Administration Manual for Cisco Unified Contact Center Management Portal

Release 7.1(3)

December 2006

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

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, “Unified Contact Center Management Portal Overview”

Provides information on the components that make up the Unified Contact Center Management Portal and the configuration that needs to be done for each.

Chapter 2, “Web Server”

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, such as importing data from an ICM into a tenant folder.

Chapter 3, “System Provisioning”

Introduces system security and system management and explains where to find further information.

Chapter 4, “Provisioning Component Monitoring”

Explains how to use the Provisioning component monitoring web site for the Unified Contact Center Management Portal Provisioning component. This allows support agents to monitor busy times, capacity statistics, event logs and so on, and provides access to audit reporting for the Unified Contact Center Management Portal.

Chapter 5, “SNMP Configuration”

Explains how to set up SNMP traps for the Unified Contact Center Management Portal Provisioning component, and describes the traps that it raises.

Chapter 6, “Audit Trails”

Describes the audit histories of individual items and the audit report used to measure actions taken upon entities in the Unified Contact Center Management Portal.

Chapter 7, “Bulk Upload”

This chapter details the process required to bulk upload dimension data into the Unified Contact Center Management Portal, the

templates used to do so and details on how to understand any upload failure.

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 UNIFIED CONTACT CENTER MANAGEMENT PORTAL OVERVIEW

Operational Overview

The Unified Contact Center Management Portal 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 IPCC Hosted and Enterprise Editions product set.

The Unified Contact Center Management Portal consists of six components:

- The **Database** server component, which utilizes an application called the **Importer** to import enterprise data from different data sources into a Microsoft SQL Server 2000 Enterprise Edition management information database. The database consists of separate database elements that sit on top of SQL Server and which provide data to different reporting elements:
    - The **RDBMS Database** (known as the *Datamart*) holds the imported enterprise data
    - The **Reporting Services Database** imports and processes data from the datamart so that SQL Server Reporting Services can use it to populate reports
- The **Reporting Extensions** server component holds the report templates used to run audit reports and retrieves the data from the reporting services database to populate reports with
- The **Application** server component manages security and failover. It manages security by ensuring that users can only view specific folders and folder content as defined by their security login credentials. It 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 via an alternative database server
- The **Web** server component provides a user interface to the platform that allows users to interact with report data, as well as performing administrative functions
- The **Provisioning** server component and its various connectors enable it to communicate with network equipment to assist in the making of intelligent call routing decisions. It communicates with back office databases and systems to extract information for routing and reporting purposes

- The **Data Import** server component is an Extract, Transform and Load (ETL) server for data warehouses. The Data Import component imports the data used to build reports. It is designed to handle high volume data (*facts*) such as call detail records as well as data that is rarely changed (*dimensions*) such as agents, peripherals and skill groups

If these components are installed on more than one machine, the Data Import, Database and Provisioning components are normally installed on the Database Server. The Reporting Extensions, Application and Web components are usually installed on the Web Application Server.

2 WEB SERVER

The Unified Contact Center Management Portal 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, and a tenant folder in which to put all the tenant's resources.

Further information on the web server is available from the *User Manaul for Unified Contact Center Management Portal Release 7.1(3)*.

Import a Tenant from the ICM

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

How does it work?

The Unified Contact Center Management Portal maintains a complete data model of the contact center equipment to which it is connected and periodically synchronized. In addition to configuration information, for example agents or skill-groups, the Unified Contact Center Management Portal can optionally record the events logged by the equipment, such as call records for management information and reporting purposes. The Unified Contact Center Management Portal data model and synchronization activity allows for items to be provisioned either through the Unified Contact Center Management Portal's Web interface or from the standard equipment specific user interfaces.

Portal Users

In regards to the Web component server there are typically a small number of different user types:

- The **host administrator** is responsible for the whole platform and therefore has a view across all the equipment and resources
- The **tenant administrator** is responsible for the slice of the system assigned to the tenant by the host administrator
- The **tenant user** has access only to the resources and tools assigned by the tenant administrator. Several sub-classes of tenant user may be created by the tenant administrator using user groups and roles to achieve their business requirements, for example one type of user may 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
- Ensuring that the tenant equipment (peripherals) are 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

Note To map a prefix to a tenant for the importing of ICM data, the user must have **host administrator** privileges.

Configuring Imported Resource Data

After the initial data import, resources imported from CallManagers associated with specific tenants will be stored in those tenant folders. Where multiple tenants share a CallManager, resources will be put in the Unallocated folder and the administrator must place these in the appropriate folder. Resources associated with more than one tenant, such as phone types and button templates, should be placed in a subfolder of the Shared folder that should be set to be readable only by users from those tenants. More information on how to manage security in the Management Portal can be found in the *User Manual for Cisco Unified Contact Center Management Portal Release 7.1(3)*.

Caution: Resources may **not** be moved out of tenant folders

Prefixes can be used to search through items in the Unallocated folder and identify the specific items to be moved into a selected tenant folder.

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. Click **Tools**. The **Tools** page is displayed
2. Click **System Manager**. The **System Manager** page is displayed
3. From the **Filter** drop down list select **Tenant**. The page refreshes and the tenant folders in the system are displayed as a list
4. Click the properties icon displayed next to the prefix name. To the right of the screen the **Update the details for the selected tenant folder** section is displayed
5. Click the **View Prefixes...** link. The prefixes associated with the selected tenant are displayed as a list

To **create** a prefix (add a prefix to a system folder), click the **Create Prefix** button. The **Create a Prefix** page is displayed. Perform the following:

1. In the **Prefix** field enter the prefix
2. From the **Type** drop down list, select the system resource type to which the prefix is to be applied
3. In the **Priority** field enter a unique numerical value (0 - 9999)
4. Click **OK**

To **edit** a prefix, click the properties icon displayed next to the prefix name. To the right of the screen the **Update the details for the selected tenant** section is displayed.

1. You may only modify the name entered in the **Prefix** field
2. Click **OK**

Note Once a prefix has been created, its type cannot be changed.

To **assign** a priority to a prefix, use the up or down buttons displayed next to the prefix name. The higher the prefix is in the list, the more relevant and useful it is to your data.

To **delete** a prefix, select the tenant folder in the tree whose associated prefixes you wish to view. The prefixes associated with the selected folder are listed.

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

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 **Security Manager**, and the **Security Manager** page is displayed
3. Click on the **Users** tab to the top left to access the **User Browser** page.
4. Select the tenant folder and click **New**
5. Fill in the following fields:
   - In the **User Name** field enter the name as it will appear in the system for the new user
   - In the **Password** field enter the password for the new user
   - In the **Confirm Password** field re-enter the selected password
   - In the **First Name** and **Last Name** fields enter the user's details
   - In the **Email** field enter the email address of the new user
   - In the **Description** field enter any explanatory text, if required
6. Select the **Advanced Mode** checkbox and any of the following checkboxes if applicable:
   - The **Enabled** checkbox to ensure that the user is live in the system. If unchecked the new user is saved in the system but cannot access it

- The **User must change password at next Logon** checkbox to prompt the new user to change their password after their first login
- The **Password Never Expires** checkbox to assign the password to the new user indefinitely
- The **User cannot change password** checkbox to prevent the new user from being able to change their password

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

7. Click **OK**. You are returned to the **User Browser** page

Assigning Administrator Privileges

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

1. Click on the properties icon for the administrator user to display the **Edit User** page
2. Click on the **Groups** tab to show the available groups

Note All users created are automatically assigned to the group <tenant> Users.

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

3 SYSTEM PROVISIONING

All system and security management for the Management Portal is performed through the web interface. For further information on how to use the web interface, please see the accompanying *User Manual for Unified Contact Center Management Portal Release 7.1(3)*. 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 the Management Portal is folder based. This means that the folder hierarchy should ideally be designed with security requirements in mind
- **Users and Groups** Users can be assigned to groups of users with the same security permissions. A number of predefined groups with commonly required permissions are provided. For example, all users within a tenant are automatically assigned to a tenant users group that gives them read-only permissions on resources within that tenant
- **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 included 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 rather than removing permissions from folders individually.

Security is explained in more detail in the Security Management chapter of the User Manual.

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 via the System Manager interface. This lets you remotely configure and administer key aspects of your IPCC system.

4 PROVISIONING COMPONENT MONITORING

Note In some circumstances the Provisioning server component is referred to as the *Gateway*.

The Provisioning server component has monitoring tools to track real time and historical customer activity. One such tool is the Web monitoring site. It is the most popular method for tracking customer activity as it can be easily accessed from the support Agents' desktop.

To access the Web monitoring site, open Internet Explorer on the machine that is hosting the Provisioning component and enter the following address: **http://localhost/monitor**.

Once the web site is displayed, a user can start or stop a web monitoring script activity on a given processor, by clicking the **Start** or **Stop** hyperlinks in the **Action** column.

Customer information is displayed in the following columns:

COLUMN	DESCRIPTION
Processor	Displays the computers configured to be monitored.
State	The color displayed indicates whether the script being monitored is Active (green), going online or being taken offline (amber) or Inactive (red).
Transactions	Total number of requests for this script.
Errors	Total number of errors for this script.
Filtered	Number of errors filtered out of the script.
Outstanding	Number of requests being processed at that time.
Restart	The total amount of time required to restart the system.
Oneshot	Displays whether the oneshot function is enabled or not.
Enabled Period	The total time since the script has been active.

Note The web page automatically refreshes every few seconds.

Performance Counters

The Unified Contact Center Management Provisioning component integrates with Windows performance counters (accessed by running the *perfmon* command) to provide real time activity monitoring. Perfmon can also connect to remote computers, if necessary.

The Unified Contact Center Management Provisioning component appears as a separate *Data Gateway* object in perfmon. The performance counters available for the Data Gateway object are:

COUNTER	MONITORS
Call Error Rate	Number of errors (excluding timeouts) per second.
Call Reject Rate	Requests rejected per second (a request is rejected when there is no script available to process it).
Call Request Rate	Requests processed per second (a request is counted as processed once its reply is sent).
Call Timeout Rate	Requests timed out because no response was received by the customer data system.
Outstanding Calls	The number of requests currently being processed (in progress) by the Provisioning component.
Total Call Errors	Total number of errors accumulated since the Provisioning component service started.
Total Call Requests	Total number of requests processed since the Provisioning component service started.
Total Call Timeouts	Total number of requests timed out since the Provisioning component service started.
Total Calls Rejected	Total number of requests rejected since the Provisioning component service started.
Total Processor Starts	Total number of customer scripts that have been started since the Provisioning component service started.
Total Processor Stops	Total number of customer scripts that have been stopped since the Provisioning component service started.

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.

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

Event Log Alarms

The alarm generator monitors activity in the Provisioning component and writes entries to the event log. The events include provisioning scripts starting and stopping and requests failing. Rather than writing an entry every time a request fails, the Provisioning component plugin summarizes every minute. The default reporting period is one minute; however it can be changed in the *minute* attribute in **plugins.xml**.

An application called **evntwin.exe,** which ships as part of Windows, is used to convert the alarms into SNMP traps; see chapter 5.

5 SNMP CONFIGURATION

The Unified Contact Center Management Portal Provisioning component can be configured to produce Simple Network Management Protocol (SNMP) traps. SNMP trapping is a means of monitoring and logging events on the network, such as faults or errors that impact upon the Unified Contact Center Management Portal Provisioning component. SNMP trap configuration is a three stage process.

Stage 1 - Configure the Provisioning component alarm generator

The alarm generator monitors activity in the Unified Contact Center Management Portal Provisioning component and writes events to the event log, including scripts starting, scripts stopping and requests failing.

Stage 2 - Add alarms to the Windows event log

To view an example of an alarm:

1. Click **Start** > **Administrative Tools > Event Viewer**. The **Event Viewer** dialog window is displayed
2. Double click on an alarm in the right-hand pane
3. The **Event Properties** dialog window is displayed in which the alarm properties are detailed

To add alarms to the Windows event log:

1. Navigate to the Windows folder /**evntwin.exe** application and run it. This enables events in the Event Log to be translated out as SNMP traps.

Note If **evntwin.exe** cannot be found, you may not have the **Simple Network Management Protocol** Windows component installed. Click **Start > Add or Remove Programs > Add/Remove Windows Components** and look at the details for Management and Monitoring Tools to see if this component is installed. If it is not, check the box to install it and click **OK**

2. The events are displayed down the right hand side. Select the required events and add them to the top panel list.
3. If you need to configure trap throttling, click **Settings** on the main window. In the **Settings** dialog window, select the **Apply Throttle** radio button in the **Trap Throttle** panel.
4. Click **OK**.

Stage 3 - Setup the Windows SNMP service

1. Click **Start > Control Panel** > **Administrative Tools** and then **Services**. The **Services** dialog window is displayed.
2. Right click **SNMP Service** and select **Properties** from the drop down list. The **SNMP Service Properties** dialog window is displayed. This allows the trap destination and SNMP community to be configured.
3. In the **Community Name** field, enter the name of the community.

4. Click **Add**. A pop up dialog window is displayed. Enter the IP address of the Trap destination.
5. Click **OK**.

Provisioning Component Alarms Reference

The following sections describe the SNMP traps raised by the Unified Contact Center Management Portal Provisioning component.

Provisioning Component Alarm Service has Started

Meaning

This message simply indicates that from this point onwards the Provisioning component will log events to the application log.

Occurrence

Either the provisioning component service has just been started or the alarms plugin has just been added. The alarms plugin is the subsystem in the Provisioning component service that is responsible for raising alarms and it can be loaded dynamically. This event is rare because the provisioning component service is not regularly restarted and there is no reason to reload the alarm service.

Provisioning Component Alarm Service has Stopped

Meaning

This message simply indicates that from this point onwards the Provisioning component will no longer log events to the application log.

Occurrence

Either the Provisioning component service has just been stopped or the alarms plugin has just been unloaded. The alarms plugin is the subsystem in the Provisioning component service which is responsible for raising alarms and it can be loaded dynamically. This event is rare because the Provisioning component service is not regularly restarted and there is no reason to reload the alarm service.

Provisioning Component Customer Script is Online

Provisioning Component customer script %1 is online.

Meaning

%1 is replaced by the script name. This event indicates that the specified script has just been brought online.

Occurrence

This alarm is raised when a customer configuration script is added or a script is restarted after being taken offline for any reason.

Comment

This is an important alarm to monitor because in most situations it indicates either a recovery from an earlier problem or an attempted recovery. For example, if connectivity is lost to a customer system, then a script may be configured to stop so that a failover script can be used. After a specified period of time, the script is restarted in order to reconnect to the customer system.

Use

The actual script affected is referenced within the event text. Therefore, to use this alarm effectively, the actual text must be scanned in order to discover the script name.

Provisioning Component Customer Script is Offline

Provisioning Component customer script %1 is offline.

Meaning

%1 is replaced by the script name. This event indicates that the specified script has just been taken offline.

Occurrence

This alarm is raised when a script is removed or a script is stopped for any reason.

Comment

This is an important alarm to monitor because in most situations it indicates a problem processing transactions. For example, if connectivity is lost to a customer system, then a script may be configured to stop so that a failover script can be used. After a specified period of time, the script is restarted in order to attempt to reconnect to the system.

Use

The actual script affected is referenced within the event text. Therefore, to use this alarm effectively, the actual text must be scanned in order to discover the script name.

Provisioning Component Failed Transactions

Provisioning Component failed %1 transactions for %2 in the last %3 minute(s).

Meaning

%1 is the number of failed transactions; %2 is the name of the script that relates to the failed transactions; %3 is the period of time over which the failures occurred. It indicates that the specified script is having problems processing transactions.

Occurrence

The specified script has failed a number of transactions for some reason.

Comment

This alarm is likely to be raised shortly before the script is taken offline. The tolerance of a script to errors determines the number of these messages to be received before a script is taken offline.

Use

The actual script affected and number of errors is referenced within the event text. Therefore, to use this alarm effectively, the actual text must be scanned in order to discover this information.

Provisioning Component Timed Out Transactions

Provisioning Component timed out %1 transactions for %2 in the last %3 minute(s).

Meaning

%1 is the number of timed-out transactions; %2 is the name of the script with the timed-out transactions; %3 is the period of time over which the timeouts occurred. It indicates that the specified script is not receiving responses in a reasonable period of time.

Occurrence

The specified script has not received replies from the connected system in a reasonable period of time (defined in the script). It will occur in any situation when no response is received from the customer data system in a timely manner, or an incorrectly formatted reply is received.

Comment

This alarm is likely to be raised shortly before the script is taken offline. The tolerance of a script to errors determines the number of these messages before a script is taken offline.

Use

The actual script affected and number of errors is referenced within the event text. Therefore, to use this alarm effectively, the actual text must be scanned in order to discover this information.

Provisioning Component Rejected Transactions

Provisioning Component rejected %1 transactions for %2 in the last %3 minute(s).

Meaning

%1 is the number of timed-out transactions; %2 is the name of the script with the timed-out transactions; %3 is the period of time over which the timeouts occurred. It indicates that there was not a script available to process the transaction when it arrived at the Provisioning component.

Occurrence

A transaction was received for a non-existent script (unlikely). A transaction was received and the associated script and failover scripts were all offline.

Comment

This alarm is only likely to be raised during periods where the customer system is completely unavailable to the Provisioning Component. That is to say, both normal and failover scripts have failed and been taken offline and have not yet restarted.

Use

Information regarding the actual script affected and so forth is referenced within the event text. Therefore, to use this alarm effectively, the actual text must be scanned in order to discover this information.

Trap Guidelines

The most important alarms are those that check the state of scripts stopping and starting. Different customer systems have different levels of reliability and therefore, the associated scripts are given different levels of error tolerance. Where errors are rare, the tolerance is low or non-existent and the script is stopped as soon as an error is detected.

In this case it is important to detect the script offline event. In the case where the backend system is prone to errors/timeouts then the error tolerance is quite high. It is not that important to pick up the timeout/error events as these are expected, so it is only when the script is offline that truly requires monitoring.

MESSAGE	IMPORTANCE
Provisioning Component alarm service has started	Low - Rarely occurs. Does not indicate a problem.
Provisioning Component alarm service has stopped	Low -See above.
Provisioning Component customer script %1 is online	High - Indicates that the Provisioning Component is trying to recover from a problem.
Provisioning Component customer script %1 is offline	High - indicates that the Provisioning Component has taken action due to too many transaction errors.
Provisioning Component failed %1 transactions for %2 in the last %3 minute(s)	Medium - useful for checking situation before script restarts, if more information is later required.

Provisioning Component timed out %1 transactions for %2 in the last %3 minute(s)	Medium - see above.
Provisioning Component rejected %1 transactions for %2 in the last %3 minute(s)	Medium - see above.

6 AUDIT TRAILS

The Unified Contact Center Management Portal enables provisioning users to view the audit histories of individual items. Users with sufficient privileges can run an audit report on the Unified Contact Center Management Portal 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.

Audit Data Report

Audit reports are viewed from the Reporting tool.

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 is displayed. For example, a report parameter that is a single tenant will produce a report that displays only data associated with that tenant. Parameter sets should 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. Click the **Parameter Sets** option. The Parameter Sets page will be displayed
3. Select a folder. All the parameter sets for the selected folder will be displayed
4. Click on **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**

Vewing an Audit Report

More information on viewing reports is available in the User Manual.

The **Audit Data** report contains the following columns:

Column 1 displays the following:

Tenant – the customer that platform operations relate to.

Item Type Name – the type of entity in the system that an action was performed on, such as *Agent* or *Skill Group*.

Date – the date and time when the action was performed.

Column 2 displays the following:

Audit Name – There is currently only one audit report and therefore the description of the audit defaults to *generic*.

Column 3 displays the following:

Audit User – The user who made the listed change. System indicates changes made by the Management Portal.

Column 4 displays the following:

Resource Name – This identifies the database on which the actioned entity resides.

Column 5 displays the following:

Item Name – This identifies the name of the actioned entity, for example, an agent *name* or *identification number*.

Column 6 displays the following:

Description – This describes the action that was taken, for example, *moved* or *deleted*.

Column 7 displays the following:

Event Outcome – This describes whether the action was a success or a Failure.

There are a number of totals displayed for the report. Beneath each **Item Type** group a row is displayed that states **Item Type Success %:** and the percentage of actions on that **Item Type** that were successful are displayed beneath the **Event Outcome** column.

At the bottom of the report table two further total types are displayed:

The **Tenant Success %:** total displays a percentage of actions taken on entities belonging to a tenant that were successful. The result is displayed as a percentage beneath the **Event Outcome** column.

The **Report Success %:** total displays a percentage of actions taken on entities belonging to all tenants that were successful. The result is displayed as a percentage beneath the **Event Outcome** column.

7 Bulk Upload

The bulk upload tool is used to import hundreds of resource items into the Unifed Contact Center Management Portal Platform. 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 which dictate where each value goes. To facilitate this the Unifed Contact Center Managemret Portal uses templates. Templates are a CSV file with all the headers set up. 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 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 whilst maintaining the integrity of the CSV format.

NoteThere are a few known issues with Excel and the CSV format. If you find 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 Guide

This section runs through every Template and describes the columns included in the Template.

For further information about the Data Type column in the tables below see the **Data Types** on page 37.

Global Template Columns

These columns are common to every template file.

The **Required?** column in the tables below tells you if you can remove the column should you not wish to set a value. An asterisk indicates that this column cannot support a field that is empty.

The **Description** column tells you if you may leave the field blank. Anything with **No** in this column must appear in every CSV file otherwise the upload will fail.

COLUMN NAME	DATA-TYPE	REQUIRED?	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. **Note** 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 completely 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 won't ever be provisioned.
Description	-	Yes	Describes the dimension being created. This never gets provisioned.
Enterprise Name	SNC	Yes*	The name for the dimension being created. This does get provisioned and **cannot** be omitted. If you leave it blank an Enterprise name is generated for you.
Effective From	Date	No*	The date from which the dimension is active from, default is today.
Effective To	Date	No*	The date from which the dimension is inactive default is today.

Agent Template

COLUMN NAME	DATA-TYPE	REQUIRED?	DESCRIPTION
Peripheral Member	Enterprise Name	Yes*	The Peripheral to assign this Agent to.
Desk Setting Member	Enterprise Name	No*	The Desktop this Agent will use.
Agent Team Member	Enterprise Name	No*	The team this agent belongs to. The team must be on the same Peripheral otherwise provisioning will fail. This column may also 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.
Portal Login	-	No	This column is a placeholder for a future feature and cannot be used yet. It is recommended that you remove it before uploading.
First Name	SNC	Yes*	The first name of the agent.
Last Name	SNC	Yes*	The last name of the agent.
Login Name	SNC	Yes*	The peripheral login name for the agent.
Pass Phrase	Password	Yes	The peripheral login password for the agent.
Supervisor	Boolean	No	Indicates whether the agent is a supervisor. This won't create a Portal user, as this is a future feature, however it enables you to bind this agent to a domain login name.
Peripheral Number	Numeric	Yes*	The service number as known at the peripheral, note that you cannot leave this field empty.
Agent State Trace	Y/N	No	Indicates whether the software collects agent state trace data for the agent.

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. So for the *Login-name*: DOMAIN\USERNAME, the Username is simply USERNAME.

Folders Template

COLUMN NAME	DATA-TYPE	REQUIRED?	DESCRIPTION
Security	CSS Styled List	No	Allows you to set security on the folder you upload. To see an example, see **Incorrect Data type Example** on page 37.

Agent Desktop Template

COLUMN NAME	DATA-TYPE	REQUIRED?	DESCRIPTION
Wrap up Data 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
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

Remote Agent Type	Numeric	Yes *	Even though this field is mandatory, it is not actually used until version 7.2 of ICM, see the ICM documentation for more details.

Agent Team Template

COLUMN NAME	DATA-TYPE	REQUIRED?	DESCRIPTION
Peripheral Member	Enterprise Name	Yes *	Same as Agent Peripheral Member.
Dialed Number Member	Enterprise Name	No	The dialed number to use for this Agent team.

Enterprise Skill Group Template

This does not contain any dimension specific columns.

Skill Group Template

COLUMN NAME	DATA-TYPE	REQUIRED?	DESCRIPTION
Peripheral Member	Enterprise Name	Yes *	Same as Agent Peripheral Member.
Peripheral Number	Numeric	Yes *	Same as Agent Peripheral Number.
Peripheral Name	SNC	No *	The name of the Peripheral as it is known on the site.
Available Hold-Off Delay	Numeric	No	The value for this Skill Group instead of using the one associated with this peripheral.
IPTA	Y/N	No	Indicates whether the ICM picks the agent.
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.

Service Level Type	Numeric	No	For Non-IPCC Enterprise, indicates how the ICM software calculates the service level for the service. See the ICM documentation to determine value meanings. Valid Values are 0, 1, 2 or 3.
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.
Extension	Numeric	Yes *	The extension number for the service (used by Lucent DEFINITY ECS).

User Variable Template

This does not contain any dimension specific columns.

Using the Bulk Upload Tool

To use the bulk upload tool, perform the following: Open the **System Management** page, select the required tenant, click on **Upload** and then select the item types you want to bulk upload from the drop down list. The **Bulk Upload Control** page is displayed.

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.

Firstly 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 is presented allowing you to save this CSV file onto your machine.

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

Return to the **Bulk Upload Control** page and make sure the path is set correctly. Browse to the CSV file you have just entered the data into. 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 something goes wrong, pause the upload and check why an item failed. For further information about how an upload can fail, please see the **Reasons for Upload Failure** on page 38.

If the upload tool encounters a problem that affects all rows and not just the current one, an alert box appears that describes the problem's description and will return you back to the **Bulk Upload Control** page.

Once every row has been processed a summary dialog appears to inform you of how many rows failed and how many passed. Please note this dialog does not give you the result of provisioning these items; only the result of uploading the items into the Unifed Contact CenterManagement Portal system.

Data Types

The Data Type **SNC** means **Standard Naming Convention** and is the same as what the UI allows you to type into the name fields in the provision pages, for example, Alphanumeric, no exclamation mark or hyphens, and so forth.

The 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).

Fields using the Data-Type **BOOLEAN** can contain the values: **TRUE**, **FALSE** or be left empty. Leaving these fields empty defaults the field to **FALSE**.

Y/**N** Data-Type is similar to Boolean however ts can only contain the values **Y** or **N**.

Date format is the universal date format <**Year**>-<**Month**>-<**Day**> for example 2006-08-30.

Incorrect Data Type example

It is vital to make sure that the values you place in the template are of a valid data-type. In the example below, an alphabetic data type has been used instead of a numeric one for a single field.

```
Name,Description,PortalLogin,FirstName,LastName,LoginName,Peripheral
Number,BadAgent,imported agent,bada,bada,bada,bada,p
```

Note Some required columns have been omitted for the sake of simplicity.

This produces the following error:

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

Agent Security Field Example

Dos-styled Syntax Example:

```
<USERORGROUPNAME>:<ROLENAME>;<USERORGROUPNAME>:<ROLENAME>[:<MULTIPLE
ROLENAMES>]
```

This is an example of what can be put into 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.

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 **Path** column when attempting to upload items which cannot live in the **Root** 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.

8 INDEX

N

O

P

R

S

T

U

W

Y