign Users/Groups to a Global Role?

1. Login to the Unified Contact Center Management Portal as a *system administrator*.
2. From the home page click **Security Manager**.
3. Click the **Roles** button on the action toolbar.
4. Click the role which is to be changed.
5. Check the boxes for the security tasks to be assigned to this role.

The changes are made immediately. Click **Home** when finished.

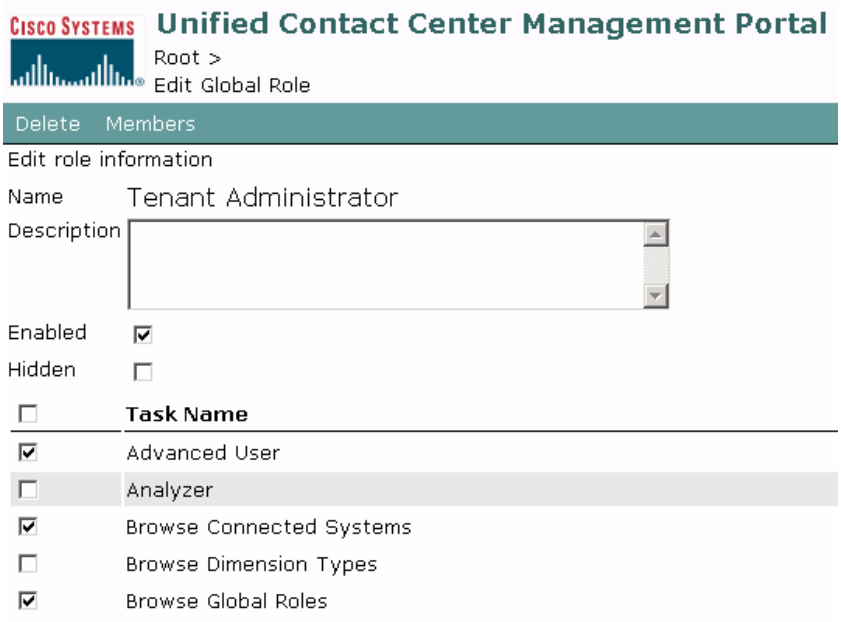
How Do I Assign Users/Groups to a Non-Global Role?

1. Login to the Unified Contact Center Management Portal as a *system administrator*.
2. Navigate in the **Security Manager** to the user/group resource.
3. Check the box next to the resource in the right hand pane.
4. Click the **Assign Permissions** button on the action toolbar.
5. Check the boxes for the security roles to be assigned to this user/group.
6. Click **Save** to submit the changes into the system.



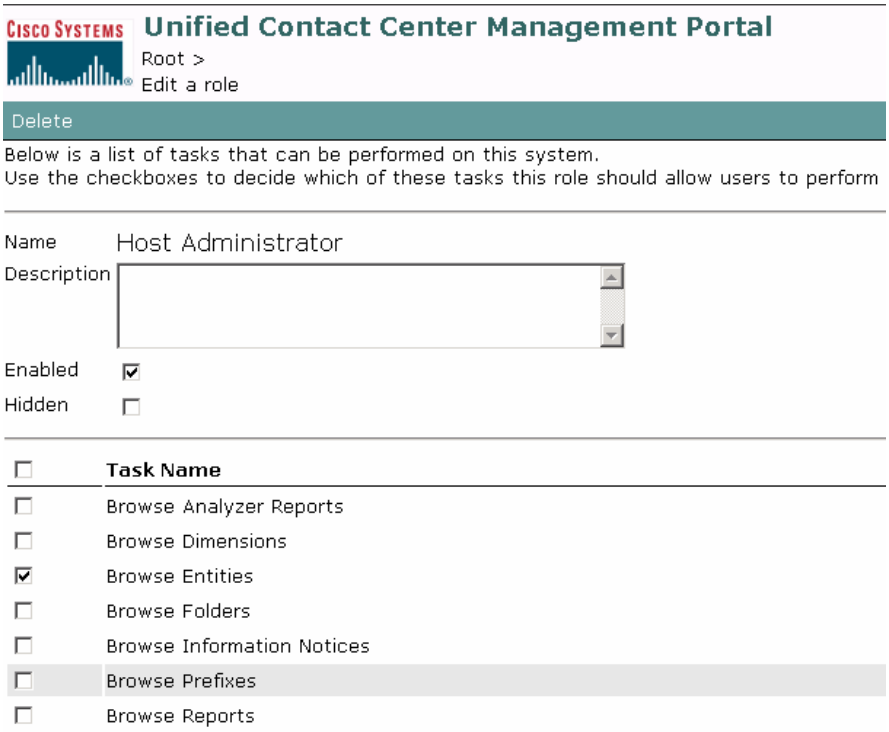
How Do I Edit Global Security Roles?

1. Login to the Unified Contact Center Management Portal as a *system administrator*.
2. Click **Settings** from the menu in the top right corner.
3. Click **Security Settings** from the left hand list.
4. Check the boxes for the security tasks to be assigned to this role.
5. Click **Save** to submit the changes into the system.



How Do I Edit Non-Global Security Roles?

1. Login to the Unified Contact Center Management Portal as a *system administrator*.
2. Click **Settings** from the menu in the top right corner.
3. Click **Security Settings** from the left hand list.
4. Check the boxes for the security tasks to be assigned to this role.
5. Click **Save** to submit the changes into the system.



Sharing IPCC Lines

In IPCC, two types of line exist: CallManager internal lines and ICM/CICM controlled lines. For ICM controlled lines the Unified Contact Center Management Portal automatically configures the necessary device targets and labels on ICM. Note however that an ICM controlled line can only be associated with one phone in the Unified Contact Center Management Portal and cannot be shared. For CallManager internal lines, multiple phones can share the same line.

Supported Phone Types

Only supported phone types are imported into the Unified Contact Center Management Portal, all others are filtered out and will not be visible in the System Manager. If the Data Import component server fails when importing a phone from CallManager it will change the state of the phone to **error**. To resolve this problem, load the phone in the System Manager and click **Save**. The system will then synchronize the phone with CallManager and resolve any problems.

Tenants and Cluster Configuration

Tenants are configured in the Unified Contact Center Management Portal Cluster Configuration tool. It is vital that the CallManager peripheral user name is entered correctly as the Unified Contact Center Management Portal requires this user name to integrate CallManager and ICM/CICM. If this user name is entered incorrectly, logging into the phone will not be

possible. Furthermore ICM will not be able to control the phone properly and so it will not ring.

The solution is to first correct the peripheral user name in the Cluster Configuration tool. Then each phone must be loaded in System Manager and saved. The Unified Contact Center Management Portal will update CallManager / ICM and reconfigure the phone correctly.

Note It is very important that the peripheral user name is not changed after the system is commissioned. The peripheral user name must also be unique across a peripheral.

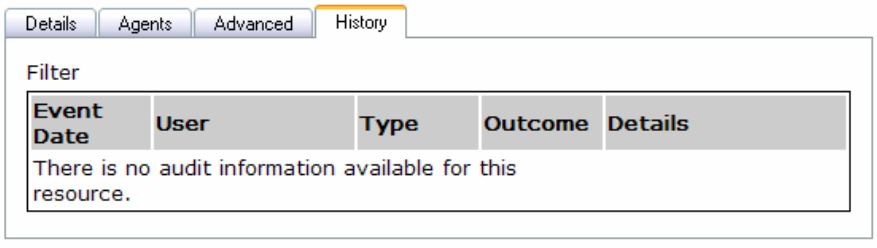
Phone Button Templates

Button templates are imported from the CallManager but cannot be edited or created in the Unified Contact Center Management Portal. The number of lines can be set in a phone template on the CallManager but this is not reflected in the Unified Contact Center Management Portal. This means a phone can be assigned to more lines in the System Manager than the button template actually permits.

Known Application Error Codes

The Unified Contact Center Management Portal does not use status codes to convey information through the system. The following list represents the known error codes displayed to US-English locale users of the system. These error codes are generally very user friendly and so when combined with the context of what a user was doing when they got the error, these should be sufficient to resolve the problem.

The Unified Contact Center Management Portal also displays errors returned by the ICM and CallManager. These are visible through the audit reports provided by Unified Contact Center Management Portal and also in the history tab for a resource item. These ICM and CallManager error messages are always displayed in US-English and are documented on the Cisco web site.



The Unified Contact Center Management Portal error codes also contain some Report Builder and Analysis Services messages which are not relevant to the Unified Contact Center Management Portal.

An Unknown error occurred. Please contact the system administrator, or try again.
Un-able to insert item. Please check and try again.
The update was un-successfull. Please check your details and try again.
The item you tried to delete could not be removed. Please try again later.
The item could not be added as the row count is incorrect.
The update could not complete due to the row count being incorrect.
Deletion failed as the row count is incorrect.
One or more of the items specified is an invalid entry. Please check your entries and try again.
Folders can only be bulk moved from a single parent folder.
Destination folder does not exist.
Folder with specified name already exists in destination folder.
Failed to move folder in reporting services.
Failed to create folder in reporting services.
Record already exists. Cannot insert duplicate object.
The move destination is invalid.
The command failed to execute on all report servers and was not successfully rolled back.
Unable to create instance of ADOMD Cellset object.
Unable to set connection property of ADOMD Catalog object.
Unable to set source property of ADOMD Cellset object.
Unable to get pointer to connection property of ADOMD Catalog object.
Unable to set connection property of ADOMD Cellset object.
Unable to execute MDX query against ADOMD Cellset object.
Unable to determine number of dimension members on columns axis of ADOMD Cellset object.
Unable to determine number of dimension members on rows axis of ADOMD Cellset object.
Unable to determine number of result columns on columns axis of ADOMD Cellset object.
Unable to determine number of result rows on rows axis of ADOMD Cellset object.
Unable to retrieve cell value from ADOMD Cellset object.
Unable to create temporary table for MDX query results.
Unable to execute INSERT statement for MDX query results.

Unable to destroy instance of ADOMD Catalog object.
Unable to destroy instance of ADOMD Cellset object.
Unable to determine Analysis Services server / database to use for query.
Temporary table with that name already exists.
Unable to create instance of ADOMD Catalog object.
The specified subscription could not be found.
The template XML for this template is corrupt. Please select another.
The user or group name is already in use. Please use another name and try again.
There was an error setting your password. Please contact an administrator quoting the error code (%d).
Your security settings have become corrupt. Please contact an administrator quoting the error code (%d).
Invalid location.
User or Group does not exist.
Users and groups cannot be members of themselves.
Invalid Operation.
Invalid User or Group. Please select another.
Access has been denied.
Password changes have been denied for this account.
The password entered does not meet the systems complexity requirements. Please enter a more complex password or contact your system administrator for assistance.
The system licence count has been exceeded. Please contact your system administrator.
Recursive group membership is not allowed.
The user account has been locked, please contact the system administrator.
The password has expired, please change it to continue.
The Role name you are trying to add already exists. Please try a different name.
The Policy name you are trying to add already exists. Please try a different name.
The Security Item does not have a root policy.
Invalid date was entered.
The 'From' date is greater than 'To' date.
The item you are trying to delete cannot be deleted as it is a system object.

The item you are trying to modify cannot be saved as it is a system object.
The item type is unknown.
Prefixes can only be added to tenants.
Invalid object type.
The Parameter Set could not be found.
The Report could not be found.
Un-able to create schedule. An error has occurred.
An error occurred creating schedule.
Deleted objects can not be modified.
Report stylesheet not found.
Un-able to find page layout.
Folder not found.
This Group can not be modified as it is Read Only.
A group can not be added to itself.
User or group already member of group.
Role assignments prohibited.
You cannot force a user to change their password that does not have permission to do so.
User account locked.
User authentication failed.
Password change disabled.
Your password does not meet the required complexity. Please enter a new password and try again.
You can not delete a role that is still used.
Folder already has root policy defined.
Folder is not a policy root.
Cannot revert to parent security on tenant.
Cannot revert to parent security on system folder.
Folder has no parent.
Cannot delete self.
User can not be deleted with active schedules.
A sub folder with the same name already exists in this folder.
A report with the same name already exists in this folder.
A parameter set with the same name already exists in this folder.
A user or a group with the same name already exists in this folder.
Login failed, please check your credentials and try again.

Access denied.
The collection is empty.
Items cannot be moved outside their tenant.
The role you are trying to delete is not of a valid type.
You cannot remove this user from this group.
Home folder already exists.
Invalid role name.
Invalid task name.
Invalid role id.
Tenants can only be created in the root folder.
The member type is unknown.
Unable to create report in reporting services.
Unable to create schedule in reporting services.
Unable to create subscription in reporting services.
Unable to delete report from reporting services.
Unable to delete schedule from reporting services.
Unable to delete subscription from reporting services.
Unable to edit report in reporting services.
Unable to retrieve schedule extension settings from reporting services.
Unable to retrieve report datasources from reporting services.
Unable to retrieve report information from reporting services.
Unable to retrieve report parameters from reporting services.
Unable to retrieve subscription properties from reporting services.
Unable to retrieve subscription from reporting services.
Unable to list schedule extensions in reporting services.
Unable to list report history in reporting services.
Unable to list schedules in reporting services.
Unable to list subscriptions in reporting services.
Unable to move folder in reporting services.
Unable to create folder in reporting services.
Unable to move report in reporting services.
Unable to update subscription properties in reporting services.
Unable to update the report in reporting services.
Unable to upload the report in reporting services.
Failed to login to reporting services.

The dimension type is invalid.
Use Default.
Ignore Abandoned Calls.
Abandoned Call has a Negative Impact.
Abandoned Call has a Positive Impact.
Agent has more than one personality.
No peripheral configured.
No routing client configured.
The IP phone has more than one line association.
The remote equipment cannot be found.
The number of teams to which the agent can belong has been exceeded.
The number of agents supported by a single peripheral has been exceeded.
Voice Skill Groups must let system pick the agent.

5. INDEX

R

S

T

U

W