## CONTENTS

Preface ................................................................................................................................. 7

Purpose ............................................................................................................................... 7

Audience ............................................................................................................................ 7

Organization ...................................................................................................................... 7

Obtaining Documentation ............................................................................................... 7

Documentation Feedback ............................................................................................... 8

Cisco Product Security Overview .................................................................................. 9

Obtaining Technical Assistance ...................................................................................... 10

1. Welcome ....................................................................................................................... 13

About the Web Administration Portal .......................................................................... 13
   Overview ......................................................................................................................... 13
   How does it work? .......................................................................................................... 14

Getting Started ............................................................................................................... 14
   Overview ......................................................................................................................... 14
   Host Administrator First Steps .................................................................................... 14
   Tenant Administrator First Steps ................................................................................ 14
   Tenant User First Steps ............................................................................................... 15

Open the Online Help ...................................................................................................... 15

Log in and log out ............................................................................................................ 15
   Logging in ...................................................................................................................... 15
   Logging out .................................................................................................................. 17

Home Page ...................................................................................................................... 17
   Your Home Page ......................................................................................................... 17
   User Categories .......................................................................................................... 17

Change Your Password .................................................................................................. 20

Web Tool Commands and Browser Interaction ......................................................... 21
   Supported Browsers .................................................................................................... 21
   Using Popup Blockers ................................................................................................. 21

System Administration ................................................................................................ 21
   Administrator Tasks .................................................................................................... 21
# Table of Contents

## 2. Basic Mode ................................................................. 25
- Team Management ......................................................... 25
- Agent Reskilling .............................................................. 28

## 3. Settings ........................................................................ 31
- Manage Settings .............................................................. 31
- Change Your User Settings ............................................... 31
  - Basic Options ............................................................ 31
  - Advanced Options ....................................................... 32
- Change Global Security Settings ........................................ 32
  - Overview ................................................................. 32
  - Managing Global Security Settings ............................... 33
  - Preset Global Security Settings ...................................... 34
- Change the System Settings .............................................. 35
- About Settings ............................................................... 37

## 4. Information Notices .................................................... 39
- Manage Information Notices ........................................... 39
  - Overview ................................................................. 39
  - Basic Mode options .................................................... 39
  - Advanced Mode options .............................................. 39

## 5. Audit Reports ............................................................. 43
- Understanding Reports ................................................... 43
- View a Report ............................................................... 44
- Manage Reports ............................................................ 46
  - Manage Reports ........................................................ 46
  - Manage Parameter Sets .............................................. 47
- Edit a Report ............................................................... 49
- Set Report Exception Thresholds ..................................... 49

## 6. System Manager .......................................................... 51
- Manage the System ....................................................... 51
  - Page Access and Use .................................................. 51
  - Using Portal With Other Provisioning Systems ............... 51
  - What are Resources? .................................................. 51
What is the System Manager tool? ......................................................... 53
Anchor Resources................................................................................... 54

Tree Structures ......................................................................................... 54
Organizing the tree contents ................................................................. 55
Navigating the Folder Tree ..................................................................... 55
Managing the Tree .................................................................................. 55

Resource Folder Tree Panel ................................................................. 55
Panel Access and Use ............................................................................ 55
What is a Resource Folder? ................................................................. 56
How to Create a Resource Folder ......................................................... 56
How to Bulk Create Folders ................................................................. 57
How to Delete a Resource Folder ......................................................... 57
How to Move a Resource Folder ......................................................... 57

Items Panel ............................................................................................ 57
Panel Access and Use ............................................................................ 57
List Resource Items ............................................................................. 57
Select a Resource Item ........................................................................ 58
Create a Resource Item ....................................................................... 58
Move Resource Item(s) ....................................................................... 58
Delete Resource Items ....................................................................... 59

Details Panel .......................................................................................... 59
Page Access and Use ........................................................................... 59
Details Tab ............................................................................................ 59
Associations Tab ................................................................................... 59
Advanced Tab ...................................................................................... 60
History Tab .......................................................................................... 60

Resource States ..................................................................................... 60

Uploading Resources ........................................................................... 61
Template Guide ..................................................................................... 61
Using the Bulk Upload Tool ................................................................. 66

Agent Management ................................................................................ 68
Manage Persons ................................................................................... 68
Manage Agents ..................................................................................... 72
Manage Agent Desktops ................................................................. 79
Manage Agent Teams ........................................................................ 84
Manage Skill Groups .......................................................................... 87
Manage Enterprise Skill Groups ......................................................... 90

Contact Management ........................................................................... 92
Manage Dialed Numbers ................................................................. 92
Manage Directory Numbers .......................................................... 94
Manage Call Types ......................................................................... 96
Manage Labels ................................................................................ 98

Equipment Management ...................................................................... 100
Manage IP Phones ........................................................................... 100
Manage Directory Numbers ........................................................ 103
PREFACE

Purpose

This document explains how to use the Unified Contact Center Management Portal to view and alter your system.

Audience

This document is intended for all users of the 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, "Welcome"
Provides basic information on the Portal environment, and how to use the context-sensitive online help.

Chapter 2, “Basic Mode”
Provides all the information needed by the vast majority of users in order to manage agent teams and agent skill groups.

Chapter 3, "Settings"
Describes how a user can change their settings, or the settings of others, such as email address, timezone, or security privileges.

Chapter 4, "Information Notices"
Explains how to view and edit information notices.

Chapter 5, "Reports"
Describes how to set up and view audit reports.

Chapter 6, "System Management"
Describes the folder structure of the Management Portal, and explains how to set up and maintain agents, contacts, equipment and other resources using the Portal.

Chapter 7, "Security Management"
Explains how to set up security settings for individual users by means of roles and tasks, and how users with the same permissions can be added to groups to simplify management.

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:

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:
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:

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:
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:
Asian-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:
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:


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:

1. WELCOME

About the Web Administration Portal

Overview

The Portal is a browser-based management application designed for use by contact center/system administrators, business users and supervisors. It is a dense, multi-tenanted provisioning, reporting and connectivity platform that overlays the contact center equipment. The contact center equipment is viewed as consisting of configuration items, generally known as resources, such as agents or skill groups, and events logged when the resources are used by the equipment, such as call record statistics.

The Portal partitions the resources in the equipment using a familiar folder paradigm and these folders are then secured using a sophisticated security structure that allows administrators to specify which users can perform which actions within the specified folder(s). The Portal supplies a number of tools that operate on the configuration and statistics data. The tools are all inherently multi-tenanted and those supported currently are:

- The Information Notices tool that implements the "Message of the Day" functionality
- The Security Management tool that implements the user and group task/role based security strategies
- The System Management tool that implements the resource partitioning strategies and provisioning operations
- The Reports tool that implements web based reporting

The Portal's focus on supplying dense, multi-tenancy functionality plays to the business plans of hosts and large enterprises as it allows the distributed or disparate contact center equipment to be partitioned or segmented to satisfy the following business goals:

- The Portal abstracts and virtualizes the underlying contact center equipment, thereby allowing centralized deployment and decentralized control which in turn gives economies of scale whilst supporting multi-level user command and control
- The Portal allows the powerful and flexible native IPCC provisioning operations to be abstracted into simple, high level tasks that enable business users to rapidly add and maintain contact center services across the virtualized enterprise (or portion thereof)
- A Portal user will only see the resources in the platform that he/she is entitled to see, thereby giving true multi-tenancy
- A Portal user may only manipulate those resources visible to them by using the Portal tools and features he/she has been authorized to use, thereby giving role-based task control
How does it work?

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

Getting Started

Overview

A useful view of the Web Portal is to consider that there are typically a small number of different classes of user:

- The host administrator who is responsible for the whole platform and therefore has a view across all the equipment, tenants and their resources.
- The tenant administrator who is responsible for the slice of the system assigned to that tenant by the host administrator.
- The tenant user who has access just 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 class of users 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:

- Ensuring that the tenant equipment (peripherals) are correctly located in the tenant or Shared folders
- Creating an administrator user for each tenant.
- Adding them to the tenant administrators group and assigning any specific roles

Tenant Administrator First Steps

The tenant administrator is responsible for:

- Creating a resource folder structure that maps onto the tenant's business
- Moving the tenant's resources into the relevant subfolders
- Creating security groups which provide the required role based access to the subfolders
- Creating the required number of users and assigning them to the security group(s) relevant to the role of the user

**Tenant User First Steps**

The tenant user (usually called just the user) created by the tenant administrator may now login to the system. Select the appropriate tool from your home page:

- To view or manage information notices select the Information Management tool
- To manage users/security groups select the Security Management tool
- To manage resources (dimensions) select the System Management tool
- To view or manage reports select the Reporting tool

**Open the Online Help**

For security purposes the online help is only available after the user is logged in. To open the online help, click the **Help** link in the top right corner of the screen. It provides:

- Instructions for using, provisioning and managing the system
- Descriptions of the reports which you use
- A comprehensive glossary
- Logical indexing to help you quickly find the topics you need
- Search facilities

This help dialog consists of a main panel in which the topic text is displayed.

To the left of the main panel are four tabs. Click on the tab header to display the tab contents. The tabs are as follows:

- **Contents** displays the topic list as a table of contents, to help you locate the topic you require
- **Index** lists the keywords which you can use to find related topics
- **Search** enables you to search through all the topics for a particular word or phrase. Enter the text in the field provided and click **Go**. A list of all the topics in which the text occurs are then listed. Similarly you may also use the search field displayed in the top right of the dialog window
- **Glossary** comprehensively covers and explains the terms and entities comprising the Management Portal

**Log in and log out**

**Logging in**

To login to the system:
1. Open your web browser and enter the URL address of the web server in the browser's address field. This will be in the format:

   https://<Portal server>/portal

   For example, one possible web server address might be:
   https://webserver1/portal

2. The security access banner is displayed to inform the user that access to the platform is restricted to authorized users

   Note This banner can be changed by the administrator for the whole platform to meet the needs of the specific deployment (for further information see the Change Your System Settings topic). Press the agree button

3. The Login page is displayed. Enter your User Name and Password details in the fields then click Login. If the login is successful then the user's home page will be displayed

   Note Before the first time the system is used, the User Name for the host administrator is automatically set to administrator, with a blank password. A new password should be set immediately.

   Note If you do not perform any action on the system for a time, the system will automatically log you out.

   Alternative Login

   If the web page is already open, click Logout to log out the previous user and display the normal login window

   First time users

   - The first time you access the Web Tool you may be prompted to accept a security certificate. Accept this security certificate then proceed

   - After you have first logged in, you may have to change your password immediately. If prompted to change your password you must do so immediately, otherwise further access will be denied. For further information see the Change Password topic

   Note

   - The password field is case sensitive. That is, capital and lower case letters are regarded as different, so if your password was 'password1' and you entered 'PASSWORD1' your login would fail. If you have difficulty logging in, make sure that you have not accidentally pressed the caps lock key

   Note Your password should never be anything as easy to guess as this example. For tips on how to create a secure password that you can remember, see the Change Your Password section.

   - By default, the maximum number of attempts you have to log into the system correctly is three. If, after three attempts, you still have not logged in correctly, your user account will be locked out. If this is the case, contact the administrator responsible for re-enabling it
The system will automatically log out a user when the web browser window is closed

Logging out

Once your user session is finished, close your browser session to ensure that no other user can interfere with your account.

To logout of the tool, click the **Logout** button located on the top right side of your browser window. Alternatively, close the web browser window to log out automatically.

Home Page

Your Home Page

Once you have logged in you will be presented with your personalized home page which is the launch pad for accessing the rest of the system.

For a **basic mode** user, the main central panel displays your most frequently used **reports**, which are organized into related **report groups**. For further information, see the **basic mode options** section below.

For an **advanced mode** user the main central panel will display the **system management** functions which you can access. For further information, see the **advanced mode options** section below.

The **Toolbar** at the top right of the screen displays further functions, which may vary depending upon the system functions you are using and the permissions granted to you.

The very top of the page displays a list of the pages you have navigated through to access your current page. This is called the **breadcrumb trail**. Each page in the trail is displayed as a link to help you quickly return to previous pages.

To the right of the breadcrumb trail, you will find the following options:

- **Home** Click to return to your homepage
- **Help** Click to display this online help. It contains everything you need to understand and use the system features, reports and report analysis. See the Online Help topic
- **Settings** Click to select the settings you need to change. See the Manage Settings topic
- **Logout** Click to end your session. See the Logging in and logging out topic

If any of these terms are unfamiliar to you, please look them up in the **Glossary**.

User Categories

Portal users are divided into two different categories:

- **Basic users** need to view reports and define their own user settings, but do not require system management functions
Advanced users may navigate the folder tree. Advanced users manage the system and the resources it contains, system reports and analyses, as well as defining the users who can access the system and their user rights.

Basic mode options

On logging in, if you are a basic user of the Management Portal (or if you are an advanced user using basic mode) you will see a flat list of the reports you have access to. You can always return to this list of reports (this is the homepage for basic mode) by clicking on Home at the top right of the screen.

In the bar above the list of reports are a number of menu options:

- Delete Report - deletes selected report
- Run Report - runs selected report
- Agents - allows you to manage your agent teams
- Skill groups - allows you to manage your skill groups

For further information please see:

- How to change your password
- How to manage settings
- How to change your timezone settings
- How to use the online help
- How to login and logout

Advanced mode options

Advanced users require more complex reporting functionality as well as access to system management functions. To access these functions, you must be in advanced mode.

To switch between basic mode and advanced mode, click on Settings > User Settings. Check the Advanced Mode checkbox in the middle of the user settings in order to view the functions you have access to. This is the Tools page.

You will see some or all of the following display:
You can set a commonly-used tool to be your homepage using the Settings page.

Which of the following tools you can use depends on your security permissions, as determined by the global and non-global roles that have been assigned to you.

**Note** If you think you should have access to some of these tools but cannot see them in the Tools page, contact your system administrator.

- The **Audit Reports** section enables you to view and manage audit reports, which provide information about the changes made to the system.
- The **Security Manager** section enables you to create and manage users and groups, their roles, which define the tasks they may perform and manage security; the customer data and system functions they may access.
- The **System Manager** section enables you to provision and manage the entire system, the reports and the resources they report on.
The **Information Notices** section enables you to create and manage online notices; a messaging feature which informs and updates system users with important information.

Further advanced functions include:

- **Settings** This section covers the creation and administration of system, display, user and password settings. See the Manage Settings topic.

- **Prefix Management** This section covers the creation and administration of the prefixes applied to report formats. Prefixes are used by the system to enable one format to be changed into another format and for importing non-Portal reports. See the Prefix Management topic.

- **Report Uploading** This section covers the procedures used to import external reports into the Portal system. See the Upload a Report topic.

**Caution** Advanced user rights should be assigned to a strictly limited number of people. Due to the large number of users involved, organizing and maintaining the currency of system information is vital if the system is to be used effectively. It may even prove necessary to assign change rights to a limited few users and implement a change strategy to ensure that any change is approved before the advanced user is requested to enter the changes in the system. This could avoid duplication of work or prevent vital information from being accidentally deleted.

### Change Your Password

To display the **Settings** page click **Settings**. Click **Change Password**. The **Change your password settings** page will be displayed.

You will need to change your password if:

- You have logged into the Web Portal for the first time.
- The system has been configured to request you to change it after a specific length of time.
- Your password has become known to others.

To change your password

1. Enter your **Old Password**.
2. Enter your **(New) Password**.
3. Re-enter your new password in the **Confirm Password** field.
4. Click **OK**.

**Note**

- Your password must normally consist of at least 3 characters. There may also be other requirements, commonly that it must include lower case letters, upper case letters and numbers. Contact your system administrator for more details.
- Your previous passwords are stored in memory, therefore you cannot reuse passwords.
Tip You can create a password that is both memorable and secure by choosing a memorable phrase such as your proverb or a line of your favourite poem, selecting the first letters of each word in that phrase, and turning some of those letters into numbers. For example, the proverb 'a chain is no stronger than its weakest link' shortens to 'acinstiwl', which can be turned into a password 'AC1nst1WL' which is easy to remember but difficult for a hacker to crack.

Web Tool Commands and Browser Interaction

Supported Browsers
This Web Tool is designed for use with specific Web browsers and browser versions. The Login page will display an alert if the browser (or browser version) you are using is unsupported. It will also display information on supported browsers.

Using Popup Blockers
This Web Tool may be adversely affected by browser or third-party popup blocking utilities. When using this tool either disable popup blocking or exclude this tool's domain from popup blocking.

To disable popup blocking (in other words, to enable popups) in Internet Explorer (IE):
1. Click on Tools and select Internet Options
2. Select the Privacy tab
3. At the bottom of the window, click on the Block pop-ups box to remove the checkmark. If the box is already empty, leave it as it is
4. Click on OK

Alternatively, you can enable popups for the Web Tool only. To do this using IE, use the Web Tool normally until a message is displayed at the top of the browser window telling you a popup has been blocked. By clicking on this you may choose to permanently allow popups from the Web Tool, while still remaining protected against popups from other sites.

Different browsers may have different methods of disabling popup blocking.

System Administration

Administrator Tasks

Overview
This section identifies the primary tasks that users with tenant administrator permissions perform in the Management Portal. Tasks do not need to be performed in the order shown below; however, this order offers expediency as it reflects the dependency of certain record types on the pre-existence of others.
Some of the tasks listed below may need to be performed only once; for example, specifying global values for reporting purposes. Others will be ongoing, such as creating and maintaining agent accounts.

**Note:** Users with System Administrator permissions can also perform all of the tasks in this section.

### Agent and Group Related Tasks

The tasks listed below pertain to agent record creation and agent groupings.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Agent Desk Settings.</td>
<td>Agent Desk Settings associate a set of permissions or characteristics with specific agents, such as how and when calls to these agents are redirected, how and when they enter various works states, and whether they can make outbound calls. You can create a Default Desk Setting that is the set of permissions automatically assigned to all new agents unless overridden.</td>
<td>Manage Agent Desk Settings page</td>
</tr>
<tr>
<td>Create Persons, Agents and Agent Supervisors. Assign Agent Desktops to agents.</td>
<td>Every individual who uses IPCC must be represented by a person item. You can then define these persons to be Portal users and/or agents. You can designate certain agents as supervisors, allowing them to be later designated as supervisors of agent teams. Supervisors - provided they have an Active Directory account on IPCC's AD domain - can be given access to WebView Reporting. You can assign different desk settings to different agents based on their needs, and, as necessary, temporarily suspend their login privileges or turn on Agent State Trace, which allows you to track their transition through various states of readiness.</td>
<td>Manage Agents page</td>
</tr>
<tr>
<td>Create Skill Groups and assign agents to skill groups.</td>
<td>A skill group is a collection of agents that share a common set of skills. In IPCC, skill groups are one of the primary devices for routing and reporting.</td>
<td>Manage Skill Groups page</td>
</tr>
</tbody>
</table>
An agent can be associated with multiple skill groups and each skill group is associated with a specific media routing domain (MRD) such as voice, chat, or e-mail. Note that the IPCC Web Administration Tool allows you to create, view, and assign agents to Voice skill groups only. If you are deploying other MRD options, skill groups associated with those MRDs must be administered via the Administration interfaces for those applications.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Agent Teams. Assign agents and supervisors to teams.</td>
<td>Agent teams allow you to associate a set of agents with a specific supervisor. In addition to reporting uses, this association also allows IPCC to determine which supervisor to route an agent's Supervisor Assist requests to.</td>
<td>Manage Agent Teams page</td>
</tr>
<tr>
<td>Optionally, create Enterprise Skill Groups. Assign skill groups to enterprise skill groups.</td>
<td>An enterprise skill group is a logical grouping of skill groups, and can include skill groups from different MRDs. Through enterprise skill groups, you can generate reports that include any grouping of skill groups you desire. Note: Unlike the Skill Groups page, the Enterprise Skill Groups page in IPCC Web Administration can display skill groups from all MRDs.</td>
<td>Manage Enterprise Skill Groups page</td>
</tr>
</tbody>
</table>

**Contact Routing Tasks**

The tasks listed below pertain to contact (voice and non-voice) routing configuration.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Call Types.</td>
<td>A call type is a category of incoming routable task. Specific call types are associated with Dialed Numbers. In this association, each call type has a schedule that determines which routing script(s) are active for that call type at any time. Because the call type determines which routing script is run for a call, the call type defines call treatment in an IPCC</td>
<td>Manage Call Types page</td>
</tr>
</tbody>
</table>
| Enterprise system.  
There are two classes of call type/dialed number associations: voice and non-voice. | Create Dialed numbers.  
Map Call Types to Dialed Numbers. | Manage Dialed Numbers page |
|---|---|---|
| In IPCC, you set up a Dialed Number List, which identifies all of the phone numbers in your contact center that customers can dial to initiate contact. Dialed numbers are mapped to call types; this mapping is used to identify the appropriate routing script for each call.  
A typical call center requires a number of dialed number definitions. In addition to answered calls, dialed numbers also need to be set up for ring on no answer, dialed number plan entries, and for supervisor/emergency assist calls. |  | |
2. BASIC MODE

Team Management

The Agents option allows supervisor agents to manage the agents in their agent teams.

To see an agent team, click on the My Agent Team drop-down box and select the team you wish to work with. A list of the agents in the team will be shown below the box.

The agent list shows each agent's name, their status within the system (such as Ready or Pending), and the date from which they have been active in the system (an Active From Date in the future indicates an agent who has not yet started work). There is also an agent details icon that allows you to view and edit agent details, and a copy icon that allows you to create a copy of an agent (for example, if you wish to add to your team a new agent who has exactly the same skills as an existing agent).

To view or edit an agent

1. Select an agent team from the drop-down list
2. Click on the agent icon (not the copy icon beside it). The Edit the current Agent page will open, showing you the agent's details
3. Make any changes to the agent. Selecting a different tab (such as Supervisor or Agent Teams) will show a different set of fields. You can always go back to previous tabs

Note You are unlikely to need to use the Advanced tab unless you are changing start or finish dates for an agent
4. Click Save to save your changes or Cancel to leave the agent's details as they were before you started editing

To set an agent's starting or leaving date

1. Select an agent team from the drop-down list
2. Click on the agent icon (not the copy icon beside it) for the agent you wish to edit. The Edit the current Agent page will open, showing you the agent's details
3. To set or change an agent's starting or finishing date, select the Advanced tab. You may either type in the date manually (it is in the format day/month/year) or:
   - Click on the calendar icon beside the Active To Date (finish date) or Active From Date (start date) field. A calendar popup will appear
   - Make sure the month and year shown at the top are correct
   - To change the month, click on the pairs of arrows to the left and right to scroll through the months until you find the one you want
- To change the year, click on the pairs of arrows to the left and right. Going right from December will take you to January of the next year, and vice versa
- Select the date
4. Set the time on the selected date on which the agent is starting or finishing (for example, 17h 00m for someone leaving at the end of business hours)
5. Click Save to save your changes or Cancel to leave the agent's details as they were before you started

To add a new agent

**Note** All agents must be associated with a person. If a person record for the new agent does not already exist on the system, you can create one as part of adding a new agent.

1. Click the New menu option. The Create a New Agent page will be displayed.
2. Fill in the fields for each tab.
3. All the fields that you must fill in are marked with a red asterisk. These fields are on the Details tab. The Save button will not be enabled until all the required fields have been filled in.

- On the Details tab
  1. Fill in the Agent's Name (such as BOates or Beth_Oates)
  2. Give a description of the agent (such as a job title)
  3. Select a Peripheral to create the agent on (if you are a supervisor agent, this should usually be the same peripheral that you use)
  4. Choose whether to associate the agent with an existing Person, or to create a new one. A Person can have more than one agent identity if all those agents are created on different peripherals

- Select an existing person from the drop-down list, or search for a specific person by typing a part of their name in the Search box. The new agent will use the details specified in that Person’s Peripheral Login box to log on to their Agent Desk Setting.
- To Create a New Person, enter the first name and last (or family) name for the person, and fill in the details they will use to login to the peripheral. The person will be automatically created and associated with the agent.
Note Multiple Agents may be associated with a single Person, if all Agents involved are on different peripherals

- On the Supervisor tab
  1. If the agent is to be a supervisor, check the Supervisor checkbox. If this box is checked, you will also need to set a domain account
  2. If the agent is a supervisor, they must be associated with a domain account (the account they will use to log into a computer on the contact center network). Type in part of the account name, click Find and then select the correct account

Note You cannot set up a domain account from the Management Portal. Contact your IT department if you are uncertain of the domain account to use.

- On the Agent Teams tab
  1. Select an agent team for the agent to belong to. Agents may only be a member of a single team, but a supervisor can supervise multiple teams. Use the Selected Path drop-down to see agent teams in other folders
  2. Click the Add button to associate the team with this agent
  3. Check the Member box to make the agent a member of the team. Supervisors can supervise a team without being a member
  4. If the agent is a supervisor, they can supervise the team without being a member. Select a primary or secondary supervisory role for any team they are to supervise

- On the Skillgroups tab
  1. Select skillgroups for the agent to belong to. Use the Selected Path drop-down to change folders
  2. Click Add to add the agent to the selected skillgroups

- On the Advanced Tab

Note You will probably only edit these settings to set an agent's start or finish date

  1. Enterprise Name is the name the agent is known as within the Management Portal
  2. Agent Extension is the internal extension number for the agent
  3. Agent Desktop allows you to specify the agent's desk settings (also called the Agent Desk Setting)
4. Check State Trace if you wish to let the system track the agent’s state, such as whether they are logged off or talking.

5. Use the Active From Date box to set the agent's starting time and date (you may enter the date manually in day/month/year format, or select a date from the calendar).

6. Use the Active To Date box to set the agent's leaving date.

4. Check the Create Another checkbox to create another agent whose settings are identical to this agent's except for their name and login details.

5. Click **Save** to create the agent, or **Cancel** to cancel agent creation and return to your homepage.

To change an agent's team:

1. Select the agent team to which the agent belongs from the drop-down list.

2. Click on the agent details icon (not the copy icon beside it) for the agent you wish to edit. The **Edit the current Agent** page will open, showing you the agent's details.

3. Click on the **Agent Teams** tab. The agent's current team membership is shown.

4. Select the agent team and click on the **Remove** button.

5. You may optionally select a team from the list below and click on **Add** to add the agent to that team. You can add the agent either as a member of that team by checking the **Member** box, or as a primary or secondary supervisor if they are a supervisor agent.

6. Click **Save**.

### Agent Reskilling

The **Skill groups** option allows you to view and edit agent skill groups.

To see a skill group, click on the **Skill group** drop-down box and select the skill group you wish to work with. A list of the agents associated with the skill group will be shown below the box. A complete list of all the agents who can be associated with the skill group (those who are on the same peripheral as the skill group) is shown below that.

The agent list shows each agent's name, their status (such as R for Ready or S for Synchronizing), and the date from which they are active in the system (an **Active From Date** in the future indicates an agent who has not yet started work). Clicking on the green arrow icon allows you to edit the agent.

To add an agent to a skill group:

1. Select a skill group for the agent or agents to belong to.
2. Select agents to belong to the skill group using the checkboxes. Use the **Selected Path** drop-down to see agents in other folders.

3. Click the **Add** button to associate the agents with this skill group.

4. Click **Save** to save your changes, or **Cancel** to leave the details as they were before you started.

To remove an agent from a skill group:

1. Select a skill group to remove an agent or agents from.

2. In the top list, select agents to remove from the skill group using the checkboxes.

3. Click the **Remove** button to remove the agents from this skill group.

4. Click **Save** to save your changes, or **Cancel** to leave the details as they were before you started.
3. SETTINGS

Manage Settings

Settings enable you to control how the system is displayed, user security and the functionality available to users.

To display the Settings page click the Settings link.

The settings which you can customize are as follows:

- **User Settings** Enable you to change your timezone, name and description. Advanced users may also change their homepage settings.
- **Security Settings** Enable system users with sufficient security privileges to create and manage users, groups, tasks and roles.
- **System Settings** Enable system users with sufficient security privileges to control the entire contents of the system.
- **Display Settings** Enable you to customize the management features displayed in your homepage.
- **Password Settings** Enable you to change your password.

Change Your User Settings

Basic Options

To display the Settings page click the Settings link. Then click User Settings. The Update settings for this user page will be displayed.

To change your user settings, select or overwrite the required fields and click OK. These fields are explained below.

- **Timezone** Select your local region from the drop-down list
- **First Name** and **Last Name** Change your name. You may want to do this if you have married, or if you normally use a name other than the First Name entered here (such as a middle name)
- **Email** Enter the email address you want the Management Portal to send your emails to, if any
- **Description** Enter a suitable description of yourself (such as job title or departmental role)
- **Page Transition** Select from the drop-down list to determine the graphical effect used when refreshing the page or displaying a new page. The choices are:
  - **None** The new page will simply appear
  - **Pixelate** The page blurs into large squares and then resolves itself into the new page
  - **Gradient Wipe** The new page gently wipes across the old page from left to right
- **Spiral** The new page replaces the old one in a spiral from the outside to the center
- **Wheel** The new page replaces the old one in several lines wiping around the page, like a turning windmill
- **Radial Wipe** The new page replaces the old one in a line wiping around the page, like a clock hand
- **Iris** The new page appears in a cross that wipes outward over the old page
- **Transition Duration** This drop down list determines the length of time the Page Transition will take to change the screen. Select from 1 (the fastest) to 5 (the slowest)
- **Data Paging Size** This field dictates the number of selected items to be displayed per page, for example in the central Items panel of the System Manager. Numbers above 20 are not recommended
- **Text Only Mode** Check this box to set your display to a simplified text-only view. You will have to log out and log back in for your display to change

**Advanced Options**

If you have sufficient security credentials you may access further functions. Select or overwrite the required fields and click **OK**. These fields are explained below:

- **Advanced Mode** This checkbox changes your homepage view from a set of reports (this view is the only view possible for basic users) to the homepage specified by the **Default Homepage** field below. By default, this will be a view of the tools you have access to
- **Show Hidden Items** Check this checkbox to view all hidden items you have permission to see
- **Show Disabled Items** Check this checkbox to view all disabled items you have permission to see. Items are sometimes disabled so that they can be edited without affecting live reporting operations
- **Default Homepage** Allows you to change your homepage. Select a tool from the drop-down menu to display that tool as your homepage when you are in Advanced Mode. To see all your tools in your homepage, select the **Tools View**
- **Tools Layout** Allows you to change the format of the Tools Page. You may choose between a list of tools or a table

Click **OK** to save your settings.

**Change Global Security Settings**

**Overview**

Security settings define the tools which users or groups can use, via global roles.
Managing Global Security Settings

To display the Security Settings page click the Settings link. Then click Security Settings.

The global roles available in the system are listed beneath the Name column. Any explanatory text is listed beneath the Description column.

To view or edit a global role

1. Click the properties icon next to the role name. The Edit Global Role page will be displayed. Any of the fields below can be modified:
   - The Name section displays the name of the user or group (this is not a field and cannot be edited)
   - The Description field contains explanatory text
   - Select the Enabled checkbox to ensure that the role is live in the system
   - Select the Hidden checkbox if you wish the role to be saved in the system but not yet accessible to users

2. All the tasks associated with the selected role are displayed beneath the Name column. Select tasks to allow the members of this global role to perform them within the system.

3. Click OK.

To create a new role click New. Fill in a name, and then proceed as for editing a role, above.

To edit the members of a global role

1. Select the Properties of the global role. You will see the Edit Global Role page.

2. Select the Members menu option. You will see a tree structure on the left, and a list of users and groups associated with the global role on the right. The central panel allows you to select users and groups to add to the role.

3. Using the left hand tree structure, navigate to the folder containing the user or group you wish to associate with the role.

4. Select either User or Group from the drop-down box in the central panel. All items of that type within the folder will be displayed.

5. Select users and groups to associate with the role. No OK button is available to be pressed, as the panel on the right will update automatically.

You can remove users added from a role by clicking on the red cross next to the properties icon in the right hand panel.
To delete a global role, select the checkbox of the role to be deleted and click **Delete**.

**Caution** It is recommended that you only delete global roles that you have created.

### Preset Global Security Settings

The Management Portal comes with a number of groups and roles predefined. To give a user administrator privileges over your entire system, for example, it is only necessary to assign them to the `<Tenant>` Administrators group. The following table shows what groups are supplied with the system and what global roles they are assigned. The tasks that make up each of the roles are also listed.

<table>
<thead>
<tr>
<th>Group</th>
<th>Whereabouts</th>
<th>Roles (global)</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone</td>
<td>Root folder</td>
<td>Tenant User</td>
<td>Browse Dimension Types, Schedules, Manage Self, Reports</td>
</tr>
<tr>
<td><code>&lt;Tenant&gt;</code> Users</td>
<td>Tenant folder</td>
<td>Tenant User</td>
<td>Browse Dimension Types, Schedules, Manage Self, Reports</td>
</tr>
<tr>
<td><code>&lt;Tenant&gt;</code> Supervisors</td>
<td>Tenant folder</td>
<td>Tenant Supervisor</td>
<td>Provision Agent, AgentTeam, Skill group</td>
</tr>
<tr>
<td><code>&lt;Tenant&gt;</code> Administrators</td>
<td>Tenant folder</td>
<td>Tenant Administrator</td>
<td>Browse Connected Systems, Global Roles, Global Security, Roles, Provision Agent, AgentDesktop, AgentTeam, CallType, DialedNumber, IPEndpoint, Line, Skill group, UserVariable, Information Notices, Security Manager, System Manager, Bulk Import Dimensions</td>
</tr>
<tr>
<td>Administrators</td>
<td>Tenant folder</td>
<td>Host Administrator</td>
<td>Browse Connected Systems, Global Security, Manage Global Roles, Global Security, Roles, Schedules, Site, Provision Agent, AgentDesktop, AgentTeam, CallType, DialedNumber, IPEndpoint, Line, Skill group, UserVariable, Advanced User, Security Manager, System Manager, Information Notices, Bulk Upload Dimensions</td>
</tr>
</tbody>
</table>
Caution Host administrators must always be able to perform the Advanced User, Manage Global Roles, Manage Global Security and Security Manager global tasks.

Caution It is strongly recommended that you do not remove any global security privileges from the Everyone group or users could become unable to access the system.

There are also four non-global roles corresponding to the four global roles provided. Non-global roles specify permissions for individual folders.

**Change the System Settings**

Typically, only a user with sufficient permissions has the right to access and manage system settings. System settings mostly enable a user to define user password requirements.

To display the **Settings** page click the **Settings** link. Then click **System Settings**.

To edit the system settings
1. Display the **System Settings** page as described above
2. Change any or all of the following:
   - The **Product Name** field displays the name of the application
   - The **Login Message** field contains the message displayed to a user when the user logs into the system. By default a WYSIWYG editor is used, but by clicking on the <> button you can choose to work in plain text or insert your own HTML tags instead

   **Note** The login message should not exceed 250 characters in the default 8pt font

   **Note** To user the WYSIWYG editor to format the login message, you must highlight the text to be formatted and use the appropriate editor function. The editor functions do not allow you to format the text as you type, that is, clicking the / button (for example) will not 'switch on' italics mode for the text typed afterwards.
The Message Agreement Link field contains the text shown on the button that the user must click to proceed from the login message set above to the login page. This text should be no longer than 40 characters.

The Password Format field contains the required format for the password entered by a user. The options are:

1. **Custom** This is for users with high privileges only. It requires *regular expressions* and a knowledge of *system configuration*.
2. **Low** Any string
3. **Medium** Any string between the minimum and maximum password length
4. **Medium/High** Any string between the minimum and maximum password length, which must contain lowercase, uppercase, and numeric values
5. **High** Any string between the minimum and maximum password length, which must contain lowercase, uppercase, numeric values and any of the following characters: @ # $ % ^ & + = !

The Password Expiry (days) field displays the length of time the system will accept a password before the user is requested to change it.

The Number of previous passwords to check field displays the number of previous passwords the system accepted for a specific user. If any one of these previous passwords is used, the user will be denied further access to the system.

The Login attempts before lockout field indicates the number of times a user can enter the wrong password before being locked out of the system.

The Minimum Password Length field indicates the minimum number of characters the system will accept as valid for a password.

The Maximum Password Length field indicates the maximum number of characters the system will accept as valid for a password.

3. Click OK to save your settings.

To view information regarding system events which have occurred in the Management Portal:

1. Click the View application log option in the toolbar. The information is displayed in a table, which has 4 columns:
   - **Event** displays information regarding the event
   - **Date Time** displays the date and the time when the event occurred
• **Source** displays the data source the system was connected to when the event occurred

• **Message** displays any pertinent information relating to the event

2. When you have finished viewing the log, click the **Back** button to return to the **System Settings** page

**About Settings**

To display the **Settings** page click the **Settings** link. Then click **About**.

The **about this installation** page describes the version of Portal which you have installed on your system.
4. INFORMATION NOTICES

Manage Information Notices

Overview

Information notices (also sometimes called system notices) are similar to a notice board or Message of the Day feature. Information notices are a useful way to inform all contact center staff of general information in one action and in one location, rather than having to inform each staff member individually. Notices may typically include changes to agent assignments or important customer information. Once you have logged in, any information notices which apply to you are displayed in your homepage in a scrolling window at the top right corner of the screen.

Basic Mode options

To view an information notice

1. Hover your mouse pointer over the information notices panel. The panel will be expanded
2. Click the name of the required notice from the list. The notice text will be displayed in full
3. Once you have finished reading the notice, click Cancel

Note

- The information notices panel will only display current or valid notices. Notices which are out of date or pending are not displayed
- If you have sufficient user privileges, you may edit the notice. Click the Edit this Notice... link. Further information can be found in the Advanced Mode options section below

Advanced Mode options

To open the Information Notices tool as your homepage

1. Click the Settings link
2. In the Settings page, select User Settings
3. Select Information Notices from the Default Homepage drop-down list
4. Click OK
5. Click Home. The All System Notices page will be displayed

Alternatively, you may access the Information Notices section by clicking Tools. The Tools page will be displayed. Click the Information Notices header. The All System Notices page will be displayed.

Note The Tools page can only be accessed by users who have been granted Advanced Mode status. See the User Settings topic.
To create an information notice

1. Click New. The New System Notice page will be displayed

![Image of Cisco Unified Contact Center Management Portal]

2. Select the folder in the tree, whose users are the target audience for the new notice. The folder name will be displayed at the top of the page. Then perform the following:
   - In the Subject field enter a title for the notice
   - In the Content field enter the text. You can format the text as required by using the editor functions displayed above the text field. Functions include: text formatting, justification, bullet points and numbering, indenting, web linking and table add-ins. Click the <> icon to remove the editor functions or display them if they have been removed from the view
   - In the Valid From and Valid To fields, enter start and end dates to define the lifetime of the notice, by clicking on the calendar icons and selecting the appropriate months and days
   - Select the Create Another checkbox if you wish to add another notice after the creation of the current notice

3. Click OK

Alternatively, click Tools. The Tools page will be displayed. Click Create a Notice. The New System Notice page will be displayed, and you may proceed as per the bulleted list above.

To edit an information notice

1. Click the name of the notice to be modified beneath the Information Notices header. The notice will be displayed

2. Click Edit. The Edit Information Notices page will be displayed
3. Make the required modifications to the notice in the fields provided, as explained for creating an information notice above.

You may also edit an information notice by clicking **Tools**. The **Tools** page will be displayed. Select the notice to be edited from the **Edit a Notice** drop down list and click the **Edit** button. The **Edit Information Notices** page will be displayed.

**Note** To format the information notice, you must highlight the text to be formatted and use the appropriate editor function. The editor functions do not allow you to format the text as you type, that is, clicking the *I* button (for example) will not 'switch on' italics mode for the text typed afterwards.

To delete an information notice, click the red cross displayed next to the name of the notice to be deleted.

Alternatively, click the name of the notice where it is displayed beneath the **Information Notices** header. The notice will be displayed. Click **Delete**.

To move an information notice

1. Click **Tools**. The **Tools** page will be displayed
2. Click the **System Manager** header. The **System Manager** page will be displayed
3. Select the folder in the tree whose users or groups are the audience for the intended notice
4. In the **Items** drop down list select **Information Notices**. All the information notices for the selected folder will be displayed
5. Select the checkbox of the notice to be moved and click **Move**. The folder tree will be displayed
6. Select the folder to move the notice to and click **OK**
5. AUDIT REPORTS

Understanding Reports

A report is a 'snapshot' or overview of contact center operations; the customers, their resources and the agents (and agent groups) who provide them with customer service. Reports enable users to understand what is happening in the contact center; they provide information for auditing purposes.

A report is a combination of three factors:

- Report Data
- Report Template
- Report Parameters

**Report Data** consists of resources (such as Dialed Numbers) and the agents who provide Customer Service. These entities are stored in an hierarchical folder structure or Report Tree.

**Report Template** determines the exact ways in which the report can display data, and the data that it displays. Four audit report templates are included with the Management Portal. These are:

- **Audit Data Report** This report shows every change to a resource that has occurred within the system during the specified time period. This includes the name of the resource, the name of the user who made the edit, and whether the change was successful
- **Daily Audit Summary** This summarizes the changes made to resources during the day, showing the percentage and total of successful and failed changes at different times for individual items
- **Weekly Audit Summary** This summarizes the changes made to resources during the last week, showing the percentage and total of successful and failed changes on different days for individual items
- **Monthly Audit Summary** This summarizes the changes made to resources during the last month, showing the percentage and total of successful and failed changes on different days for individual items

**Report Parameters** provide the means of controlling the type and amount of information you wish to see in your report, as well as determining how the report is displayed. Not all reports have the same parameters. However some common parameters are as follows:

- **Sort Column** This is used to arrange the report columns so that you can focus on the column data which is of interest to you
- **From Date** and **To Date** The start and end dates of the time period covered by the report
- **Rows per page** The maximum number of report table rows displayed per page
View a Report

A report is displayed as a table; column headers display the name of the resources whose data is used in the report, for example agent or dialed number, and the rows display the data values for each column header.

Once you have logged in, all of the reports which you can view are displayed.

To open a report:

1. Select a report from the report group list(s) in your homepage by clicking the underlined report name. The View Report page will be displayed.

   Alternatively, you may open the report in one of the following formats, by clicking the associated icon:
   - **PDF** Click this icon to display the report in an Adobe Portable Document Format
   - **Excel** Click this icon to display the report in an Excel spreadsheet
   - **Enhanced HTML Renderer** Click this icon to display the report in HTML format

2. Before the report can be displayed select the parameters that apply to the selected report. These help you control how the report is displayed, the report format, and how to search through the report data. Options include the following:
   - **Parameter Set** The parameter set to view the audit report for. Some audit reports require parameter sets based on certain resource types. In these cases the resource type (such as Tenant) will be shown instead. The default `<new>` must be changed to a parameter set before you can run the report.
   - **Show only exceptions** If you check the Yes radio button, only items outside the report's exception thresholds will be shown, and it will be necessary to set exception thresholds to see any data at all.
   - **Header Text** Set a subtitle to be displayed under the main report title. This should explain the purpose of the report, for example 'Successful provisioning operations'.
   - **Date/Time From/To** The time periods that this report shows data for. You can choose to either set specific dates (Absolute) or set the date to Yesterday, Last Week and so on (Relative).
   - **Sort On** Select what field the report is to be ordered by. This should be the aspect of the report that interests you most. For example, if you are most interested in which provisioning operations have failed, you should sort the report by Event Outcome, which will group the data into Success and Failure within each resource type.
- **Sort Order** Whether the field you chose to sort on is to be displayed in alphabetical (Ascending) or reverse alphabetical (Descending) order.

The following options are available from the toolbar:

- **Edit** Enables you to modify the report details (not the report contents). For further information see the Edit a Report topic.
- **Save** Saves the changes you have made to the report's parameters.
- **Save as** Click to display the Enter details of the report to be saved page. Then perform the following:
  - In the **Name** field enter a unique name for the new report.
  - In the **Question** field enter a question which reflects the report contents, such as 'How many provisioning operations have failed?'

**Note** Linking or Save as means that the new report version is automatically linked back to the original report in the system.

- **Delete** Removes the report from the system.
- **Thresholds** Allows you to set thresholds for the report.

**Caution** A report saved under a different name shares the same references as the original and is therefore linked together in the system. Deleting a report may result in all linked reports being deleted.

Click **View Report**. The following options become available:

- If the report is too large to display on one page, it will be displayed across multiple pages. You can enter the number of the required page in the page number field or use the forward and backward navigation buttons to locate the page you need.
- The displayed report can be resized on the screen. Select the report size from the drop down list. 100% indicates that the report is displayed at the size it would be if printed.
- The **Search** field is used to look for specific items within the report. Enter the name or value you are looking for and click the **Find** button. You will be taken to the first occurrence of the data you are looking for. If the item occurs more than once, click the **Next** button to be taken to the next occurrence.
- Select the format you wish to view the report in from the drop down list. The following options are available:
  - **Hyper Text Markup Language (HTML) with Office Web Components**
  - **Extensible Markup Language (XML)** The report is displayed as pure XML script. This is useful if the report data is to be imported into a different system and can also be used with later versions of Microsoft Office to create Excel spreadsheets or Access databases.
- **Comma Separated Variable (CSV)** The report is displayed in a spreadsheet, with all data values separated by a comma.
- **Tagged Image File Format (TIFF)** The report is saved as an image and therefore cannot be edited.
- **Acrobat Portable Document Format (PDF)** This format enables you to distribute and print the report on any machine, provided the Adobe Acrobat reader software is installed.
- **Web archive** This option creates a stand alone HTML file with the extension .mhtml.
- **Excel** The report is displayed in a Microsoft Excel spreadsheet, which is useful if you wish to manipulate the report values at a later date.

Click **export** to view the report in the selected format.

- Click the **Refresh** icon to update the data displayed in the report.
- On the upper right of the **Report Parameters** panel, there is a double arrow icon. Click this to remove the **parameters** section of the page. This is useful if you have a large report and need the full screen to display it.

You may also open the report by clicking **Tools > View Reports**, selecting the folder in the tree which contains the report to be viewed, and selecting the correct report from the list.

**Note** The Tools page can only be accessed by users who have been granted Advanced Mode status. See the User Settings topic.

**Manage Reports**

**Manage Reports**

Report management involves moving reports within the Web Portal folder tree. Reports can be moved individually or in bulk. System users with sufficient security privileges can also edit multiple reports in one operation.

To display the **Reports** section

1. Click the name of the report in your homepage. The **View Report** page will be displayed.
2. Select the folder in the tree which contains the required report. A list of reports will be displayed for the selected customer/folder.
3. Select the required report. The **View Reports** page will be displayed.
4. Select the required parameters.
5. Click **View Report**. The report will be displayed.
Alternatively, click **Tools**. The **Tools** page will be displayed. Click **View Reports**. The **View Reports** page will be displayed. Then proceed as above.

**Note** The Tools page can only be accessed by users who have been granted Advanced Mode status. See the User Settings topic.

To save a report, click **Save**.

To save a report as (into a specified location)

1. Click **Save as**. The **Save Report As** page will be displayed.
2. Select a folder location for the new report to be saved in. Then perform the following:
   - In the **Name** field enter a name for the new report (parameter set).
   - In the **Sub Title** field enter a simple question which reflects the report contents and which is used as the displayed title for the report. For example, 'How many calls are queued?'
3. Click **OK**

To move a report

1. Click **Edit**. The **Edit Report Details** page will be displayed.
2. Click **Move**. The folder tree will be displayed in a new section.
3. Select the folder to move the report to and click **OK**

To delete a report, click **Delete** or click the red cross displayed alongside the report name in your homepage.

To print a report, click the print icon. The **Printer** dialog will be displayed. Select the print parameters and click **OK**.

**Manage 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.

To display the report's parameter sets

1. Click **Parameter Sets**. The **Parameter Sets** page will be displayed.
2. Select a folder. All the parameter sets for the selected folder will be displayed. The following options are available in the toolbar:
   - **New**
   - **Delete**
   - **Move**

To create a new parameter set

1. Click **Parameter Sets**. The **Parameter Sets** page will be displayed.
2. Select a folder. All the parameter sets for the selected folder will be displayed
3. Click on New to display the Create a new parameter set page
4. Select the item type to view from the Item type drop down list
5. Click Create Parameter Set
6. From the Folders tab, select the folder containing the resources, and choose whether you will be adding items in subfolders as well
7. 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
8. Click Add to add the specified resources to the parameter set
9. You may also remove resources from the parameter set by checking them and clicking Remove
10. Select the Save As option
11. In the Name field enter a name for the new report (parameter set)
12. Click OK

Note If a report is specified as using a particular type of parameter, such as tenant, you will not be able to use parameter sets that use different resource types, like Agent or Agent Team, with that report.

To modify the properties of a parameter set
1. Click Parameter Sets. The Parameter Sets page will be displayed
2. Select a folder. All the parameter sets for the selected folder will be displayed
3. Click the properties icon displayed next to the required parameter set. The Edit an existing parameter set page will be displayed. Then perform the following:
   • In the Name field modify the name of the report
   • Click the Enabled checkbox to ensure that the report is available to system users
   • Click the Hidden checkbox to prevent users from accessing it
4. Click OK

To delete a parameter set
1. Click Parameter Sets. The Parameter Sets page will be displayed
2. Select a folder. All the parameter sets for the selected folder will be displayed
3. Check the box of the parameter set (or sets) you wish to delete.
4. Select the Delete option.
5. Click OK
Edit a Report

The Web Portal provides the basic reports you need in order to understand your operations. You can, however, edit a report by selecting an existing report and modifying the parameters that define it. Parameters enable you to control the type and amount of information displayed in your report and the way in which it is presented.

Note When editing a report, you cannot change the type of resource, for example from dialed number to call type, used in the report.

To display the Reports section, click the name of the report in your homepage. The View Report page will be displayed.
Alternatively, click Tools. The Tools page will be displayed. Click View Reports. The View Reports page will be displayed.

Note The Tools page can only be accessed by users who have been granted Advanced Mode status. See the User Settings topic.

To edit a report:

1. Click the name of the report in your homepage. The View Reports page will be displayed
2. Click Edit. The Edit Report Details page will be displayed
3. In the Name field enter a new name for the report
4. In the Sub Title field enter a simple question which reflects the report contents and which is used as the displayed title for the report, such as How many calls are queued?
5. In the Description field enter any explanatory text, if required
6. Click the Enabled checkbox to ensure that the report is available to system users
7. Click the Hidden checkbox to prevent users from accessing it
8. Click Save to apply the new parameters

In the Toolbar, a number of options are available:

- **Thresholds** For further information about applying threshold values to report data, see the Set Report Exception Thresholds topic
- **Move** Click to display the report tree and select a folder to relocate the report to. For further information see the Manage Reports topic

Set Report Exception Thresholds

Reports may contain many hundreds, even thousands of rows. Most of the data displayed in those rows reflects normal operational conditions and would fall within acceptable limits. Exception thresholds enable you to set conditions on the data displayed in the report. Any data value which fails those conditions can be highlighted, enabling you to quickly identify areas of poor performance.

To create or edit a report exception threshold
1. Click the name of the report in your homepage
2. Click **Thresholds**. The **Set Threshold** page will be displayed
3. Select a threshold to edit
4. Then perform the following:
   - In the **Name** field enter the name to identify the threshold value
   - From the **Relation** drop down list, select one of the following:
     1. = (equals)
     2. <>(does not equal)
     3. IIN (If In)
     Then enter the value in the field provided.
     If however, you selected the IIN option, two value fields will be displayed. Enter the lowest and highest value, or a comma-separated list of values to match.
   - Select the **Back color**, **Font color** and **Font size** from the relevant drop down lists. Then select the radio buttons of the font attributes; **Bold**, **Italic** or **Underlined**.
5. Click **OK**.
6. SYSTEM MANAGER

Manage the System

Note When the term ‘IPCC’ is used in this chapter, it refers to both Hosted and Enterprise editions

Page Access and Use

Use the Systems Management tool page to create resource folders and resources.

To display the System Manager section, click Tools then click the System Manager header and the System Manager tools page will be displayed.

Tip Alternatively, if you use the System Manager tool regularly you may wish to make it your default page. To do this:
1. Click Settings and the Settings page will be displayed
2. Click User Settings
3. Select System Manager from the Default Homepage drop-down list
4. Click OK
5. Click Home. The System Manager will be displayed as your homepage

Note The Tools page can only be accessed by users who have been granted Advanced Mode status. See the User Settings topic.

Using Portal With Other Provisioning Systems

The Management Portal can be used alongside other provisioning systems, such as the Hosted Unified Communication System (HUCS), but should not be used to provision resources normally provisioned by the alternate system, as these resources may be deleted.

What are Resources?

Resources are the entities in the system which reports display data about. Each tenant in the system has resources assigned to them, such as dialed numbers, agents and so on. These resources are used on a daily basis as a part of contact center network operations. Reports show you how these resources are used. However it is important to differentiate between the types of resources used by the system. There are two different types:

- **System Items** (users, folders and so on) are entities which can be created and managed in the system. For further information see the resource links below
- **Resource Items** (agents, dialed numbers and so on)

The system resources you can create and manage are:
- **Folder** The placeholders in the system for related information. For further information see the Manage Folders topic
- **Group** The contact center team members who are permitted to access the Portal. For further information see the Manage Groups topic
- **Information Notice** A means of displaying information to all users. For further information see the Manage Information Notices topic.
- **Report Parameter Set** The means by which contact center data is organized and displayed. For further information see the Manage Reports topic.
- **User** The contact center members who are permitted to access the Portal. For further information see the Manage Users topic.

The resource items you can create and manage are:

- **Person** The representation of a physical person on the system. A person can be a user and/or one or more agents. For further information see the Manage Persons topic.
- **Agent** A person who handles customer contacts. For further information see the Manage Agents topic.
- **Agent Desktop** A set of permissions or settings for a particular agent, such as how much time is allocated to wrap-up and what outbound calls can be made. For further information see the Manage Agent Desktops topic.
- **Agent Team** A group of agents, managed by one or more supervisors. For further information see the Manage Agent Teams topic.
- **Skill Group** A collection of agents with the same skills and assigned to a single media routing domain. For further information see the Manage Skill Groups topic.
- **Enterprise Skill Group** A logical grouping of skill groups. These may be from different media routing domains. For further information see the Manage Enterprise Skill Groups topic.
- **Call Type** A category of incoming routable task. The call type determines the routing script that is run for the call. For further information see the Manage Call Types topic.
- **Dialed Number** The number dialed by the caller. This helps to determine the call type. For further information see the Manage Dialed Numbers topic.
- **Label** A string that is passed to a routing client for each network target. For further information see the Manage Labels topic.
- **IP Phone** An IP device with a single line used by an agent to make and receive calls. For further information see the Manage IP Phones topic.
- **Directory Number** The line connected to an IP Phone. For further information see the Manage Directory Numbers topic.
- **Printer** For further information see the Manage Printers topic.
- **User Variable**: A named object that holds a value - often used in routing scripts. For further information see the Manage User Variables topic.

- **VRU Script**: A script used by the voice response unit to play a message at the caller. For further information see the Manage VRU Scripts topic.

**Note**: You cannot provision a VRU Script through the Management Portal, you may only change its associated audio file.

**Note**: You may also view the details of items provisioned through IPCC, such as Media Routing Domain or Script, but you will not be able to edit these.

### What is the System Manager tool?

The System Manager tool allows the user to partition their resources in a hierarchical structure. This is achieved by the use of a folder tree located at the left hand side of the tool. The user may view the subfolders of specific folders by selecting them. Users with sufficient security privileges can access and manage the entire contents of the system via the System Manager interface. The Web Administration Portal lets you remotely configure and administer key aspects of your IPCC system including:

- Agents, agent teams, skill groups and desktop settings
- Dialed numbers and call types

**Note**: You cannot manage security in the System Manager. See the Manage Security topic for details of how to manage security in the Management Portal.

The System Manager tool consists of the following panels:

- The **standard toolbar, breadcrumb trail** (which shows the path by which the user accessed the current page) and **Information Management** panels are displayed at the top of the browser.

- The **Folder Tree** panel is displayed on the left of the browser. The folder structure partitions all the resources the user is allowed to see based on their security rights (for further information see the Tree Structures topic). Selecting a folder allows you to see its contents in the Items panel. There is a minimize arrow located on the right edge of this panel to give the user more screen space if the folder tree is not required.

- The **Items** panel is displayed in the middle of the browser. This panel is closed by default - click on the right-hand arrow, or select a folder to view, to open it. The Items panel shows the items contained in the currently selected folder. Selecting a type of resource displays a list of items of that resource type in the currently selected folder. Selecting a particular item allows you to see its contents in the Details panel. There is a minimize arrow located on the right edge of this panel to give the user more screen space if the resource items list is not required.
Note Not all of the item types displayed can be provisioned or edited through the Portal

- The Details panel is displayed on the right hand side of the browser. This panel displays the details of the resource item currently selected in the Items panel. If you have sufficient security permissions, you may be able to edit these.

Anchor Resources

If a tab is selected in the right-hand Details panel, then when the selected item is changed in the center Items panel the view is anchored by the Details panel so that the same tab will be viewed for the new item.

The reverse is also true: if you select an associated resource that is shown in the Details panel (for example, a skill group would be an associated resource shown for an Agent), the type of resources shown in the Items panel will also change.

Tree Structures

The tree structure is organized into folders and tenant folders, which contain all the information relevant to reporting: the resources (such as dialed numbers) whose data is used in reports, the customers who own those resources and system security; the system users and user groups who provide customer service, their assigned user or group rights, called roles, and the system functions, or tasks which comprise them.
Organizing the tree contents

All the information relevant to the system is organized into tenant and resource folders. Each customer in the system is represented by a unique tenant folder and each system resource (dialed numbers, IVR scripts, and so on) owned by that customer are contained in related resource folders.

Note
It is possible to have many layers of tenant and resource folders. For example, tenant folders can be created and linked as a child tenant folder to a parent tenant folder higher in the tree structure.

System security is based on the permissions that users have on these folders and the items within them. Security roles define how the user may access the customer and resource information in the system (a user may not even be permitted to see information that is not relevant to them), for example you may be allowed to run a report, but not change or delete it.

More information on security is available in the Security Management section.

Navigating the Folder Tree

Tree structures can be expanded and contracted using the + (plus) and - (minus) icons displayed next to a folder. Folders are organized into a parent and child structure. Any folder with the + icon displayed next to it is a parent folder, which contains related subfolders or child folders. Click on the + icon to expand the tree and display the list of child folders contained in the parent folder. Similarly, click the - icon to collapse the tree and hide child folders.

Managing the Tree

If a user has access rights to a larger number of customers than can be displayed, the tree displays a restricted number of customers only. The tree display will include a select box. Customers are displayed alphabetically and split onto separate pages, so to find a customer that is not displayed on the current page browse through the pages until the required customer page is located.

Note
The tree contains the entire contents of the system, but will only display the folders and tenants that are relevant to you as defined by your security (login) credentials.

Resource Folder Tree Panel

Panel Access and Use

This panel is displayed at the left of the browser and shows the user of the System Management tool the hierarchical partitioning structure typically setup by the tenant administrator. The user may select one folder at a time and view the items inside. The folder tree can be minimized using the arrow at the top right.
What is a Resource Folder?

Users, customers and resources are contained in folders, which are organized into a tree hierarchy. The tree is organized into a standard, familiar structure with the root folder at the top of the tree; this is usually the service provider. Beneath the root folder, customers, their resources and the users who can access them are organized into parent/child folders. Folder management is accessed via the System Manager section. Each customer in the system is represented by a unique tenant folder and each system resource (dialed numbers, agent teams and so on) owned by that customer are contained in related resource folders.

Note

- It is possible to have many layers of resource folders
- Limiting the number of resource items of a given type in any resource folder to under 1000 assists in system management

There are several types of folder:

- *Unallocated* system folder. This is a single system folder that contains all the resources that are not allocated to a tenant or shared across all tenants. It may only be accessed by the host Administrator
- *Shared* system folder. This is a single system folder that contains resources that may be shared across tenants. It may only be accessed by the host Administrator.
- *Tenant* folder. There is one folder per tenant recorded in the system and each is normally created by the host Administrator

How to Create a Resource Folder

To create a folder:

1. Select the position in the folder tree where you wish the new folder to be added (for example, the tree root folder or within a customer folder).
2. In the Items panel, select **New ▼ > System Item > Folder**
3. The **Create a new Folder** page will be displayed

Alternatively, click **Tools**. The **Tools** page will be displayed. Click **Create a Folder**. The **Create a new folder** page will be displayed.

**Caution** It is not possible to modify a folder once it has been created, therefore choose the information to be entered into the following fields with care:

- In the **Name** field enter a name for the new folder
- In the **Description** field enter any explanatory text for the folder, if required
- Click **Save** to save the new folder in the tree
- Select the **Create Another** checkbox if you wish to create further folders to be placed into the tree structure at the same level
Note A folder inherits the security properties of the parent folder. Tenant folders stand alone and do not inherit any security permissions from a parent folder.

How to Bulk Create Folders
In addition to creating folders one at a time, you can also bulk load user variable records previously output to a CSV (comma separated values) file. See the Bulk Upload section for further information.

How to Delete a Resource Folder
To delete a folder:
1. Move all the resources in the folder and child folders to a different folder, or delete them
2. In the resource items list panel, select the checkbox of the folder to be deleted
3. Click the Delete button. The folder and its subfolders will be removed from the tree

How to Move a Resource Folder
To move a folder:
1. In the Items panel, select the checkbox of the folder to be moved
2. Click the Move button
3. The Move the current items page will be displayed, showing the folder tree
4. Select the folder location in the tree that you wish to move the selected folder to. Click OK

Items Panel

Panel Access and Use
The Items panel is designed to show the items contained in the folder selected in the Folder Tree panel. It has its own tool bar containing New, Upload, Move and Delete buttons that represent operations that can be performed within that selected folder. From the displayed list, you can perform various actions on the item, such as edit, move or copy. The actions that can be performed depend upon the item selected.

Note the Items panel is closed by default when the System Manager is opened.

List Resource Items
To list resource items:
1. From the left hand Folder Tree panel select a folder using a left mouse click. If the middle Items panel is minimized then it will automatically be opened by this action. A list of summary totals of the resources available in this folder will be displayed
2. In the Items panel, click on the type of resource you wish to view

**Note** You can return from viewing a particular item type to viewing the summary list of resources by clicking on the folder in the left hand Folder Tree panel again.

**Note** The paging of the resources is an essential feature since the folder may contain many thousands of items. An attempt to list this many items would cause the browser great difficulties, perhaps even causing it to crash.

**Tip** The list of paged resource items may further be refined by using the Find facility. If the user enters text into the Find box and presses Find then the returned list shows only those resources that contain that text.

By default items are identified by their user-entered names, but the drop-down Display field allows you to view the unique Enterprise Names of items instead.

**Select a Resource Item**

Resource items are selected in two different ways for two different purposes.

To select one or more resource items to move or delete, click on the checkboxes to the left of the items. You can select or deselect the entire list by clicking on the checkbox above the list.

To view or edit the properties of a single resource item, click on the representative icon (such as a head-and-shoulders shape for an agent) to the left of the item. The properties will be shown in the Details panel.

**Create a Resource Item**

To create a new resource item:

1. On the Items panel, hover your mouse pointer over the down arrow ▼ beside the New option. Select the correct category of item (choose between system items such as folders and groups, and resource items such as agents), and select the correct resource

2. A new page will be displayed. The contents of this page depend on the resource that is being created. Fill in the details and press **OK** to confirm or **Back** to cancel the operation

3. You will be returned to the System Manager and the new resource item will appear in the resource item list

**Tip** You can create a resource item of the same type as those you are currently viewing by simply clicking the New button.

**Move Resource Item(s)**

To move a resource item(s)

1. On the resource items list select one or more resource entries checkboxes

2. Click the **Move** toolbar button and the right hand panel will display a confirmation dialog
3. Press the **OK** button to cause the Web Portal to begin the move operation

**Delete Resource Items**

To delete a resource item(s)

1. On the resource items list select one or more resource entries checkboxes
2. Click the **Delete** toolbar button and a confirmation dialog will be displayed
3. Press the **OK** button to cause the Web Portal to begin the delete operation

**Details Panel**

**Page Access and Use**

Use the resource items page to enter or change the details and associations of the selected resource type, such as agent.

To create a new resource item from the Web Administration menu select **System Manager > Resource Folder > Resource Item > New > <resource type>**

To edit an existing resource item from the Web Administration menu select **System Manager > Resource Folder**. Right click on the folder to choose a type of resource, then click on the properties icon of the desired resource item.

The user is presented with a tabbed dialog, each tab representing an operation to be performed.

**Details Tab**

The details tab is a form which contains a series of fields for information that belong to the resource, such as **First Name** in the case of an **Agent**. Each field may be either mandatory, optional or read-only (that is, the Portal fills it in automatically). Each field has a help text item to guide the user on its use and an indication as to whether it is mandatory or not.

**Associations Tab**

Depending on the type of resource there may be one or more association tabs that allow the user to associate other resources with this resource. For example, if a skill group has been selected then there will be an Agents tab to allow the user to specify which agents are to be associated with this skill group.

**Tip** The associations are normally symmetrical in that they can modified from each "side" of the association, so for example to add an agent to a skill group you can either select the skill group and use its agents tab or select the agent and use its skill group tab.
Each association tab has two sub-panels, one above the other. The top sub-panel shows the resource items that are already associated with this resource, the bottom sub-panel shows the available resources that may be added. The contents of this available items sub-panel is filtered by the logged in user's security privileges and any other pertinent business rule. For example, if adding agents to a skill group then the sub-panel will only show those agents who are on the same peripheral as the skill group. The user may move resource items between the top and bottom sub panels in order to get the required associations.

**Advanced Tab**

Depending on the type of resource there may also be an advanced tab. This shows information that is normally set by the system but may be overridden by the user.

**History Tab**

The history tab shows audit information for the resource. If you scroll your mouse pointer over the events listed you will find that some are links. Click on these to open up a table showing details of that particular change. Also, next to some of the events is a details icon which can be clicked to switch to viewing the other item associated with that event.

If the audit history for a resource is long, you can use the Edit Filter link to show only certain events, such as unsuccessful change attempts.

**Resource States**

Each resource in the Management Portal can be in one of five states that indicate its stage in the resource life cycle.

When a resource is first provisioned through the Web Server its state is set to **Pending Active** (sometimes shortened to just **Pending**). This indicates that while it has been provisioned successfully within the Portal, it has not yet been fully provisioned within IPCC. A resource can be deleted while it is in this state.

When a resource has been successfully provisioned within IPCC its state will be set to **Ready**. A resource will normally remain in this state until it is deleted.

Where the resource is unable to be provisioned, it will enter the **Error** state. You can attempt to fix this either by editing the item, in which case its state will become **Pending Active** again, or you can delete it, in which case it will be set to **Awaiting Deletion** (or **Delete Pending**).

When you delete a resource through the Web Server (or when the Portal automatically deletes a resource that has reached its **Active to date**) it enters the **Awaiting Deletion** state, which means that it has been successfully marked as deleted within the Management Portal but has not yet been deleted from IPCC.
Once the resource has been successfully deleted from IPCC it enters the state **Deleted**. Resources are never actually deleted from the Management Portal, only set to the state **Deleted**, as their histories are kept for audit reporting purposes.

**Uploading Resources**

The bulk upload tool is used to import hundreds of resource items into the Unified Contact Center Management Portal. It is used to generate resources such as Agents or Skill Groups by filling in resource attributes using the standard CSV format.

All CSV files require headers that dictate where each value goes. To facilitate this the Portal uses templates. Templates are a CSV file with all the headers set up. There is a Template for every resource type; for example, one for Agents, one for Skill Groups, and so on.

**Note:** Templates do not indicate the value type allowed in the field, such as numeric vs alphanumeric values.

**Editing CSV files**

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

**Note:** There are some 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 section.

**Global Template Columns**

These columns are common to every template file.

The **Required?** column in the tables below tells you whether 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.

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
</table>


<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>Path</td>
<td>No</td>
<td>Describes where in the tree the resource will be created. If you wish to supply the path in the bulk upload screen, you must remove this column.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note</strong>: 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.</td>
</tr>
<tr>
<td>Name</td>
<td>SNC</td>
<td>Yes*</td>
<td>The name of the resource in the Portal. This must be a unique name, and will not be provisioned.</td>
</tr>
<tr>
<td>Description</td>
<td>-</td>
<td>Yes</td>
<td>Describes the dimension being created. This is never provisioned.</td>
</tr>
<tr>
<td>Enterprise Name</td>
<td>SNC</td>
<td>Yes*</td>
<td>The name for the resource being created. This field is provisioned and cannot be omitted. If you leave it blank an Enterprise name is generated for you.</td>
</tr>
<tr>
<td>Effective From</td>
<td></td>
<td>No*</td>
<td>The date from which the resource is active. The default is the current date.</td>
</tr>
<tr>
<td>Effective To</td>
<td>Date</td>
<td>No*</td>
<td>The date on which the resource becomes inactive. The default is forever.</td>
</tr>
</tbody>
</table>

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.

Person Template

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>SNC</td>
<td>Yes*</td>
<td>The first name of the person.</td>
</tr>
<tr>
<td>Last Name</td>
<td>SNC</td>
<td>Yes*</td>
<td>The last name of the person.</td>
</tr>
<tr>
<td>Login Name</td>
<td>SNC</td>
<td>Yes*</td>
<td>The peripheral login name for the person.</td>
</tr>
<tr>
<td>Pass Phrase</td>
<td>Password</td>
<td>Yes</td>
<td>The peripheral login password for the person.</td>
</tr>
</tbody>
</table>
### Agent Template

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peripheral Member</td>
<td>Enterprise Name</td>
<td>Yes*</td>
<td>The Peripheral to assign this Agent to.</td>
</tr>
<tr>
<td>Agent Desktop Member</td>
<td>Enterprise Name</td>
<td>No*</td>
<td>The Desktop this Agent will use.</td>
</tr>
<tr>
<td>Person Member</td>
<td>Enterprise Name</td>
<td>Yes</td>
<td>The Person that this Agent represents.</td>
</tr>
<tr>
<td>Agent Team Member</td>
<td>Enterprise Name</td>
<td>No</td>
<td>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.</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Boolean</td>
<td>No</td>
<td>Indicates whether the agent is a supervisor. This will not create a Portal user, as this is a future feature, however it enables you to bind this agent to a domain login name.</td>
</tr>
<tr>
<td>Peripheral Number</td>
<td>Numeric</td>
<td>Yes*</td>
<td>The service number as known at the peripheral.</td>
</tr>
<tr>
<td>Agent State Trace</td>
<td>Y/N</td>
<td>No</td>
<td>Indicates whether the software collects agent state trace data for the agent.</td>
</tr>
<tr>
<td>Domain Login</td>
<td>NETBIOS login name</td>
<td>If Agent is a supervisor</td>
<td>The login name for the domain user this Agent is associated with. This will often be of the form <code>&lt;domain&gt;&lt;username&gt;</code></td>
</tr>
<tr>
<td>Domain User Name</td>
<td>NETBIOS username</td>
<td>If Agent is a supervisor</td>
<td>The username of the domain user this Agent is associated with.</td>
</tr>
</tbody>
</table>

### Folders Template

**Note** Folders do not use the Enterprise Name, Effective To or Effective From global columns
### Security

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security CSS</td>
<td>CSS Styled List</td>
<td>No</td>
<td>Allows you to set security on the folder you upload. To see an example, see the Agent Security Field Example.</td>
</tr>
</tbody>
</table>

### Agent Desktop Template

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrap up Data Incoming Mode</td>
<td>Numeric</td>
<td>Yes*</td>
<td>Indicates whether the agent is allowed or required to enter wrap-up data after an inbound call. 0 = Required, 1 = Optional, 2 = Not allowed</td>
</tr>
<tr>
<td>Wrap up Data Outgoing Mode</td>
<td>Numeric</td>
<td>Yes*</td>
<td>Indicates whether the agent is allowed or required to enter wrap-up data after an outbound call. 0 = Required, 1 = Optional, 2 = Not allowed</td>
</tr>
<tr>
<td>Wrap up time</td>
<td>Numeric</td>
<td>Yes*</td>
<td>The amount of time in seconds (1-7200) allocated to an agent to wrap up the call</td>
</tr>
<tr>
<td>Remote Agent Type</td>
<td>Numeric</td>
<td>Yes*</td>
<td>Indicates how mobile agents are handled. 0 = No remote access, 1 = Use call by call routing, 2 = Use nailed connection, 3 = Agent chooses routing at login</td>
</tr>
</tbody>
</table>

### Agent Team Template

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Data Type</th>
<th>Required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peripheral Member Name</td>
<td>Enterprise Name</td>
<td>Yes*</td>
<td>The Peripheral to assign this Agent team to.</td>
</tr>
<tr>
<td>Dialed Number Name</td>
<td>Enterprise Name</td>
<td>No</td>
<td>The dialed number to use for this Agent team.</td>
</tr>
<tr>
<td>Column Name</td>
<td>Data Type</td>
<td>Required?</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Peripheral Member</td>
<td>Enterprise Name</td>
<td>Yes*</td>
<td>The Peripheral to assign this Skill Group to.</td>
</tr>
<tr>
<td>Peripheral Number</td>
<td>Numeric</td>
<td>Yes*</td>
<td>The service number as known at the peripheral.</td>
</tr>
<tr>
<td>Peripheral Name</td>
<td>SNC</td>
<td>No*</td>
<td>The name of the Peripheral as it is known on the site.</td>
</tr>
<tr>
<td>Available Hold-Off</td>
<td>Numeric</td>
<td>No</td>
<td>The value for this Skill Group instead of using the one associated with this peripheral.</td>
</tr>
<tr>
<td>Hold-Off Delay</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority</td>
<td>Numeric</td>
<td>No</td>
<td>The routing priority of this group for the skill. This should be set to 0.</td>
</tr>
<tr>
<td>Extension</td>
<td>Numeric</td>
<td>No*</td>
<td>The extension number for the service (used by Lucent DEFINITY ECS).</td>
</tr>
<tr>
<td>IPTA</td>
<td>Y/N</td>
<td>No</td>
<td>Indicates whether the ICM picks the agent.</td>
</tr>
<tr>
<td>Service Level Threshold</td>
<td>Numeric</td>
<td>No</td>
<td>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.</td>
</tr>
<tr>
<td>Service Level Type</td>
<td>Numeric</td>
<td>No</td>
<td>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.</td>
</tr>
<tr>
<td>Default Entry</td>
<td>Numeric</td>
<td>No</td>
<td>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.</td>
</tr>
</tbody>
</table>
Using the Bulk Upload Tool

To use the bulk upload tool

1. Open the System Management page
2. Select the required tenant
3. 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.

4. Select a template for your chosen resource. 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
5. Open the template in the editor you require (such as Notepad) and begin to enter your data or paste it from another source
6. Return to the Bulk Upload Control page and make sure the path is set correctly.
7. Browse to the CSV file you have just entered the data into
8. Click Upload

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

**Caution:** 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 section.

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 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 onto IPCC, only the result of uploading the items into the Unified Contact Center Management Portal.

**Data Types**

The following data types are used:
- **SNC** means Standard Naming Convention and is the same as the UI allows in the name fields on the provisioning pages. That is, alphanumeric characters, no exclamation mark or hyphens, and so on.

- **BOOLEAN** means one of the following values:
  - TRUE
  - FALSE
  - Empty field. Leaving these fields empty defaults the field to FALSE

- **Y/N** is similar to Boolean however it can only contain the values Y or N

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

- A hyphen (-) indicates that there are no constraints on what can be entered in the field (except for the constraints imposed by the native CSV format)

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,PeripheralNumber,BadAgent,imported agent

**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>[:<MultipleRoles>]
```

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

- A single user with a single role
  - Administrator:Tenant User

- A single user with more than one role
  - Administrator:Tenant User:Tenant Supervisor

- 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.

**Reasons for Upload Failure**

The table below details some reasons why an upload might fail.
<table>
<thead>
<tr>
<th>Exception Type</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Capacity Left</td>
<td>The capacity limit has been reached.</td>
</tr>
<tr>
<td>Enterprise Name Already Exists</td>
<td>The enterprise name already exists.</td>
</tr>
<tr>
<td>Login Name Already Exists</td>
<td>The peripheral login name already exists.</td>
</tr>
<tr>
<td>SQL Exception</td>
<td>SQL error during upload, usually due to bad data.</td>
</tr>
<tr>
<td>Argument Exception</td>
<td>An attribute contains a bad value. This usually occurs when you have an empty string in the Path column when attempting to upload items which cannot be contained in the Root folder.</td>
</tr>
<tr>
<td>Security Exception</td>
<td>You do not have security permissions to upload to the folder.</td>
</tr>
<tr>
<td>Format Exception</td>
<td>Invalid data in a column.</td>
</tr>
<tr>
<td>No Identity Available</td>
<td>Identity not available.</td>
</tr>
</tbody>
</table>

## Agent Management

### Manage Persons

#### Page Access and Use

Use the Persons page to create, edit, and delete individual persons, and to define their access to the Management Portal (if any) and their associated agents. To open the page, from the Web Administration menu, select System Manager > Resource Folder > New ▼> Resource Item > Agent.

#### What is a Person?

Each person item represents a single physical person who handles customer contacts or uses the Management Portal. This person may be associated with a user account on the Management Portal, or with one or more Agents.

**Note** To associate a person with more than one Agent, each Agent must be on a different peripheral.

#### How to Create a Person

To create a person:

1. On the Items panel, click New ▼> Resource Item > Person
2. Enter a first name, last name, login name and password for the person. They will use the details specified in the Peripheral Login box to log on to their Agent Desk Setting. Names can be
up to 24 characters long, and must consist of letters, numbers, underscores and periods only

Note The peripheral login details cannot be edited once the agent has been created.

3. Complete fields as described in the Persons fields table below. Active from and to dates can be set in the Advanced tab

4. If the person is to have a Portal account, fill in the fields in the Portal tab

5. Click Save

Note Once created, a Person’s Portal Account details cannot be edited via the agent. You must edit the user directly

How to Bulk Create Persons

In addition to creating persons one at a time, you can also bulk load person records previously output to a CSV (comma separated values) file. See the Uploading Resources section for further information.

How to Delete a Person

To delete one or more persons:

1. On the Items panel, select the person record(s) you want to delete

2. Click Delete

3. A message prompts you to confirm the deletion. Click OK

All agents associated with those persons will also be deleted.

| Person Fields |
|---------------|-----------------|----------------|---------|-----------------
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details Tab</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Name</td>
<td>The person's first name.</td>
<td>Up to 24 characters.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Last Name</td>
<td>The person's last name.</td>
<td>Up to 24 characters.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the person.</td>
<td>Up to 255 characters.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Required</td>
<td>Default</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>---------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Login Name</td>
<td>A unique login name for the person to allow them to login to the peripheral. <strong>Note:</strong> The IPCC database is case-insensitive in determining whether a login name is unique - for example, it considers &quot;joe_smith&quot; and &quot;JOE_SMITH&quot; to be the same. Further, agent login to agent desktop software (such as CTI OS) is not case-sensitive.</td>
<td></td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Password</td>
<td>The password that the person will use to log in to the system. Unique. At least five letters long. Longer passwords, including numbers and other characters, may be required. Ask your system administrator for details.</td>
<td></td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The same as for the Password field. This ensures that the person is not prevented from logging in by typographical errors made when setting his or her password.</td>
<td></td>
<td>Null</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| Portal Tab        | **Create Account**
Check this box to create a basic Portal user account for this person. It is advantageous for supervisors to have a Portal account in order to manage their teams.                                                                 | Checkbox | Unchecked | No                                         |
<table>
<thead>
<tr>
<th>Login Name</th>
<th>The unique name of the Portal user account. This can be the same as the login name for WebView reporting, or that for the peripheral.</th>
<th>Unique. Up to 24 characters, letters, numbers, and underscore characters only. Must begin with letter or number.</th>
<th>Null</th>
<th>If Create Account checked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>The password that the person will use to log in to the system.</td>
<td>Unique. At least five letters long. Longer passwords, including numbers and other characters, may be required. Ask your system administrator for details.</td>
<td>Null</td>
<td>If Create Account checked</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The same as for the Password field. This ensures that the person is not prevented from logging into the Portal by typographical errors made when setting his or her password.</td>
<td></td>
<td>Null</td>
<td>If Create Account checked</td>
</tr>
<tr>
<td>Groups</td>
<td>Allows you to assign the user to one or more security groups, such as the Supervisors group. You can only assign a user to groups you have permission to modify.</td>
<td>Check the boxes of the security groups this user should be a member of.</td>
<td>Unchecked</td>
<td>No</td>
</tr>
</tbody>
</table>

**Advanced Tab**

<table>
<thead>
<tr>
<th>Active From Date</th>
<th>The date from which the person will be active in the system.</th>
<th>Select from calendar.</th>
<th>Current date</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active To Date</td>
<td>The date after which the person should be deleted from the system.</td>
<td>Select from calendar.</td>
<td>Forever</td>
<td>No</td>
</tr>
</tbody>
</table>
Manage Agents

Page Access and Use

Use the Agents page to create, edit, and delete agents and supervisor agents, and to define agent properties such as passwords, voice skill group associations, and desk settings. To open the page, from the Web Administration menu, select System Manager > Resource Folder > New ▼> Resource Item > Agent.

What is an Agent?

An agent is a person who handles customer contacts. In IPCC, each agent can be a member of one or more skill groups. You can group agents into agent teams, which associate each with a specific supervisor or supervisors.

Each agent record must be associated with a Person. During agent creation, you can choose either to associate the agent with an existing person, or to create a new person for that agent. Multiple agents can be associated with a single person, should it be necessary (for example, someone who provides cover for teams on different peripherals will need to be represented by a separate agent account on each peripheral used).

Note In order to use non-voice applications (that is, Cisco Collaboration Server and Cisco E-Mail Manager), agents must be enabled for non-voice use and assigned to non-voice skill groups via the administration interfaces for these multi-channel applications. Thus, while you can create all of your new agent records using the Management Portal, you will need to use the administration interfaces of these non-voice applications to configure agents for their use.

How to Create an Agent

To create an agent:

1. On the Items panel, click New ▼> Resource Item > Agent
2. Enter a first name, and select a peripheral and Person to associate the agent with. You can choose either to associate the agent with an existing Person, or to create a new Person for that agent.
   - Select Existing Person Select a person from the drop-down list, or search for a specific person by typing a part of their name in the Search box. The new agent will use the details specified in that Person’s Peripheral Login box to log on to their Agent Desk Setting.
   - Create New Person Enter the first name and last (or family) name for the person, and fill in the details they will use to login to the peripheral. The person will be automatically created and associated with the agent.

Note Multiple Agents may be associated with a single Person, if all Agents involved are on different peripherals
3. Complete fields as described in the Agents fields table below. Active from and to dates can be set in the Advanced tab
4. Click Save

Once you've created an agent, you can assign that user as the member of an Agent Team, and to one or more Skill Groups.

**What is a Supervisor Agent?**

A supervisor agent is an agent who has a user account on the Portal that allows them to view reports and administer agents and agent teams. While a supervisor agent does not have to be assigned to supervise a specific team, an agent must be a supervisor agent to supervise a team.

A team supervisor may be a primary or secondary supervisor. A team may have any number of secondary supervisors, but only one primary supervisor.

You can define an agent to be a supervisor agent by checking the Supervisor checkbox.

*Note* When an agent is set to be a supervisor agent, then if the associated Person has a Portal user account, that user should be added to the Supervisors security group, which allows users to edit agents and agent teams.

**Adding an Agent to a Team**

You can use the Agent Teams tab to change the team an agent is a member of and, in the case of a supervisor agent, to set the agent as primary or secondary supervisor for one or more teams.

*Note* A supervisor agent does not need to be a member of a team to supervise it.

To Add an agent to a team as either a supervisor or a member:

1. On the Items panel, select the agent record you wish to add to one or (if a supervisor) more teams

2. In the Details panel, click on the Agent Teams tab.

![Agent Teams Tab](image)

Shown in the upper box is a list of teams the agent is currently assigned to, and shown in the lower box is a list of teams available in the current folder. You may see teams in other folders using the Selected Path drop-down folder list. The dates between which
each team is active are displayed, as is the primary supervisor for that team

3. Select teams in the lower box and click on the **Add** button to add the agent to them. They will automatically be moved into the upper box

4. Check the **Member** box if the agent is to be a member of the team. This box should be checked in most cases

**Note** An agent cannot be a member of more than one team, though a supervisor can supervise multiple teams.

5. If the agent is a supervisor agent, you may choose to assign them as a supervisor to that team. Select Primary or Secondary supervisor from the drop-down list. A team can have multiple secondary supervisors but only one primary supervisor

**Note** If you replace an existing primary supervisor, then the replaced supervisor will automatically become a secondary supervisor for that team.

6. You can remove the agent from a team by selecting the team (or teams) in the upper box and clicking on the **Remove** button

7. Click **Save**

**How to Bulk Create Agents**

In addition to creating agents one at a time, you can also bulk load agent records previously output to a CSV (comma separated values) file. See the Uploading Resources section for further information.

**How to Delete an Agent**

To delete one or more agents:

1. On the Items panel, select the agent record(s) you want to delete
2. Click **Delete**
3. A message prompts you to confirm the deletion. Click **OK**

**Note** Deleting an agent or agent supervisor will automatically remove that agent from any associated teams or skill groups, including multi-channel skill groups.

**Note** Deleting an agent or agent supervisor does not delete the associated person.

**Agent Example**

ExampleCorp has ten agents in its New York contact center, and five in San Francisco. These agents are to be divided into three teams.

First, ExampleCorp creates two teams (Green and Blue) in New York, and one (Red) in San Francisco. Then it creates five Persons in San Francisco and ten Persons in New York, creates an Agent associated with each, and adds each Agent to a team.

ExampleCorp wants the two teams in New York to be supervised by the same senior supervisor agent. ExampleCorp therefore edits this agent to make her into a supervisor agent, and adds her as a Primary Supervisor to
both teams. An agent can only be a member of a single team, however, so this supervisor supervises the Blue Team without being a member of it.

The user account of the Person associated with this supervisor agent is added to the ExampleCorp_Supervisors user group.

A primary supervisor is also assigned to the Red Team.

ExampleCorp then assigns secondary supervisors. It decides that the senior supervisor agent in New York should also be a secondary supervisor of the Red Team in San Francisco. Since it is possible to have any number of secondary supervisors for each team, this does not prevent them assigning a San Francisco agent as secondary supervisor to this team as well.

### Agent Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the entry. This may be the same as the login name, last name or first name fields. Your company may specify a convention for this field (such as &lt;first name&gt;_&lt;last name&gt;) to make it easier to identify agents.</td>
<td>Unique. Up to 24 characters, letters, numbers, and underscore characters only. Must begin with letter or number.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the agent.</td>
<td>Up to 255 characters.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Peripheral</td>
<td>The peripheral the agent should be created on. This will affect what teams and skill groups they may be associated with</td>
<td>Select from list</td>
<td>Default peripheral</td>
<td>Yes</td>
</tr>
<tr>
<td>Create New Person</td>
<td>Select this option if the agent record is for a new employee, or one who has not previously existed as a Person within the Management Portal.</td>
<td>Radio button</td>
<td>Checked</td>
<td>If Select Existing Person unchecked</td>
</tr>
<tr>
<td>First Name</td>
<td>The person's first name.</td>
<td>Up to 24 characters.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Last Name</td>
<td>The person's last name.</td>
<td>Up to 24 characters.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Constraints</td>
<td>Nullable</td>
<td>Required</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Login Name</td>
<td>A unique login name for the person to allow them to login to the peripheral.</td>
<td>Note: The IPCC database is case-insensitive in determining whether a login name is unique - for example, it considers &quot;joe_smith&quot; and &quot;JOE_SMITH&quot; to be the same. Further, agent login to agent desktop software (such as CTI OS) is not case-sensitive.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Password</td>
<td>The password that the person will use to log in to the system.</td>
<td>Unique. At least five letters long. Longer passwords, including numbers and other characters, may be required. Ask your system administrator for details.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The same as for the Password field. This ensures that the person is not prevented from logging in by typographical errors made when setting his or her password.</td>
<td>Null</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Select Existing Person</td>
<td>This option is used where the correct person to be associated with this agent record already exists within the system, for example if the Person record for a new employee was created before it was clear which peripheral they would be using. Select the correct person from the drop-down list.</td>
<td>Select from list. Filter list of persons by typing part of the person’s name into the search box.</td>
<td>Unchecked</td>
<td>If Create New Person checked</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>-----------------------------</td>
</tr>
</tbody>
</table>

**Supervisor Tab**

<table>
<thead>
<tr>
<th>Supervisor</th>
<th>Check this box if an agent is to be considered a supervisor. This does not require that they supervise a team.</th>
<th>Checkbox</th>
<th>Unchecked</th>
<th>No</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Associate with Domain Account</th>
<th>Associates a supervisor agent with an existing domain login (the login used to log onto the network and WebView).</th>
<th>Checkbox</th>
<th>Unchecked</th>
<th>If Supervisor box checked</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Login Name</th>
<th>The existing domain login name to be used by the supervisor agent</th>
<th>Existing domain login name. Select from list of possibilities by typing part of the login name.</th>
<th>Null</th>
<th>If Supervisor box checked</th>
</tr>
</thead>
</table>

**Agent Teams Tab**

<table>
<thead>
<tr>
<th>Agent Teams</th>
<th>The supervisory team with which the agent is associated.</th>
<th>Select from list.</th>
<th>Null</th>
<th>No</th>
</tr>
</thead>
</table>

**Skill Groups Tab**
The voice skill group(s) of which the agent is a member. Changes to an agent's skill group membership take place immediately within the agent's current session. Note: Skill groups for non-voice media routing domains (such as e-mail or chat) do not display in the IPCC Web Configuration Tool. To enable an agent for non-voice and assign an agent to a non-voice skill group, you must do it through your multi-channel application administration tool.

Note: You may not add an agent to a skill group if that skill group already has the maximum number of agents associated with it. This maximum number depends on the configuration of your installation of IPCC.

| Skill Group | The voice skill group(s) of which the agent is a member. Changes to an agent's skill group membership take place immediately within the agent's current session. Note: Skill groups for non-voice media routing domains (such as e-mail or chat) do not display in the IPCC Web Configuration Tool. To enable an agent for non-voice and assign an agent to a non-voice skill group, you must do it through your multi-channel application administration tool. Note: You may not add an agent to a skill group if that skill group already has the maximum number of agents associated with it. This maximum number depends on the configuration of your installation of IPCC. | Click Add to select from list. | Null | No |

**Advanced Tab**

<table>
<thead>
<tr>
<th>Enterprise Name</th>
<th>The name used to identify the agent within the system</th>
<th>Unique. Up to 24 characters, letters, numbers, and underscore characters only. Must begin with letter or number.</th>
<th>Auto-generated from the first and last names</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Extension</td>
<td>The internal extension number that can be used to call the agent.</td>
<td>Up to 24 numbers.</td>
<td>Auto-generated</td>
<td>Yes</td>
</tr>
<tr>
<td>Agent Desktop</td>
<td>The desktop settings to be associated with the agent.</td>
<td>Select from list.</td>
<td>None</td>
<td>No</td>
</tr>
</tbody>
</table>
Manage Agent Desktops

Page Access and Use

Use the Desktops page to create, edit, and delete agent desktops (also sometimes called agent desk settings). To open the page, from the Web Administration menu, select System Manager > Resource Folder > New ▼ > Resource Item > Agent Desktop.

What is a Desktop?

Agent Desktops associate a set of permissions or characteristics with specific agents. The settings are comparable to Class of Service settings on a PBX or ACD. You assign desk settings to each agent via the agent record.

When you create a desktop definition, you specify the amount of non-active time after which an agent is automatically logged out, whether wrap up is required following incoming and outbound calls, the amount of time allocated for wrap up, and the method used for assist and emergency calls. You also specify settings for the Re-route on No Answer feature.

IPCC ships with a system default desktop. New agent records are automatically assigned this default unless you specify otherwise when creating an agent.

How to Create a Desktop

To create a Desktop record:
1. On the Items panel, click New > Desktop
2. Enter unique name of up to 24 characters for the record. This name can use alphanumeric characters, periods, and underscores
3. Complete fields as described in the Desktop Fields table below
4. Click Save

How to Delete a Desktop

To delete one or more desktop:
1. On the Items panel, select the desktop record(s) you want to delete

<table>
<thead>
<tr>
<th>State Trace</th>
<th>Enables the system to track the agent's state, such as Logged Off or Talking</th>
<th>Checkbox</th>
<th>Unchecked</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active From Date</td>
<td>The date from which the agent will be active in the system.</td>
<td>Select from calendar.</td>
<td>Current date</td>
<td>Yes</td>
</tr>
<tr>
<td>Active To Date</td>
<td>The date after which the agent should be deleted from the system.</td>
<td>Select from calendar.</td>
<td>Forever</td>
<td>No</td>
</tr>
</tbody>
</table>
**Note** You cannot delete a desktop if it is being referenced by an Agent record or if it is specified as the Default Desktop.

2. Click **Delete**

3. A message prompts you to confirm the deletion. Click **OK**

**How to Bulk Create Agent Desktops**

In addition to creating agent desktop one at a time, you can also bulk load agent desk setting records previously output to a CSV (comma separated values) file. See the Bulk Upload section for further information.

**Desktop Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the record.</td>
<td>Unique. Up to 24 characters, alphanumeric, period, and underscore characters only. Must begin with alphanumeric.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Ring no answer time</td>
<td>The maximum number of seconds IPCC will allow a call to ring at the agent's station before redirecting the call. This can be from 1 to 120 seconds.</td>
<td>1 to 120</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Ring no answer dialed number</td>
<td>Identifies the dialed number for a new re-route destination in the case of a ring no answer. The selection list consists of the dialed numbers configured for the system.</td>
<td>Select from list</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Default</td>
<td>Required</td>
<td>Optional</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>Logout non-activity time</td>
<td>The number of seconds during which the agent has been in the not ready state and inactive that IPCC will wait before logging out the agent. A blank entry will disable the timer.</td>
<td>10 to 7200</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Incoming work mode</td>
<td>Indicates whether the agent is allowed or required to enter work mode after an incoming call.</td>
<td>Select from Required, Optional, Not Allowed, and Required With Wrapup Data.</td>
<td>Optional</td>
<td>Yes</td>
</tr>
<tr>
<td>Outgoing work mode</td>
<td>Indicates whether the agent is allowed or required to enter work mode after an outgoing call.</td>
<td>Select from Required, Optional, and Not Allowed.</td>
<td>Optional</td>
<td>Yes</td>
</tr>
<tr>
<td>Wrap-up time</td>
<td>The amount of time in seconds allocated to an agent to wrap up the call.</td>
<td>1 to 7200</td>
<td>7200</td>
<td>Yes</td>
</tr>
<tr>
<td>Assist call method</td>
<td>Indicates whether IPCC will create a consultative call or a blind conference call for the supervisor assistance request.</td>
<td>Select from consultative call or blind conference call.</td>
<td>Consult</td>
<td>No</td>
</tr>
<tr>
<td>Emergency call method</td>
<td>Indicates whether IPCC will create a consultative call or a blind conference call for an emergency call request.</td>
<td>Select from consultative call or blind conference call.</td>
<td>Consult</td>
<td>No</td>
</tr>
<tr>
<td>Default Device Port Address</td>
<td>Changes the default port for the agent telephone.</td>
<td>Unique. Up to 24 characters, letters, numbers, and underscore characters only. Must begin with letter or number.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>----</td>
</tr>
<tr>
<td>Quality Recording Rate</td>
<td>How frequently calls to the agent are recorded, in seconds.</td>
<td>1-99999</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Recording Mode</td>
<td>Specifies whether calls are routed through the CallManager Peripheral Interface Manager (PIM)</td>
<td>Select from list</td>
<td>Bypass</td>
<td>No</td>
</tr>
<tr>
<td>Remote Agent Type</td>
<td>Indicates how mobile agent call routing is handled.</td>
<td>Select from list</td>
<td>Local Only</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the desktop.</td>
<td>Up to 500 characters.</td>
<td>Null</td>
<td>No</td>
</tr>
</tbody>
</table>

**Miscellaneous**

<table>
<thead>
<tr>
<th>Auto answer</th>
<th>Indicates calls to the agent are automatically answered.</th>
<th>Checked or Unchecked</th>
<th>Unchecked</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle reason required</td>
<td>Indicates the agent must enter a Not Ready reason before entering the Idle state.</td>
<td>Checked or Unchecked</td>
<td>Unchecked</td>
<td>No</td>
</tr>
<tr>
<td>Logout reason required</td>
<td>Indicates the agent must enter a reason before logging out.</td>
<td>Checked or Unchecked</td>
<td>Unchecked</td>
<td>No</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Default</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Auto record on emergency</td>
<td>Specifies that a record request (a request to record the call) is automatically sent when an emergency call request starts.</td>
<td>Checked</td>
<td>Unchecked</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Silent Monitor Audible Indication</td>
<td>Specifies whether to indicate that silent monitoring has begun by a click.</td>
<td>Checked</td>
<td>Unchecked</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Silent Monitor Warning Message</td>
<td>Specifies whether to indicate that silent monitoring has begun with a message box on the agent's desktop.</td>
<td>Checked</td>
<td>Unchecked</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Available after Incoming</td>
<td>Whether the agent is to be automatically considered available after handling an incoming call.</td>
<td>Checked</td>
<td>Unchecked</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Available after Outgoing</td>
<td>Whether the agent is to be automatically considered available after handling an outgoing call.</td>
<td>Checked</td>
<td>Unchecked</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Remote Login Without Desktop</td>
<td>Allows the agent to log in to the contact center without using an agent desktop</td>
<td>Checked</td>
<td>Unchecked</td>
<td>Unchecked</td>
</tr>
</tbody>
</table>

*Outbound Access*
| Outbound Access | For deployments where agents can make outbound calls, determines the type of outbound calls they can make. | Select one or more from International, National, Local private network, Operator assisted, PBX, Agent to Agent, Non ACD Calls, Initiate Supervisor Calls Allowed. | Unchecked | No |

**Agent Tab**

| Agents | The agents with which the desktop is associated. | Select from list. | Null | No |

**Advanced Tab**

<table>
<thead>
<tr>
<th>Enterprise Name</th>
<th>The name used to identify the desktop within the system.</th>
<th>Unique. Up to 24 characters, letters, numbers, and underscore characters only. Must begin with letter or number.</th>
<th>Auto-generated from the name</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active From Date</td>
<td>The date from which the desktop will be active within the system.</td>
<td>Select from calendar.</td>
<td>Current date</td>
<td>Yes</td>
</tr>
<tr>
<td>Active To Date</td>
<td>The date after which the desktop will be deleted from the system.</td>
<td>Uncheck Forever box and select from calendar.</td>
<td>Forever</td>
<td>No</td>
</tr>
</tbody>
</table>

**Manage Agent Teams**

**Page Access and Use**

Use the Agent Teams page to create, edit, and delete agent teams, and to assign agents and supervisors to a team. To open the page, from the Web Administration menu, select **System Manager > Resource Folder > New ▼ > Resource Item > Agent Team.**
What is an Agent Team?
IPCC allows you to group individual agents into agent teams that can be managed by supervisors. Agents are assigned to agent teams individually. When configuring agent teams, be aware of the following rules:

- An agent can be a member of only one agent team (or of no teams)
- An agent team can have only one Primary Supervisor
- A supervisor can be a supervisor of any number of agent teams
- A supervisor for an agent team can also be a member of that agent team

How to Create an Agent Team
To create an agent team:

1. On the Items panel, click **New > Resource Item > Agent Team**
2. Enter a unique name for the team
3. Complete fields as described in the Agent Team Fields table below
4. To assign agents to the team, check the boxes of one or more agents in the **Agents** tab, and click on the **Add** button above the list

**Note** The **Selected Path** drop-down opens up a folder tree so that you can also select agents from other folders to add to the team.

5. Once an agent is added to the team, you must also check their **Member** box to make them a member of the team. This is because it is possible to be involved with a team without being a member, by supervising it

6. If an agent is a supervisor, a drop-down list appears in the right-hand column. You can use this to specify whether the agent has a supervisory role for this particular team

**Note** A team may have multiple secondary supervisors, but only one primary supervisor. If you replace an existing primary supervisor, then the replaced supervisor will automatically become a secondary supervisor for that team.

7. Click **Save**

How to Bulk Create Agent Teams
In addition to creating agent teams one at a time, you can also bulk load agent team records previously output to a CSV (comma separated values) file. See the Uploading Resources section for further information.

How to Edit an Agent Team
To edit an agent team, select the agent team in the Items panel. Click through the tabs and edit the fields you want to change.

To remove agents from a team, click on the agents tab and check the boxes of the agents you wish to remove from the team. Click the **Remove** button.
**How to Delete an Agent Team**

To delete one or more agent teams:

1. On the Items panel, select the agent team record(s) you want to delete
2. Click **Delete**
3. A message prompts you to confirm the deletion. Click **OK**

**Agent Team Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the record.</td>
<td>Unique. Up to 24 characters, alphanumeric, period, and underscore characters only. Must begin with alphanumeric.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the team.</td>
<td>Up to 500 characters.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Supervisor script dialed number</td>
<td>The dialed number identifier for the agent team.</td>
<td>Select from list.</td>
<td>None</td>
<td>No</td>
</tr>
<tr>
<td><strong>Agents Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agents</td>
<td>Individual agents associated with this team.</td>
<td>Select from list.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td><strong>Advanced Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Name</td>
<td>The name that will represent the team within the network</td>
<td>Unique. Up to 24 characters, alphanumeric, period, and underscore characters only. Must begin with alphanumeric.</td>
<td>From Name and Peripheral</td>
<td>Yes</td>
</tr>
<tr>
<td>Peripheral</td>
<td>The peripheral to associate with the team.</td>
<td>Select from list.</td>
<td>Default peripheral</td>
<td>Yes</td>
</tr>
<tr>
<td>Active From Date</td>
<td>The date from which this team must be active within the network</td>
<td>Select from calendar</td>
<td>Current date</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Manage Skill Groups

#### Page Access and Use

Use the Skill Groups page to create, edit, and delete voice skill groups, and to assign agents to these groups. To open the page, from the Web Administration menu, select System Manager > Resource Folder > New ▼ > Resource Item > Skill Group.

#### What is a Skill Group?

A skill group is a collection of agents that share a common set of skills. IPCC agents are assigned one or more skills by associating the agent with the desired skill groups.

**Note** You may not add an agent to a skill group if that skill group already has the maximum number of agents associated with it. This maximum number depends on the configuration of your installation of IPCC.

Each skill group is associated with a specific media routing domain such as voice, chat, or e-mail. In a multichannel deployment (that is, an IPCC deployment that includes non-voice applications like Cisco Collaboration Server or E-Mail Manager), when an agent logs in (via phone, or Collaboration Server, or E-Mail Manager) the agent automatically logs into skill groups associated with that agent within the correct MRD. Then, as a task request for a specific MRD begins script execution, the Agent/IVR Controller considers only the skill groups associated with that specific MRD. This allows one script to be written to handle many MRDs.

**Note** The Management Portal does not support "sub-skill groups" - skill groups defined as a subset of a parent group.

#### How to Create a Skill Group

To create a skill group:

1. On the Items panel, click **New > Resource Item > Skill Group**
2. Enter a unique name for the group
3. Complete fields as described in the Skill Groups Fields table below
4. To assign agents to the team, check the boxes of one or more agents, and click on the **Add** button above the list
5. Click **OK**

<table>
<thead>
<tr>
<th>Active To Date</th>
<th>The date after which this team will be deleted from the system</th>
<th>Uncheck Forever and select from calendar</th>
<th>Forever</th>
<th>No</th>
</tr>
</thead>
</table>
How to Bulk Create Skill Groups
In addition to creating skill groups one at a time, you can also bulk load skill group records previously output to a CSV (comma separated values) file. See the Uploading Resources section for further information.

How to Edit a Skill Group
To edit a skill group, select the skill group in the Items panel. Click through the tabs and edit the fields you want to change.

To remove agents from a skill group, click on the agents tab and check the boxes of the agents you wish to remove from the team. Click the Remove button.

How to Delete a Skill Group
To delete one or more skill groups:
1. On the Items panel, select the skill group record(s) you want to delete
   Note You cannot delete a skill group that is referenced in a script. This reference must be removed before the skill group can be deleted.
2. Click Delete
3. A message prompts you to confirm the deletion. Click OK
   Note Deleting a skill group automatically removes it from any enterprise skill groups in which it is referenced.

Skill Group Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details Tab</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique enterprise name for the record.</td>
<td>Unique. Up to 24 characters, letters, numbers, periods, and underscore characters only. Must begin with letter or number.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the skill group.</td>
<td>Up to 255 characters.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Default</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>Service Level Type</td>
<td>Optionally, use to indicate how abandoned calls should be factored in calculating service levels.</td>
<td>-</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select from Default, Ignore Abandoned Calls, Abandoned Calls Have Negative Impact, and Abandoned Calls Have Positive Impact. Note: &quot;Default&quot; = Ignore Abandoned Calls.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Level Threshold</td>
<td>The threshold, in seconds, for the ICM service level.</td>
<td>1-99999</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Agents</td>
<td>Agents associated with this skill group.</td>
<td>Null</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Advanced Tab</td>
<td>The name that will represent the team within the network</td>
<td>Unique. Up to 24 characters, alphanumeric, period, and underscore characters only. Must begin with alphanumeric.</td>
<td>From Name and Peripheral</td>
<td>Yes</td>
</tr>
<tr>
<td>Peripheral</td>
<td>The peripheral to associate with the skill group</td>
<td>Select from list.</td>
<td>Default peripheral</td>
<td>No</td>
</tr>
<tr>
<td>Peripheral Number</td>
<td>The number to be used on the peripheral for the Skill Group</td>
<td>0-999999999999999999</td>
<td>Generated automatically</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Agents Tab**

**Advanced Tab**
<table>
<thead>
<tr>
<th>Active From Date</th>
<th>The date from which the Skill Group should be active in the system</th>
<th>Select from calendar.</th>
<th>Current date</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active To Date</td>
<td>The date after which the Skill Group should be deleted from the system</td>
<td>Uncheck Forever and select from calendar.</td>
<td>Forever</td>
<td>No</td>
</tr>
</tbody>
</table>

### Manage Enterprise Skill Groups

#### Page Access and Use

Use the Enterprise Skill Groups page to create, edit, and delete enterprise skill groups. To open the page, from the Web Administration menu, select **System Manager > Resource Folder > New ▼ > Resource Item > Enterprise Skill Group.**

**What is an Enterprise Skill Group?**

An Enterprise Skill Group is a logical grouping of skill groups joined together for reporting purposes. Enterprise skill groups can include skill groups from different media routing domains.

***Note*** Unlike the Skill Groups page in IPCC Web Administration that displays only voice skill groups, the Enterprise Skill Groups page displays non-voice skill groups such as chat, multi-session chat, and email.

#### How to Create an Enterprise Skill Group

To create an enterprise skill group:

1. On the Items panel, click **New > Resource Item > Enterprise Skill Group**
2. Enter a unique name for the group
3. Complete fields as described in the Enterprise Skill Group Fields table below
4. To assign skill groups to the group, click the **Add** button below the Skill Groups box and select one or more skill groups

***Note*** The **Selected Path** drop-down at the top allows you to select agents from other folders to add to the team

5. Click **Save**

#### How to Bulk Create Enterprise Skill Groups

In addition to creating enterprise skill groups one at a time, you can also bulk load enterprise skill group records previously output to a CSV (comma separated values) file. See the Uploading Resources section for further information.
How to Delete an Enterprise Skill Group

To delete one or more enterprise skill groups:

1. On the Items panel, select the enterprise skill group record(s) you want to delete
2. Click **Delete**
3. A message prompts you to confirm the deletion. Click **OK**

### Enterprise Skill Group Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the record.</td>
<td>Unique. Up to 24 characters, letters, numbers, periods, and underscore characters only. Must begin with letter or number.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>A description of this enterprise skill group.</td>
<td>Up to 255 characters.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td><strong>Skill Groups Tab</strong></td>
<td>Skill groups associated with this enterprise skill group.</td>
<td>Select from list and click <strong>Add</strong>.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td><strong>Advanced Tab</strong></td>
<td>The name by which the Enterprise Skill Group will be known within the system.</td>
<td>Unique. Up to 24 characters, letters, numbers, periods, and underscore characters only. Must begin with letter or number.</td>
<td>Auto generates</td>
<td>No</td>
</tr>
<tr>
<td>Enterprise Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active From Date</td>
<td>The date from which the Enterprise Skill Group should be active in the system.</td>
<td>Select from calendar.</td>
<td>Current date</td>
<td>No</td>
</tr>
<tr>
<td>Active To Date</td>
<td>The date from which the Enterprise Skill Group should be deleted from the system.</td>
<td>Uncheck <strong>Forever</strong> then select from calendar.</td>
<td>Forever</td>
<td>No</td>
</tr>
</tbody>
</table>
Contact Management

Manage Dialed Numbers

Page Access and Use
Use the Dialed Numbers page to create, edit, and delete dialed numbers and associate them with call types. To open the page, from the Web Administration menu, select System Manager > Resource Folder > New ▼ > Resource Item > Dialed Number.

What is a Dialed Number?
A dialed number (DN) is the number a caller dials to initiate a call. It is sent as part of the call detail information in the route request message sent from the routing client. In IPCC, you set up a Dialed Number List, which identifies all of the phone numbers in your contact center that customers can dial to initiate contact. The Dialed Number plays an integral role in routing calls. Dialed Numbers are required pieces of call types, which are used to identify the appropriate routing script for each call. In addition to answered calls, Dialed Number also need to be set up for ring on no answer, dialed number plan entries, and for supervisor/emergency calls.

How to Create a Dialed Number
To create a dialed number:

1. On the Items panel, click New > Dialed Number
2. Enter unique name of up to 24 characters for the Dialed Number. This must consist of alphanumeric characters, periods, and underscores only
3. Complete fields as described in the Dialed Number Fields table below
4. Click Add to specify the call types and other dialing information to be associated with this dialed number.

Note The order of the entries in the Dialed Number mapping table reflects the order in which call types are processed for the Dialed Number.
5. Click Save

How to Delete a Dialed Number
To delete one or more dialed numbers:

1. On the Items panel, select the Dialed Number record(s) you want to delete

Note You cannot delete a Dialed Number that is referenced in a script. This reference must be removed before the Dialed Number can be deleted.
2. Click Delete
3. A message prompts you to confirm the deletion. Click OK
### Dialed Number Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the record.</td>
<td>Unique. Up to 24 characters, alphanumeric, period, and underscore characters only. Must begin with alphanumeric.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the record.</td>
<td>Up to 255 characters</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Dialed Number</td>
<td>For voice MRD only, the string value by which the Agent/IVR Controller identifies this Dialed Number. This must be the value the Agent/IVR Controller uses for calls to this number. For example: 8005551212</td>
<td>Up to 32 characters</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Routing Client</td>
<td>The routing client (such as NIC or PG) that this number should use to submit routing requests to the ICM</td>
<td>Drop-down list</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Agent Desktops Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Desktops</td>
<td>The Agent Desktops associated with this Dialed Number.</td>
<td>Select from list and click Add.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td><strong>Agent Teams Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Teams</td>
<td>The Agent Teams associated with this Dialed Number.</td>
<td>Select from list and click Add.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td><strong>Labels Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Labels</td>
<td>The Labels associated with this Dialed Number.</td>
<td>Select from list and click Add.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td><strong>Advanced Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active From Date</td>
<td>The date from which the Dialed Number will be active in the system.</td>
<td>Select from calendar.</td>
<td>Current date</td>
<td>Yes</td>
</tr>
<tr>
<td>Active To Date</td>
<td>The date after which the Dialed Number should be deleted from the system.</td>
<td>Uncheck <strong>Forever</strong> then select from calendar.</td>
<td>Forever</td>
<td>No</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>---------</td>
<td>----</td>
</tr>
</tbody>
</table>

Manage Directory Numbers

**Page Access and Use**

Use the Directory Numbers page to create, edit, and delete numbers. To open the page, from the Web Administration menu, select **System Manager > Resource Folder > New ▼ > Resource Item > Directory Number**.

**What is a Directory Number?**

A directory number is an extension line which is attached to an IP Phone.

**How to Create a Directory Number**

To create a Directory Number:

1. On the Items panel, click **New > Resource Items > Directory Number**
2. Select whether the number is IPCC enabled
3. Complete fields as described in the Directory Number Fields table below
4. Click **Save**

**How to Delete a Directory Number**

To delete one or more numbers:

1. On the Items panel, select the number record(s) you want to delete
2. Click **Delete**
3. A message prompts you to confirm the deletion. Click **OK**
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the record.</td>
<td>Unique. Up to 24 characters, alphanumeric, period, and underscore characters only. Must begin with alphanumeric.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>An internal description of the record.</td>
<td>Up to 255 characters.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>IPCC Enabled</td>
<td>Determines whether a Device Target must be created on the ICM for this number.</td>
<td>Checkbox</td>
<td>Unchecked</td>
<td>No</td>
</tr>
<tr>
<td><strong>Advanced Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Manager</td>
<td>The CallManager to be associated with the Directory Number.</td>
<td>Select from the list of CallManagers available for the tenant.</td>
<td>Default CallManager</td>
<td>Yes</td>
</tr>
<tr>
<td>Route Partition</td>
<td>The group of numbers (such as area codes or internal numbers) that this number is to be associated with.</td>
<td>Select from list.</td>
<td>Default Peripheral</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatically Allocate a Number Pattern/Number Pattern</td>
<td>Whether to automatically allocate the number to be used for this Directory Number.</td>
<td>Checkbox. Uncheck box to enter number of 1-20 digits manually in the Number Pattern text box that appears.</td>
<td>Checked</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Active From Date | The date from which the Directory Number will be active in the system. | Select from calendar. | Current date | Yes
---|---|---|---|---
Active To Date | The date after which the Directory Number should be deleted from the system. | Select from calendar. | Forever | No

### Manage Call Types

#### Page Access and Use

Use the Call Types page to create, edit, and delete call types. To open the page, from the Web Administration menu, select System Manager > Resource Folder > New → Resource Item > Call Type.

#### What is a Call Type?

A call type is a category of incoming routable task. Specific call types are associated in IPCC with Dialed Numbers. In this association, each call type has a schedule that determines which routing script or scripts are active for that call type at any time.

**Note** It is not currently possible to associate Dialed Numbers with Call Types in the Management Portal.

There are two classes of call type/dialed number associations:

- **Voice**: Voice call type/dialed number combinations such as phone calls are categorized by the dialed number (DN), caller-entered digits (CED), and calling line ID (CLID). The CED and CLID can be optional, depending on the call.
- **Non-voice**: Non-voice type/dialed number combinations (such as email and text chat) are categorized by the Script Type Selector, Application String 1, and Application String 2. Application String 1 and Application String 2 can be optional, depending on the application.

Because the call type determines which routing script is run for a call, the call type defines call treatment in an IPCC Enterprise system. Therefore, the call type is the highest level reporting entity. Reporting on call type activity provides insight into end-to-end customer interactions with the system and with agents by providing data such as service level adherence, transfers, average speed of answer, calls handled, and calls abandoned.

In routing scripts you can change the call type at specific points in the script to indicate that a transaction has been completed. For example, if the customer is calling a bank and successfully checks his or her account
balance using a Self-Service script, you may want to change the call type to indicate that the account balance transaction has completed and a new transaction has begun. You can also change call type in a script to invoke a new routing script associated with that call type. For example, if a call is not answered at an agent's desktop, you can change the call type in the script to redirect the call to a different script designed for Redirection on No Answer. The Redirection on No Answer script assigns a different agent to handle the call.

**How to Create a Call Type**

To create a call type:

1. On the Items Panel, click **New > Resource Item > Call Type**
2. Enter a unique name of up to 24 characters for the call type. This can contain alphanumeric characters, periods, and underscores only
3. Complete fields as described in the Call Type Fields table below
4. Click **Save**

**Task Result**

Once you have created a call type you can reference it in a dialed number configuration through IPCC.

**How to Delete a Call Type**

To delete one or more call types:

1. On the Items Panel, select the call type record(s) you want to delete
   
   **Note** You cannot delete the default call type
2. Click **Delete**
3. A message prompts you to confirm the deletion. Click **OK**

**Note** Deleting a call type automatically removes it from any dialed number mappings in which it is referenced.

**Call Type Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the record.</td>
<td>Unique. Up to 24 characters, alphanumeric, period, and underscore characters only. Must begin with alphanumeric.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>An internal description of the record.</td>
<td>Up to 255 characters.</td>
<td>Null</td>
<td>No</td>
</tr>
</tbody>
</table>
Service level threshold

Optionally, use to indicate whether this call type will use a service level threshold other than the system default.

Select from Use global setting, None, and Use specified. For Use specified, you must also enter a number in seconds from 0-99999

Use global setting

Service level type

Optionally, use to indicate how abandoned calls should be factored in calculating service levels.

Select from Use global setting, Ignore Abandoned Calls, Abandoned Calls Have Negative Impact, and Abandoned Calls Have Positive Impact.

Use global setting

Advanced Tab

Enterprise Name

The name that will represent the Call Type within the network.

Unique. Up to 24 characters, alphanumeric, period, and underscore characters only. Must begin with alphanumeric.

From Name

Yes

Active From Date

The date from which this Call Type should be active within the system

Select from calendar

Current date

Yes

Active To Date

The date after which this Call Type should be deleted from the system

Uncheck Forever box and select from calendar

Forever

No

Manage Labels

Page Access and Use

Use the Labels page to create, edit, and delete labels. To open the page, from the Web Administration menu, select System Manager > Resource Folder > New ▼ > Resource Item > Label.

What is a Label?

In IPCC the label represents a string that is passed to a routing client for each network target. The Management Portal will automatically create labels for many high level operations but the functionality is included for specific label creation such as blind transfers. The only label type supported will be type Normal, the only network target is device target.
**How to Create a Label**

To create a label:

1. On the Items panel, click *New > Resource Items > Label*

2. Enter a unique name of up to 24 characters for the label. This must contain alphanumeric characters, periods and underscores only.

3. Complete fields as described in the Label Fields table below

4. Click **OK**

**How to Delete a Label**

To delete one or more labels:

1. On the Items panel, select the label record(s) you want to delete. Click **Delete**

2. A message prompts you to confirm the deletion. Click **OK**

**Label Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the record.</td>
<td>Unique. Up to 24 characters, alphanumeric, period, and underscore characters only. Must begin with alphanumeric.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the record.</td>
<td>Up to 255 characters.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Routing Client</td>
<td>The enterprise name of the routing client associated with this label</td>
<td>Select from the supplied list of routing clients that the logged in user has the security privileges to see.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Dialed Numbers Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dialed Numbers</td>
<td>The Dialed Numbers to associate with this label</td>
<td>Select from list and click <strong>Add.</strong></td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td><strong>Advanced Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>The date</td>
<td>Select from calendar</td>
<td>Current</td>
<td>Yes</td>
</tr>
<tr>
<td>From Date</td>
<td>The date from which this label should be active within the system</td>
<td>date</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------</td>
<td>------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active To Date</td>
<td>The date after which this label should be deleted from the system</td>
<td>Uncheck <strong>Forever</strong> box and select from calendar</td>
<td>Forever</td>
<td>No</td>
</tr>
</tbody>
</table>

## Equipment Management

### Manage IP Phones

#### Page Access and Use
Use the IP phones page to create, edit, and delete telephones. To open the page, from the Web Administration menu, select **System Manager > Resource Folder > New ▼ > Resource Item > IP Phone**.

#### Using Portal with Other Provisioning Systems
When using a separate provisioning system to add IP phones to a CallManager, check the IPCC enabled checkbox for all the Directory Numbers provisioned by the external system to ensure that they are added correctly to the ICM. Do not attempt to make any other changes to phones on that CallManager using Portal.

### What is an IP Phone?
A telephone is the IP device that the contact center agent uses to make or receive calls. The telephone has a single line (typically line 1 if using a Cisco multi-line phone), whose number is known to the call routing software. The agent logs into the contact center using the Cisco CTI OS client desktop using the login name and password allocated by the Manage Agent portal page and the line number allocated in this page. Line numbers may be allocated automatically by the Web Portal or entered manually through the user interface.

#### How to Create an IP Phone
To create an IP Phone:

1. On the Items panel, click **New > Resource Items > IP Phone**
2. Select the phone type from the drop down
3. Complete fields as described in the IP Phone Fields table below
4. Optionally add directory numbers by checking the boxes of numbers to add and clicking **Add**
5. Click **Save**
Task Result
Once you have created an IP phone its status will initially be shown as Not Ready. The telephone will not be ready to use until this status changes to Available. This change usually occurs within a few minutes of saving.

How to Delete an IP Phone
To delete one or more telephones:
1. On the Items panel, select the telephone record(s) you want to delete
2. Click Delete
3. A message prompts you to confirm the deletion. Click OK

IP Phone Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details Tab</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the record.</td>
<td>Unique. Up to 24 characters, alphanumeric, period, and underscore characters only. Must begin with alphanumeric.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>An internal description of the record.</td>
<td>Up to 255 characters.</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Type</td>
<td>The model of telephone.</td>
<td>Select from list.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Template / Change Template</td>
<td>The XML template to be used to configure the IP Phone on the CallManager.</td>
<td>Select from list of templates available for the specific phone model. When editing an IP Phone, you must check Change Template to show the Template field.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Button Template</td>
<td>The configuration to use for the buttons on the CallManager</td>
<td>Select from list of button templates set up for the CallManager.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC Address of the IP phone used to uniquely identify it.</td>
<td>12-digit hexadecimal number.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>------</td>
<td>-----</td>
</tr>
</tbody>
</table>

**Directory Numbers Tab**

<table>
<thead>
<tr>
<th>Directory Numbers</th>
<th>The lines to be associated with the IP Phone.</th>
<th>Select from list.</th>
<th>Null</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>The port on the IP Phone that the line is plugged into.</td>
<td>Number.</td>
<td>Null</td>
<td>No</td>
</tr>
</tbody>
</table>

**Advanced Tab**

<table>
<thead>
<tr>
<th>Call Manager</th>
<th>The CallManager to be associated with the IP Phone.</th>
<th>Select from the list of CallManagers available for the tenant.</th>
<th>Default CallManager</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peripheral</td>
<td>The Peripheral to be associated with the IP Phone.</td>
<td>Select from the list of Peripherals associated with the selected CallManager.</td>
<td>Default Peripheral</td>
<td>Yes</td>
</tr>
<tr>
<td>Device Pool</td>
<td>A pool of phones that have similar character.</td>
<td>Select from the list of Device Pools available to the logged in user.</td>
<td>Default Device Pool</td>
<td>No</td>
</tr>
<tr>
<td>Active From Date</td>
<td>The date from which the IP Phone will be active in the system.</td>
<td>Select from calendar.</td>
<td>Current date</td>
<td>Yes</td>
</tr>
<tr>
<td>Active To Date</td>
<td>The date after which the IP Phone should be deleted from the system.</td>
<td>Uncheck <strong>Forever</strong> and select from calendar.</td>
<td>Forever</td>
<td>No</td>
</tr>
</tbody>
</table>

**Advanced Information**

The Web Portal automatically links or adds default additional information to IPCC as follows:

- Links the CallManager *calling search space* from the tenant owning folder
- Links the CallManager *route partition* from the tenant owning folder
- Links the CallManager *owner user ID* from the PG user id allocated to the tenant
- Links the CallManager *location* from the parent folder
- Creates an ICM *device target* for the phone/line.
- Creates an ICM *label* for each combination of *device target* and routing client (to route calls to an IPCC agent, you must have defined a *label* associated with the *device target*).

**Manage Directory Numbers**

**Page Access and Use**

Use the Directory Numbers page to create, edit, and delete numbers. To open the page, from the Tools page, select **System Manager > Resource Folder > New ▼ > Resource Item > Directory Number**.

**What is a Directory Number?**

A directory number is an extension line which is attached to an IP Phone.

**How to Create a Directory Number**

To *create* a Directory Number:
- On the Items panel, click **New > Resource Items > Directory Number**
- Select whether the number is IPCC enabled
- Complete fields as described in the Directory Number Fields table below
- Click **Save**

**How to Delete a Directory Number**

To *delete* one or more numbers:
- On the Items panel, select the number record(s) you want to delete
- Click **Delete**
- A message prompts you to confirm the deletion. Click **OK**

**Directory Number Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the record.</td>
<td>Unique. Up to 24 characters, alphanumeric, period, and underscore characters only. Must begin with alphanumeric.</td>
<td>Null</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Description
An internal description of the record. | Up to 255 characters. | Null | No |

**IPCC Enabled**
Determines whether a Device Target must be created on the ICM for this number. This must be checked for any phones added using a different provisioning system. | Checkbox | Unchecked | No |

#### Advanced Tab

**Call Manager**
The CallManager to be associated with the Directory Number. | Select from the list of CallManagers available for the tenant. | Default CallManager | Yes |

**Route Partition**
The group of numbers (such as area codes or internal numbers) that this number is to be associated with. | Select from list. | Default Peripheral | Yes |

**Automatically Allocate a Number Pattern/Number Pattern**
Whether to automatically allocate the number to be used for this Directory Number. | Checkbox, Uncheck box to enter number of 1-20 digits manually in the *Number Pattern* text box that appears. | Checked | Yes |

**Active From Date**
The date from which the Directory Number will be active in the system. | Select from calendar. | Current date | Yes |

**Active To Date**
The date after which the Directory Number should be deleted from the system. | Select from calendar. | Forever | No |

### Manage Printers
You may add printers to the system. Printers can be selected to be used by members of a specific folder or all folders.
To display the **System Manager** section, click **Tools**. The **Tools** page will be displayed. Click the **System Manager** header. The **System Manager** page will be displayed.

**Note** The **Tools** page can only be accessed by users who have been granted **Advanced Mode** status. See the User Settings topic.

To add a printer to a system folder:

1. Click on **System Manager** to open the System Manager page.
2. Navigate to the folder in the tree to add a printer to.
3. Click **New ▼ > Resource Items > Printer**. The **Create a new Printer Alias** page will be displayed. Then perform the following:
   - In the **Printer Name** field enter a name for the printer
   - In the **Description** field, enter a description for the printer, if required
   - In the **Email** field enter the email address of the mailbox associated with your preferred printer
   - Optionally enter a **Backup Email** address to be used in case the preferred email address is unreachable
   - In the **Subject** field enter the details of the printer parameters
4. Click **Save**.

**Audio Management**

**Manage VRU Scripts**

**Page Access and Use**

The Management Portal allows you to change the audio file associated with a network VRU script.

**Note** You cannot create a new VRU Script through the Management Portal.

To open the page, from the System Manager, navigate to the correct folder in the left-hand panel, choose Network Vru Script from the summary list of items, and select a specific VRU Script from the list shown in the Items panel. This will show you the details of the script.

**What is a Network VRU Script?**

A Network VRU (voice response unit) is a telecommunications computer, also called an Interactive Voice Response (IVR) unit, that responds to caller-entered touch-tone digits. This uses routing scripts to process a call. At various stages, this may run a VRU script to play a message to the caller, such as a repeated announcement when they are in a call queue.

**How to Associate a VRU Script with an Audio File**

To change the audio file associated with a VRU script:
1. On the Items panel, click on a VRU script to associate with an audio file. The details for this script will open in the right-hand Details panel.

2. Select the Audio tab.

   **Note** If no Audio tab is available, this may mean that the Network VRU Script has not been configured correctly. Contact your system administrator.

3. Click Save.

   **Note** The audio file will be saved under the name configured in the VRU script, replacing any previous audio file.

### Code and Variable Management

#### Manage User Variables

**Page Access and Use**

Use the Create a New User Variable page to create and delete user variables. User variables cannot be edited once created. To open the page, from the Web Administration menu, select System Manager > Resource Folder > New ▼> Resource Item > User Variable.

**What is a User Variable**

A user variable is a named object which can hold a value up to 40 characters long. Variables are used in routing scripts.

**How to Create a User Variable**

To create a user variable:


2. Complete fields as described in the User Variable Fields table below. Active from and to dates can be set in the Advanced tab.

   **Note** IPCC requires that all user variable names begin with the string 'user'. The Code Text will therefore automatically be prefixed with this string on saving. For example, if you enter a Code Text of 'Temp', the resulting user variable will be called 'userTemp'.

3. Click Save.

   **Note** User variables cannot be edited after creation.

**How to Bulk Create User Variables**

In addition to creating user variables one at a time, you can also bulk load user variable records previously output to a CSV (comma separated values) file. See the Bulk Upload section for further information.

**How to Delete a User Variable**

To delete one or more user variables:

1. In the Items panel, select the user variable(s) you want to delete.

2. Click Delete.
3. A message prompts you to confirm the deletion. Click **OK**.

### User Variable Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details Tab</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Code Text</td>
<td>The name of the user variable.</td>
<td>Up to 32 characters, consisting of letters, numbers, periods and underscores only. This <strong>does not</strong> need to begin with the string 'user'.</td>
<td>Null</td>
</tr>
<tr>
<td>Object Type</td>
<td>The type of object with which to associate the variable. You may choose not to associate the user variable with an object by selecting User Variable.</td>
<td>Select from list</td>
<td>Null</td>
</tr>
<tr>
<td>Data Type</td>
<td>The data type for the variable.</td>
<td>Select from list</td>
<td>Long</td>
</tr>
<tr>
<td>Persistent</td>
<td>Whether the user variable retains value across Central Controller restarts.</td>
<td>Checkbox.</td>
<td>Checked</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the variable and how it should be used.</td>
<td>Up to 255 characters.</td>
<td>Null</td>
</tr>
<tr>
<td><strong>Advanced Tab</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active From Date</td>
<td>The date from which the variable will be active in the system.</td>
<td>Select from calendar.</td>
<td>Current date</td>
</tr>
<tr>
<td>Active To Date</td>
<td>The date after which the variable should be deleted from the system.</td>
<td>Uncheck <strong>Forever</strong> and select from calendar.</td>
<td>Forever</td>
</tr>
</tbody>
</table>
Manage Expanded Call Variables

Page Access and Use

Use the Create an Expanded Call Variable page to create and delete expanded call (ECC) variables. To open the page, from the Tools page, select System Manager > Resource Folder > New ▼> Resource Item > Expanded Call Variable.

What is an Expanded Call Variable

An expanded call variable is a named object which is used by a VRU script to exchange call information with the ICM.

How to Create an Expanded Call Variable

To create an expanded call variable:

1. On the Items panel, click New ▼> Resource Item > Expanded Call Variable
2. Complete fields as described in the Expanded Call Variable Fields table below. Active from and to dates can be set in the Advanced tab
3. Click Save

How to Delete an Expanded Call Variable

To delete one or more expanded call variables:

1. In the Items panel, select the expanded call variable(s) you want to delete
2. Click Delete
3. A message prompts you to confirm the deletion. Click OK

User Variable Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Entry</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the call variable</td>
<td>Unique. Up to 24 characters, letters, numbers, and underscore characters only. Must begin with letter or number.</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the call variable</td>
<td>Up to 255 characters</td>
<td>Null</td>
<td>No</td>
</tr>
<tr>
<td>Maximum Length</td>
<td>The maximum length of the value of the call variable</td>
<td>Up to 210</td>
<td>Null</td>
<td>Yes</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------------------------</td>
<td>-----------</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>Provided by Cisco</td>
<td>Whether the call variable provided by Cisco. This is normally determined by the system</td>
<td>Checkbox</td>
<td>Unchecked</td>
<td>No</td>
</tr>
<tr>
<td>Persistent</td>
<td>Whether the variable is written to the historical database with the TCD/RCD record</td>
<td>Checkbox</td>
<td>Unchecked</td>
<td>No</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether the call variable is currently enabled</td>
<td>Checkbox</td>
<td>Checked</td>
<td>No</td>
</tr>
<tr>
<td>ECC Array</td>
<td>Whether the variable is an array</td>
<td>Checkbox</td>
<td>Unchecked</td>
<td>No</td>
</tr>
<tr>
<td>Maximum Array Size</td>
<td>The maximum size of elements in the array represented by the call variable</td>
<td>Up to 255. The equation &lt;Maximum Length&gt; * &lt;Maximum Array Size&gt; + &lt;Maximum Array Size&gt; + 5 must not exceed 299. For example, if the Maximum Length was 97, the array size could not exceed 3.</td>
<td>Null</td>
<td>If ECC Array checked</td>
</tr>
</tbody>
</table>
### Advanced Tab

<table>
<thead>
<tr>
<th>Enterprise Name</th>
<th>Description</th>
<th>Unique. Up to 24 characters, letters, numbers, and underscore characters only. Must begin with letter or number.</th>
<th>Created from variable name. Enterprise names for expanded call variables are automatically prefixed with 'user' by the system.</th>
<th>No</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Active From Date</th>
<th>Description</th>
<th>Select from calendar.</th>
<th>Current date</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active To Date</td>
<td>Description</td>
<td>Uncheck <strong>Forever</strong> and select from calendar.</td>
<td>Forever</td>
<td>No</td>
</tr>
</tbody>
</table>

**Notes:**
- **Active From Date**
  - The date from which the variable will be active in the system.
  - Select from calendar.
  - Current date

- **Active To Date**
  - The date after which the variable should be deleted from the system.
  - Uncheck **Forever** and select from calendar.
  - Forever

**User Manual for Cisco Unified Contact Center Management Portal Release 7.2**
7. SECURITY MANAGEMENT

Manage Security

Overview

Security Management allows you to partition (provide access only to certain areas of) the system so that each user may perform specific tasks on specific folders. This involves creating and administrating users and customers, as well as creating the folder and tenant folder tree hierarchy in which these entities and resources are organized. Security Management enables a user with sufficient privileges to create and manage further users who can access the system, to define the groups to which they belong and to assign them the roles that define the system functions they are allowed to perform on each folder.

To display the Security Manager section, click Tools. The Tools page will be displayed. Click the Security Manager header. The Security Manager page will be displayed.

Note If you have sufficient privileges, you may wish to display the Security Manager tool in your homepage. This is done as follows:

1. Click Settings. The Settings page will be displayed
2. Click User Settings
3. Select Security Manager from the Default Homepage drop-down list
4. Click OK. The Security Manager section will be displayed as your homepage

Security Management involves administrating the following entities:

- **User** A person with access to the Portal
- **Group** A collection of users who share the same security permissions. Groups may also contain other groups
- **Task** A function which a user or group can perform, such as creating resources or designing reports

- **Role** A collection of tasks (functions). Roles are divided into non-global roles that apply to specific folders, and global roles that 'switch on' non-global roles for specific users by allowing them access to the system tools they need.

These combine to specify security permissions for each individual folder.

**Note** By default, the security permissions for a parent folder also apply to all its child folders, and so on down the folder hierarchy. It is, however, possible to change these inherited permissions for individual folders.

The following scenario demonstrates how these entities can be used to partition (restrict access to) system functions and resources so that users can only interact with those parts of the system they need to.

**Getting Started with Security**

The Management Portal comes with a number of groups and roles predefined. To give a user administrator privileges over your entire system, for example, it is only necessary to assign them to the `<Tenant>` Administrators group. The following table shows what groups are supplied with the system, what folders they can access, and what roles they can perform on those folders. The tasks that make up each of the roles are also listed.

<table>
<thead>
<tr>
<th>Group</th>
<th>Whereabouts</th>
<th>Access</th>
<th>Roles (non-global)</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;Tenant&gt;</code> Users</td>
<td>Tenant folder</td>
<td>Tenant folder</td>
<td>Tenant User</td>
<td>Browse Dimensions, Information Notices, Reports and Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tree</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>&lt;Tenant&gt;</code> Supervisors</td>
<td>Tenant folder</td>
<td>Tenant folder</td>
<td>Tenant Supervisor</td>
<td>Manage Dimensions, Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tree</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>tree</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
These roles cannot be edited, and the groups themselves cannot be deleted. There are also four global roles corresponding to the four non-global roles provided. Global roles 'switch on' the functionality provided by non-global roles. If you add a new role to a user group, you should make sure that the user or group has the global roles necessary to perform that role/task.

**Caution** Host administrators **must** always be able to perform the Manage Security task on the entire folder tree.

**Security Example**

Consider a company ExampleCorp that has two contact centers, a major one in New York and a much smaller one in San Francisco, and has set up a separate folder for each. ExampleCorp wants its New York administrators to be able to manage New York's resources, but not San Francisco's.

It therefore creates a group, NYAdmin, for the New York administrators, and assigns it the ability to perform the Tenant Administrator role on the New York folder.

**Note** This group must also be assigned the Tenant Administrator global role before it can actually perform administrative tasks.

ExampleCorp now has a set of administrators that can administrate only the resources of their specific contact center.

ExampleCorp then employs a single supervising administrator who needs to perform administrator tasks in both San Francisco and New York. This can be done easily by assigning the supervising administrator to the NYAdmin group and then separately assigning him the Tenant Administrator role on the San Francisco folder. You can see how to create this setup in the security tutorial provided as part of this manual.
Note ExampleCorp could alternatively have assigned the supervising administrator to the preset ExampleCorp Administrators group, in which case he would automatically have had administrator privileges on both the New York and San Francisco contact centers (folders), and any others that opened in the future.

Security Tutorial

The Management Portal provides a flexible and powerful security management system. Before attempting to understand the complexities of the system, you should first familiarize yourself with creating and using the basic building blocks of users, groups and roles. This section provides a tutorial that will guide you through the process of assigning folder permissions to users and groups.

Overview

This tutorial guides you through the process of creating a simple security setup for the company ExampleCorp, which has a main contact center in New York and a much smaller one in San Francisco.

You will be creating two users, assigning them to a group, and assigning folder permissions to both the group and individually to one of the users. You will also be introduced to the part that global roles play in restricting access to the system.

It is possible to set up security for your system using only the items you will be working with in this tutorial, though you may wish to customize the available roles to better suit your particular business requirements.

Before You Begin

For this tutorial, you will be working with a company ExampleCorp that has two contact centers in different geographical locations.

Before you begin, you will need to set up two folders to represent these contact centers.

1. From the Tools page, click on the System Manager tool. The System Manager page will open.
2. In the center Items panel, select **New ▼> System Items > Folder**
3. Enter 'New York' in the **Name** field, and check the **Create another** checkbox
4. Select your home folder in the folder tree to the left and click **OK**. The folder will be created.
5. Change the name in the **Name** field to 'San Francisco', uncheck the **Create another** checkbox, and click **OK**. You now have two folders.

Create Users

You will now learn how to create user accounts.

Create two users in New York.
1. Click on **Tools** to open the tools page, and open the Security Manager (not the System Manager)

2. Navigate to the New York folder and click on the **Users** option, followed by the **New** option, to open the **Create a new user** page

3. Create the user as follows:
   - In the **User Name** field, enter ESmith
   - In the **First Name** field, enter Example
   - In the **Last Name** field, enter Smith
   - Check the **Advanced Mode** and **Enabled** checkboxes
   - Enter '!Password1' in the **Password** and **Confirm Password** fields, ensure that the **Create Another** checkbox is checked, and click on **OK**

4. You will automatically be returned to the **Create a new user** page. Create a second user as follows:
   - In the **User Name** field, enter EJones
   - In the **First Name** field, enter Example
   - In the **Last Name** field, enter Jones
   - Check the **Advanced Mode** and **Enabled** checkboxes
   - Enter '!Password1' in the **Password** and **Confirm Password** fields, ensure that the **Create Another** checkbox is **not** checked, and click on **OK**

**Note**

- No real users should ever be given identical passwords, or passwords based on real words
- The suggested password will be valid in almost all systems. If it is not accepted, refer to your system's password requirements

The New York folder now contains two users, ESmith and EJones.

**Note** All users are automatically made members of two groups. These are the `<Tenant> Users` group, which allows them to see (browse) the folder structure created by the tenant, and the `Everyone` group, which allows them to see the folder structure within the shared resources folder.

Confirm group membership

1. Click on the properties icon for ESmith and select the Groups option. You will see that ESmith has been automatically made a member of these groups
2. Click the **Back** button
3. If you wish, you may select the **Access** option to confirm the security permissions that ESmith's group memberships have given him
Create a Group

ESmith and EJones will both need to be able to manage resources within the New York contact center. Creating a group with both ESmith and EJones as members, and then assigning permissions once to that group rather than twice to each individual, will make this task much quicker. This is especially true if you expect to have to allow other users the same permissions at a later date.

Create a NYAdmin group with ESmith and EJones as members

1. Click Tools and select the View Groups option
2. If necessary, navigate to the New York folder
3. Select the New option. This will open the Create a new user group page
4. Name the new group 'NYAdmin'. Ensure the Create Another checkbox is not checked and click OK
5. The NYAdmin group can now be seen in the Group Browser page. Click on its properties icon to open the Update Group page
6. Select the Members option to add ESmith and EJones to the group
7. In the central panel, select Users from the drop-down Items menu. You may also add existing groups to a new group in exactly the same way by selecting Groups from the drop-down menu
8. Check the boxes for ESmith and EJones. The group membership will update automatically. Click the red cross next to the EJones user to remove him from the group, and then check the box again to re-add him. There is no need to click on any button to save your changes

Assign Permissions to a Group

You now have a single NYAdmin group to which both ESmith and EJones belong. Now you can assign permissions to the group, and by extension to ESmith and EJones.

Assign the NYAdmin group the Tenant Administrator role for the New York folder

1. Click on Back to return to the Update Group page
2. Click on the Roles option. You will see a page showing the roles that this group may perform on the current folder. These are grayed out, showing that the folder is currently inheriting its security permissions from its parent folder
3. If necessary, navigate to the New York folder. Click on the link above the list. This shows you the current folder permissions
4. Select the Edit Item Security option to change the folder permissions. Click OK on the dialog box that pops up. The folder retains all of its existing permissions, but these can now be edited
5. Select the Groups option and check the box to select NYAdmin
6. Select the **Assign Permissions** option. This takes you to the
Assign Permissions page.

7. Check **Tenant Administrator** to assign the NYAdmin group
provisioning functions for the New York contact center. Click **OK**

8. You will be returned to the **Group Browser** page. Click on the
properties icon for the NYAdmin group and select the **Access**
option to see that members of the NYAdmin group now have the
ability to manage resources within the New York folder.

**Assign a Global Role**

Before ESmith and EJones can actually manage the resources, however,
they have to be granted access to various tools. This can be done by
adding the group to the appropriate global role.

Assign the NYAdmin group to the Tenant Administrators global role

1. Click **Settings** to go to the settings page, and select **Security Settings**
from the sidebar. You will see a list of the available
global roles. These determine the tools that users and groups can see in their homepage.

2. Click on the properties icon for the **Tenant Administrator** global role.

3. Select the **Members** option to open the **Global role members**
page. This is very similar to the page you used to add members to
a group.

4. Select **Groups**, navigate to the New York folder, and add the
NYAdmin group to the **Tenant Administrators** global role.

Now logout, and log back in as ESmith with the password '!Password1'.
You will be able to use the System Manager to create an information
notice within the New York folder, but not within the San Francisco
folder.

**Assign Permissions to a User**

ESmith and EJones are now both able to manage resources within the New
York contact center. EJones, however, is a supervising administrator who
also needs to be able to administrate the San Francisco contact center as
well. You will now separately assign to him the ability to perform the
Administrator role within the San Francisco folder.

Assign ESmith the Tenant Administrator role for the San Francisco folder

1. Logout as ESmith and log yourself back in.

2. Click on **Security Manager**.

3. Navigate to the San Francisco folder and select the **Edit Item Security**
option to change the folder permissions.

4. Click **OK** on the dialog box that pops up. The folder permissions
can now be edited.
5. Select the Users option. Navigate to the New York folder and check to select ESmith
6. Select the Assign Permissions option
7. Navigate to the San Francisco folder, and check Tenant Administrator to assign ESmith administrative functions for the San Francisco contact center
8. Click OK

You have now completed this tutorial. You know how to create users and groups, and assign them security permissions for folders. You may now proceed to the Manage Roles and Tasks topic to learn the theory behind what you have been doing.

Delete Your Examples

You may wish to retain the items you created during this tutorial for reference while you set up your first real security permissions. Once they are no longer needed, however, they should be deleted.

Delete your examples
1. Click on View Users to open the User browser page
2. Navigate to the New York folder, check the box above the list to select all the users within the folder, select the Delete option and confirm
3. Return to the Tools page, click on View Groups, and delete the NYAdmin group in the same way
4. Return to the Tools page, and open the System Manager
5. Navigate to your home folder, and click on Folders from the summary resource list to view the list of folders in the Items panel
6. Check the New York and San Francisco folders, select the Delete option, and confirm

The items you created for this tutorial have now been deleted.

Note: You cannot delete a folder while it still contains items. You should therefore delete all the users and groups you created before attempting to delete the folders.

Manage Roles and Tasks

Overview

Tasks (system functions) are grouped together into roles (for example, the Tenant Supervisor role includes the tasks manage dimensions (resources) and manage users). The way in which a specific user can interact with a specific folder is defined by the roles that he or she has been assigned on that folder.

There are two types of role, which perform different functions
- Non-global roles are applied to individual folders. Non-global roles enable a user to perform a specific set of tasks on that folder.

- Global roles 'switch on' the functionality provided by non-global roles. In system terms, they give the users and groups associated with them the ability to view the tools that perform certain functions.

**Note** Different security permissions are required to change global roles from those required to change non-global roles.

For example, a user who has been assigned the Tenant Administrator non-global role for a folder cannot actually perform any content management tasks until that functionality has been 'switched on' for that user (until that user has been given access to the System Manager tool) by assigning him to the Tenant Administrator global role.

The Management Portal provides a number of default roles that reflect common business needs, however you can create your own roles to correspond exactly to the tasks your specific classes of user need to perform.

**Managing Global Roles**

Global roles are managed via the Settings section. The system provides a number of preset roles that correspond to common requirements for normal users, supervisors, and administrators. You may edit these and create new roles that fit your business model.

**Caution** The host administrator must be able to perform the Advanced User, Manage Global Roles, Manage Global Security and Security Manager tasks. It is strongly recommended that these tasks never be removed from the preset Host Administrator global role.

To display the Settings section, click Settings, then click Security Settings. The roles available in the system will be displayed as a list.

To create a global role

1. Click New. The New Role page will be displayed. Then perform the following:
   - In the Name field enter the name of the role as it will appear in the system
   - In the Description field enter any explanatory text, if required

2. The tasks which can be added to the role are listed beneath the Name column. Explanatory text for each task is displayed beneath the Description column. Select the checkboxes of the tasks to be added to the role.

3. Click Save. The Roles page will be displayed. The new role will be listed beneath the Name column.

To edit a global role

1. Click the properties icon displayed next to the role name. The Edit Global Role page will be displayed.
2. Modify the following:
   - The Name of the role is displayed. This cannot be changed
   - In the Description field, enter any explanatory text if required
   - Click the Enabled checkbox to ensure the role is available in the system
   - Click the Hidden checkbox to ensure the role is saved in the system but cannot be used

3. All the available tasks are listed beneath the Name column. A description of each role is listed beneath the Description column. Select or deselect the checkboxes of the tasks to be associated with the selected role.

4. Click Save.

To delete a global role, select the checkbox of the role to be deleted and click Delete. The role will be removed from the system.

To edit the users or groups associated with a global role
   1. Click on the Properties icon for the global role. You will see the Edit Global Role page.
   2. Select the Members menu option. You will see a tree structure on the left, and a list of users and groups associated with the global role on the right. The central panel allows you to select users and groups to add to the role.
   3. Using the left hand tree structure, navigate to the folder containing the user or group you wish to associate with the role.
   4. Select either User or Group from the drop-down box in the central panel. All items of that type within the folder will be displayed.
   5. Select users and groups to associate with the role. No OK button is available to be pressed, as the panel on the right will update automatically.

You can remove users added from a role by clicking on the red cross next to the properties icon in the right hand panel.

**Managing Non-Global Roles**

Non-global roles are managed via the Security Manager section. The system provides a number of preset roles that correspond to common requirements for normal users, supervisors, and administrators. You may edit these and create new roles that fit your business model.

**Caution** The host administrator must be able to perform the Manage Security task. It is strongly recommended that these tasks never be removed from the preset Host Administrator non-global role.

To display the Security Manager section
   1. Click Tools. The Tools page will be displayed.
2. Click the Security Manager header. The Security Manager page will be displayed.

3. Click Roles. The Roles page will be displayed.

   Alternatively, click Tools. The Tools page will be displayed. Click View Roles. The Roles page will be displayed.

   Note: The Tools page can only be accessed by users who have been granted Advanced Mode status. See the User Settings topic.

The roles available in the system will be displayed as a list beneath the Name column. Explanatory text for each role is displayed beneath the Description column.

To create a non-global role

1. Click New. The New Role page will be displayed.

2. Perform the following:
   - In the Name field enter the name of the role as it will appear in the system
   - In the Description field enter any explanatory text, if required

3. The tasks which can be added to the role are listed beneath the Name column. Explanatory text for each task is displayed beneath the Description column. Select the checkboxes of the tasks to be added to the role.

4. Click OK. The Roles page will be displayed. The new role will be listed beneath the Name column.

To edit a non-global role

1. Click the properties icon displayed next to the role name. The Edit Role page will be displayed. Then modify the following:
   - The Name of the role is displayed. This cannot be changed
   - In the Description field, enter any explanatory text if required
   - Click the Enabled checkbox to ensure the role is available in the system
   - Click the Hidden checkbox to ensure the role is saved in the system but cannot be used

2. All the available tasks are listed beneath the Name column. A description of each role is listed beneath the Description column. Select or deselect the checkboxes of the tasks to be associated with the selected role.

3. Click OK.

To delete a non-global role, select the checkbox of the role to be deleted and click Delete. The role will be removed from the system.
Manage Folder Permissions

Users or groups can be assigned permissions to perform functions on a folder, such as move report, or on its contents.

To display the Security Manager tool, click Tools. The Tools page will be displayed. Click Security Manager. The Security Manager page will be displayed.

Note The Tools page can only be accessed by users who have been granted Advanced Mode status. See the User Settings topic.

Folders are organized into parent/child relationships. A child folder inherits the security of a parent folder.

To change the security permissions of a folder

1. From the Security Manager tool, select a resource folder (not a tenant folder) from the tree structure on the left and click on the Edit Item Security menu item
2. A dialog box will be displayed requesting you to confirm the change
3. Click OK. The selected folder will now no longer inherit the security permissions of the parent folder
4. You may remove all the permissions a user or group has on the folder by clicking on the red cross next to the properties icon

To reinstate the permissions of the parent folder, select the folder in the tree, click Revert to Parent Security, and click OK to confirm the change. The folder will now inherit the security permissions of the parent folder.

To assign folder permissions to selected user(s) or group(s)

1. From the Security Manager tool, click on the Users menu option (or the Groups menu option if you wish to assign permissions to groups)
2. Navigate to the folder in the tree that contains the users whose permissions you wish to modify
3. Select the checkboxes of all users that you wish to assign a specific folder permission and click on the Assign Permissions menu option
4. If roles are grayed out, this means that the folder is currently inheriting security from its parent. Click on the link above the list of roles and confirm to allow alternative security permissions to be assigned to it
5. Select the role(s) you wish the users to perform and the folder in which you wish them to perform it
6. Click OK
Manage Users

A user is anyone who has been given rights to access the Portal and the resources it contains. User management is accessed via the Security Manager section. Each user can be assigned specific roles that they can perform on specific folders. The specific way (the list of roles) in which a user can interact with specific folder is sometimes called that user's folder permissions.

To display the User browser page

1. Click Tools. The Tools page will be displayed
2. Click the Security Manager header. The Security Manager page will be displayed
3. Click Users. The User browser page will be displayed

Alternatively, click Tools. The Tools page will be displayed. Click View Users. The User browser page will be displayed.

**Note** The Tools page can only be accessed by users who have been granted Advanced Mode status. See the User Settings topic.

To edit a user

1. Select the folder in the tree that contains the users to be edited. The users associated with the folder will be displayed
2. Click the properties icon of the user to be edited. The Edit User page will be displayed
3. Modify the following fields as required:
   - The User Name field is grayed out because this cannot be modified
   - In the First Name and Last Name fields modify the user's details
   - In the Email field modify the email address of the user
   - In the Description field modify the description for the user
   - In the User Home Folder field modify the folder that opens in the user's homepage
4. Select the following check boxes if applicable:
   - The Advanced Mode checkbox if you wish the user to have the report manager enabled in their homepage
   - The Account Enabled checkbox ensures that the user is able to access the system
   - The Account Locked checkbox to prevent the user from accessing the system
   - The Password Never Expires checkbox to assign the password to the user indefinitely
   - The User cannot change password checkbox to prevent the user from being able to change their password
- The **User must change password at next Logon** checkbox to prompt the user to change their password after their first login
- The **Reset Password** to display the **Password** and **Confirm Password** fields. Enter and confirm the user's new password

5. Click **OK** to save the changes made to the selected user

To delete a user, select the folder in the tree that contains the user to be deleted. The users associated with the selected folder will be displayed. Select the checkbox of the user to be deleted and click **Delete**. The user will be removed from the folder.

To move a user

1. Select the folder in the tree, which contains the user to be moved
2. Select the checkbox of the required user
3. Click **Move**. The **Move the Current Items** page will be displayed, as well as a folder tree
4. Select the folder in the tree to move the user to and click **OK**

To add a user to a group

1. Select the folder in the tree that contains the user(s) to be added
2. Select the checkbox of the required user
3. Click **Add to Group**
4. Select the folder in the tree that contains the group to add the user to. The groups associated with the selected folder will be displayed
5. Select the checkbox of the required group and click **OK**. The user will now be added to the selected group

**Note** The user inherits the security permissions of the group to which they are added, in addition to any permissions specifically assigned to that user.

To assign folder permissions to a user

1. Select the folder in the tree that contains the user(s) whose permissions are to be changed. The users associated with the selected folder will be displayed.
2. Select the checkbox of the user to add folder permissions to and click **Assign Permissions**.
3. Select the folder in the tree that you want to change this user's ability to interact with. The roles which you can apply to the selected user for this folder are displayed beneath the **Name** column. A description for each role is displayed beneath the **Description** column.
4. Select the check boxes of the roles that the user should have for this folder and click **OK**.

**Note** The user will only be able to actually perform the specified roles on the folder if they have the necessary global roles to access the required tools.
To view the roles assigned to a user

1. Select the folder in the tree that contains the user(s), whose roles are to be viewed. The users associated with the selected folder will be displayed.
2. Click the properties icon displayed next to the name of the required group. The Edit User page will be displayed.
3. Click Roles. The User/Group role assignments page will be displayed. Navigate through the folder tree to see the permissions the selected user has on each folder. These roles will be displayed beneath the Name column. A description of each role is displayed beneath the Description column. Any roles whose check boxes have been selected are assigned to the user for the selected folder.

If you wish to add or delete a role assigned to the user, select or deselect the check boxes of the required roles. The page will refresh and the user's roles will have been modified.

If you wish to create a new role for the selected user, click New Role. For further information see the Manage Roles and Tasks topic.

The bottom section of the page displays the groups that the user belongs to beneath the Groups column and the roles the user has as a member of that group are displayed beneath the Roles column. Click the name of a group to edit the group. For further information see the Manage Groups topic.

To view, edit or delete the group associations (the groups which your user is a member of)

1. Select the folder in the tree that contains the required user.
2. Click the properties icon displayed next to the name of the user. The Edit User page will be displayed.
3. Click Groups. The Groups to which this user/group belongs page will be displayed. Beneath the Items section, the groups associated with the selected folder are listed. The groups whose check boxes are selected are the groups which your user belongs to. These are listed on the right of the page beneath the Group column. The Path column displays the path to the tree folder in which the group is located.
4. To edit the group associations, select the check boxes of the required groups listed beneath the Items section.
5. To delete the group associations, click Clear All.
6. Click Back to return to the Edit User page.

To move a user between groups, follow the instructions for editing a group association above.

To view the folders a user can access

1. Select the folder in the tree that contains the required user(s). The users associated with the selected folder will be displayed.
2. Click the properties icon displayed next to the name of the required user. The Edit User page will be displayed.
3. Click **Access**. The **User/Group system access** page will be displayed. The **Path** column displays the network paths to the folders which the user can access. The **Role** column displays the roles the user has per folder.

4. Click **Back** to return to the **Edit User** page

**To change a user's folder permissions**

1. Select the folder in the tree that contains the required user(s). The users associated with the selected folder will be displayed.

2. Click the properties icon displayed next to the name of the required user. The **Edit User** page will be displayed.

3. Click **Access**. The **User/Group system access** page will be displayed.

4. Click **Change Access**. The **User/group role assignments** page will be displayed.

5. Select the folder in the tree you wish the user to have access to and then select the check boxes of the roles you wish the user to have on that folder.

6. Click **OK**

**Note** The roles the user has for the selected folder are explicitly assigned to that user for that folder and are not affected by the role permissions the user may have as a member of a group.

**Create a User**

A user is anyone who has been given rights to access the Portal and the resources it contains. User creation is accessed via the security manager section.

**To display the User browser page**

1. Click **Tools**. The **Tools** page will be displayed.

2. Click the **Security Manager** header. The **Security Manager** page will be displayed.

3. Click **Users**. The **User browser** page will be displayed.

Alternatively, click **Tools**. The **Tools** page will be displayed. Click **View Users**. The **User browser** page will be displayed.

**Note** The **Tools** page can only be accessed by users who have been granted Advanced Mode status. See the User Settings topic.

**To create a new user**

1. Select the folder in the tree to which you wish to add the new user.

2. Click **New**. The **Create a new user** page will be displayed.

3. 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
- Leave the **User Home Folder** blank to set it to the same folder as the user is created in. This is the folder in which the user starts when they log in. For example, a supervisor user in Basic Mode will be able to browse any teams and skill groups in their home folder, plus teams and agents they are a supervisor for

4. Select the following checkboxes if applicable:
   - The **Advanced** checkbox if the user is to be capable of accessing the **Tools** page in order to potentially create resources, manage security, or other advanced functions
   - The **Enabled** checkbox to ensure that the user is live in the system. If unchecked the new user will be saved in the system but will not be able to 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

5. If you wish to create more than one new user for the selected folder, select the **Create Another** checkbox

6. Click **OK**

7. You may now optionally Assign Permissions to the new user, or Add to Group

You can also create a user via the **System Manager** tool.

**Note** All users created for a tenant are automatically assigned to the **Tenant Users** group and so by default have permission to view reports throughout the tenant's folder hierarchy.

**Manage Groups**

Any user in the system can view reports and may be assigned further roles (a set of system functions or tasks), which are specific to them as an individual. If however there is more than one user who will require the same folder permissions, they can be collected together as a group, and the group is granted specific folder permissions by the system users with
sufficient security privileges to do so. Group management is accessed via the security manager section.

The system provides a number of preset groups with appropriate global and non-global roles defined. All users are automatically added to the <Tenant> Users and Everyone groups, and user accounts linked to supervisor agents are automatically added to the <Tenant> Supervisors group.

To display the Group browser page

1. Click Tools. The Tools page will be displayed
2. Click the Security Manager header. The Security Manager page will be displayed
3. Click Groups. The Group browser page will be displayed

Alternatively, click Tools. The Tools page will be displayed. Click View Groups. The Group browser page will be displayed

**Note** The Tools page can only be accessed by users who have been granted Advanced Mode status. See the User Settings topic.

To edit a group

1. Select the folder in the tree that contains the group(s) to be edited. The groups associated with the folder will be displayed
2. Click the properties icon displayed next to the required group's name. The Update Group page will be displayed
3. Modify the following fields as required:
   - The Name field is grayed out because this cannot be modified
   - In the Description field modify any explanatory text, if required
4. Click the Enabled checkbox to render it accessible to users
5. Click OK

To edit a group's users (members)

1. Select the folder in the tree that contains the group to be edited. The groups associated with the folder will be displayed
2. Click the properties icon displayed next to the required group's name. The Update group page will be displayed
3. Click Members. The Manage members belonging to this security group page will be displayed
4. In the Items drop down list select User. A list of users which can be associated with the selected group will be displayed
5. Click Clear All to remove all users from the selected group, or click the checkboxes of the users to be added to the group. The page will refresh and the user(s) will be added to the list for the selected folder, which is displayed on the right of the page under the User/Group Name section
To delete a group
Select the folder in the tree that contains the group to be deleted. The groups associated with the selected folder will be displayed. Select the checkbox of the group to be deleted and click Delete. Alternatively, click the properties icon displayed next to the name of the group to be deleted. The Update Group page will be displayed. Click Delete. Click OK. The selected group will be removed from the tree.

To move a group
1. Select the folder in the tree that contains the group to be moved. The groups associated with the selected folder will be displayed
2. Select the checkbox of the group to be moved and click Move. The Move the current Items page will be displayed, as will the folder tree
3. Select the folder in the tree to move the group to and click OK
Alternatively, click the properties icon displayed next to the name of the group to be deleted. The Update Group page will be displayed. Click Move. The folder tree will be displayed. Select the folder to move the new group to and click OK.

To add a group to a group
1. Select the folder in the tree that contains the group to be added. The groups associated with the selected folder will be displayed
2. Select the checkbox of the group to be added and click Add to Group
3. Select the folder in the tree which contains the groups you wish to add your previously selected group to
4. Select the checkbox of the group to be added and click OK. Your group will now be added to the selected group
Alternatively, in the Security Manager page, click the properties button of the group to which a group will be added. Click Members. Select either User or Group from the drop down list and select the checkbox of the user or group you wish to add.

To view, add or delete the group associations (the groups which your group is a member of)
1. Select the folder in the tree that contains the required group
2. Click the properties icon displayed next to the name of the group. The Update Group page will be displayed
3. Click Groups. The Groups to which this user/group belongs page will be displayed
4. Beneath the Items section, the groups associated with the selected folder are listed. The groups whose checkboxes are selected are the groups which your selected group belongs to. These are listed on the right of the page beneath the Group column. The Path column displays the path to the tree folder in which the group is located
5. To add group associations, select the checkboxes of the required groups listed beneath the **Items** section.

6. To delete individual group associations, click the red crosses next to the group on the right of the page that is to be removed.

7. To delete all group associations, click **Clear All**.

8. Click **Back** to return to the **Update Group** page.

To assign folder permissions to a group:

1. Select the folder in the tree that contains the group(s) whose permissions are to be changed. The groups associated with the selected folder will be displayed.

2. Select the checkbox of the group to add folder permissions to (or remove them from) and click **Assign Permissions**.

3. Select the folder in the tree that you want to change this group's permissions on. The roles which you can apply to the selected folder for this group are displayed beneath the **Name** column. A description for each role is displayed beneath the **Description** column.

   **Note** If the available roles are grayed out, this means that the folder is currently inheriting permissions from its parent. You will have to break the inheritance link before you can assign folder-specific permissions to this folder.

4. Select the checkboxes of the roles that the group should have for this folder and click **OK**.

   **Note** The group will only be able to actually perform the specified roles on the folder if they have the appropriate global role to see the necessary tools.

To view the roles assigned to a group:

1. Select the folder in the tree that contains the group(s), whose roles are to be viewed. The groups associated with the selected folder will be displayed.

2. Click the properties icon displayed next to the name of the required group. The **Update Group** page will be displayed.

3. Click **Roles**. The **User/Group role assignments** page will be displayed. Navigate through the folder tree to see the permissions the selected group has on each folder. These roles will be displayed beneath the **Name** column. A description of each role is displayed beneath the **Description** column. Any roles whose checkboxes have been selected are assigned to the group for the selected folder.

4. If you wish to add, edit or delete a role assigned to the group, select or deselect the checkboxes of the required roles.

5. Click **Save**.

6. Alternatively, if you wish to create a new role for the selected group, click **New Role**. For further information see the Manage Roles and Tasks topic.
To view the folders a group can access

1. Select the folder in the tree that contains the required group(s). The groups associated with the selected folder will be displayed
2. Click the properties icon displayed next to the name of the required group. The Update Group page will be displayed
3. Click Access. The User/Group system access page will be displayed. The Path column displays the network paths to the folders which the group can access. The Role column displays the roles the group has per folder
4. Click Back to return to the Update Group page

Note The roles the group has for the selected folder are explicitly assigned to that group for that folder and are not affected by the role permissions the group may have as a member of a different group.

Create a Group

Any user in the system can view reports and may be assigned further system functions (tasks) that are specific to them as an individual. If however there is more than one user with the same task privileges, it is convenient to gather these users together as a group, and grant the group the appropriate permissions. Group creation is a function accessed from the security manager section.

To display the Group browser page

1. Click Tools. The Tools page will be displayed
2. Click the Security Manager header. The Security Manager page will be displayed
3. Click Groups. The Group browser page will be displayed

Alternatively, click Tools. The Tools page will be displayed. Click View Groups. The Group browser page will be displayed

Note The Tools page can only be accessed by users who have been granted Advanced Mode status. See the User Settings topic.

To create a group

1. Select the folder in the tree to which you wish to add the new group
2. Click New. The Create a new user group page will be displayed
3. Fill in the following fields:
   - In the Name field enter a name for the new group
   - In the Description field enter any explanatory text, if required
4. If you wish to create more than one new group for the selected folder, select the Create Another checkbox
5. Click OK to save the new group in the selected folder
8. GLOSSARY

A

Agent
Any contact center operative dealing with customers, usually by answering incoming phone calls. Each agent is associated with a peripheral and can be a member of one or more skill groups.

Agent Desk Settings
Settings for an enterprise or IPCC agent's phone or PC screen. Agent desk settings can be associated with each IPCC agent or with an IPCC peripheral. Also called agent desktop.

Agent Desktop
See Agent Desk Settings.

Agent Team
Any organizational or functional grouping of agents. An agent team is generally served by the same peripheral and has a common business focus such as a specific aspect of technical support. Agents may belong to several teams and skill groups.

Aggregate
The sum total of many similar elements or a summary of underlying values.

Alphanumeric
Consisting of both letters and numbers.

Announcement
A verbal message played to the caller.

Application log
A folder in the system that records details of events which have occurred in the system. The data recorded can be any data; this is determined by an appropriate system administrator.

Ascending
Defines a list as either starting with the letter A or with the lowest number (compare with Descending).

Assignment
The granting of specific task permissions to a user. See Role/Task.

Attribute
Attributes are features of the graphic user interface that can be customized, such as the company logo, screen colors or icons.
Audit
A report that provides data regarding the operation of the platform itself

Automate
To define a procedure that is carried out electronically, and independent of manual intervention

Breadcrumb Trail
The route by which the user arrived at the current help page. Each previous page in the 'trail' can be accessed by clicking the displayed link

Browser
See Web Browser

Cache
Memory on the application server, which stores the information used to generate a report for up to one month in case the information is required again

Call Type
A category of routable task determined by dialed number (DN), caller-entered digits (CED) and calling line ID (CLID). Each call type has a schedule that determines which routing script or scripts are active for that call type at any time

Cell
See Field

Chart
A graphical means of displaying report data

Checkbox
A small box displayed next to an entity in the system. By selecting the checkbox, the associated entity is made accessible for editing, deleting and so on
Child
In folder terms a child folder is one that is contained within another folder, called the parent. A child inherits the security permissions of its parent folder. Note that a single folder may be both the child of one folder and the parent of another. See Parent

Cluster
A grouping of similar resources, such as individual dialed numbers

Column
In a table, a column is a vertical slice through the table rows. Each column consists of a certain kind of data, indicated by the column header, whose values appear in the fields beneath. See Field, Row

Comma Separated Variable (CSV)
A method of representing a spreadsheet using a text file. The values are separated by commas, and each record is ended by a line break. The column headers are contained in the first record

Create
To add an entity to the system, such as a new user, customer, resource or mapping

Credentials
See Permissions

CSV
See Comma Separated Variable

Customize
To change an entity in the system to suit a unique purpose. Also to change the system settings to suit an individual user's requirements

D

Data
The information generated by a computer based system

Data Field
In analysis services, data fields provide the total values to be summarized in a report view

Data Mart
A server running the Microsoft SQL Server analysis services application, which stores in memory the online analytical processing (OLAP) cubes used in report analysis

Database
A server running the Microsoft SQL Server application, which stores in memory the data used in reporting
Datasource
A reporting engine, which provides access to the data to be displayed in the spreadsheet, chart and pivot table

Default
The value that will be used when no alternative value is supplied by the user

Delete
To remove an entity, parameter or mapping from the system

Descending
Defines a list as either starting with the letter Z or with the highest number (compare with Ascending)

Destination
Code describing the target for an outgoing call (dialed number)

Destination Number
The telephone number to which the call was routed by the network. See Label

Detail Field
See Total Field

DIALED Number
The telephone number dialed by the calling party

Dimension
A means of grouping and separating contact center data of a similar type in the SQL Server database. Together with measures, they are organized into fact tables. The relationship between Dimensions and Measures is similar to that between Columns and Rows. Also another term for a resource

Drill down/up
To navigate through trees or data. Drill down to view child folders or data in finer detail and drill up to view parent folders or summarized data values

Drillthrough
To use a field in one report to link to the same data item in another report

Edit
To change the properties of an entity in the system
Enable
To make an entity in the system either accessible or functional

Enterprise
Collective term describing all parts of a company serviced by a single call distribution system. This may include several contact centers served by different peripherals

Enterprise Service
Organizational grouping of agents within a company, perhaps spanning several contact centers and served by different peripherals, providing a specific customer service, such as technical support

Enterprise Skill Group
Organizational association of contact center agents within a company, perhaps spanning several contact centers and served by different peripherals. Agents in a skill group share common talents such as technical or language abilities, or skills in dealing with complaints

Error
An event on the platform that prevents it from operating as expected

Excel
The spreadsheet application provided by Microsoft corporation

Exception
A value which falls outside set parameters. Exceptions may be highlighted for ease of identification. See Threshold

Expiry
A date and time, configured in the system, at which point a defined process or piece of information is rendered invalid

Export
To save a report as a document type that can be published and distributed independently of the platform

Extensible Markup Language (XML)
A markup language used to create special-purpose markup languages. It facilitates the sharing of data across different systems, particularly systems connected via the Internet

Extension (filenames)
Different report format file names use a character extension that is unique to each format type

Extension (telephone)
Either a telephone number that is local to the switch or a telephone station served by a PBX (Private Branch Exchange)
**F**

**Field**  
An area in a table in which data can be included. The value in a field represents the value from the data represented by that specific row that belongs in the context defined by the column. See also Row, Column

**Filter**  
A means of choosing what data to view

**Folder**  
A system folder that can be linked to other folders in the system in parent/child relationships (compare with Tenant Folder). See also Parent, Child

**G**

**Generate**  
To run a report

**Global role**  
A role that applies throughout the entire system

**Graphical User Interface (GUI)**  
The front-end to the application that provides the user with the means to define and generate reports

**Group**  
A collection of users who share the same security permissions

**GUI**  
See Graphical User Interface

**H**

**Header**  
The field in a report grid which describes the contents of the column beneath it or the row beside it

**Hierarchy**  
A tree structure in which the root folder at the top of the tree is the parent folder to all the folders beneath it. Folders are organized into parent/child relationships in which the subordinate child folders inherit the security permissions of a parent folder. Tenant folders are unusual in being stand alone and unable to inherit the permissions of a parent folder
Historical
Historical data reflects the past activities occurring in the organization

HTML
See Hypertext Markup Language

Hypertext Markup Language (HTML)
A markup language used to build web pages and other information which can be viewed in a web browser

Icon
A picture displayed in the GUI that represents a system function or object. Some icons may be purely representative. Other icons, however, may be used as shortcuts to the object or function they represent. For example, the Properties icon acts as a link to the properties page in which the properties of the selected object may be modified

IE
See Internet Explorer

Import
To load data into the platform from an external source

Increment
One of a series of regular additions. Specifically, the adding of a new version of a report to a list of previous versions

Information Notice
Information notices are used to inform contact center staff of general information or new announcements. Information notices are displayed in the homepage

Interactive Voice Response (IVR)
Also called VRU (Voice Response Unit) or ARU (Audio Response Unit). A device that routes a call automatically using a customer's replies to a series of prompted messages. An IVR may respond directly to a customer's voice or to a sequence of dialed digits (CED)

Interface
See Graphical User Interface

Internet Explorer
The web browser developed by Microsoft Corporation. Several versions are available, providing different levels of functionality

IP Phone
A telephone that can be integrated into an IP network
IVR
See Intelligent Voice Response

J

Job
A task performed by the system

L

Label
An identifier, usually a destination number, that is associated with a specific peripheral target or with a specific network target used for call routing purposes

Layout
The way in which information is displayed

Legend
A quick means of identifying the different elements displayed in a report.

Link
The system enables you to access certain functions or pages by clicking certain text or buttons. Link text is usually distinguished from normal text by being underlined or bold

Linked Report
When a report's parameters (items) are changed and saved under a new report name, the new report is linked in the system back to the original report

List
A series of alphabetical or numerical objects or values

Log in
For a user to identify themselves to the Web Portal. No user can use the Web Portal without logging in. This is a security measure which ensures that each user may only use those data and functions to which they have been granted access. This process is also called logging on (compare Log out). See Login ID, Password

Log out
To leave the system, disabling access to functions and data. A user should log out once they have finished working with the system to prevent other individuals gaining access to functions and data they are not authorized to use (compare Log in)
Login ID
This is the same as the user name. Along with a password, it allows a user to log in to the system. See Log in, Password

Mapping
The process of associating one item with another. For example, you might associate a user with a security group that has permission to access particular resources, or a security group with a resource group, or a dialed number with a destination number (label)

Measure
A means of grouping and separating Enterprise contact center data of a similar type in the SQL Server database. Together with dimensions, the measures are organized into fact tables. The relationship between Measures and Dimensions is similar to that between Rows and Columns

Member
A user who belongs to a user group

Message
A piece of useful or instructional text

Navigate
To search though a hierarchical folder structure in the tree, or to follow a set of commands to access a page or function within the system

Notice
See Information Notice

Office Web Components (OWC)
Tools based on Microsoft Excel technology, but used in the web browser rather than the desktop. They consist of the Spreadsheet, Chart, Pivot Table and Data Source components

Online
To be able to communicate across a network

OWC
See Office Web Components
Parameters
Settings that enable you to define the type and amount of information displayed in a report as well as the way in which the data is presented.

Parent
A folder that contains one or more sub-folders (child folders). A parent folder sets the default security permissions of its child folders (compare with Child).

Password
A word or specific string of characters, usually consisting of letters and numbers, that is used by a given user to access an application. The word is known only to that user and acts as a security measure to ensure that each user can only access their own data and functions. See Log in, Login ID.

PDF
See Portable Document Format.

Peripheral
An individual device or switch providing routed customer phone calls to contact center staff. The term peripheral is also used to describe parts of a contact center Enterprise receiving calls from the device.

Permissions
A security measure. The set of roles a user can perform on a specific folder or folders. See also Role.

Pivot Table
An office web component that is similar to a spreadsheet, except that the row and column data values are summarized values of underlying data, which can be drilled down into to explore highly detailed report values.

Portable Document Format (PDF)
A file format developed by Adobe systems that stores documents independent of the software or hardware used to create them. A PDF document will appear exactly the same regardless of the platform on which it is displayed.

Prefix
A character added to a folder to specify where to place imported resources.

Print
To make a paper copy of a document or report.

Privilege
See Permissions.


**Properties**
The qualities possessed by an object which define it

**R**

**Radio button**
Similar to a checkbox. A small circle displayed next to an entity in the system. By selecting the button the associated entity is made accessible for editing, deleting, and so on.

**Refresh**
To upload the latest data in a browser window

**Render**
The process of creating a report in a specific format

**Report**
A view of information or data, which is summarized and displayed numerically in a pivot table or graphically in a chart

**Resource**
An entity or value in the data mart that represents an asset belonging to a customer, such as a dialed number, agent, call route, and so on. Resources are stored in folders. Also called dimensions

**Rights**
See Permissions

**Role**
A defined set of tasks that determine how users can interact with folders. See also Task

**Routing Script**
Routing scripts are programs that determine the best way of handling a call. Reports on script activity show which reports have been called, the nodes executed within the scripts and so on

**Routing Table**
A table that states which dialed number is directed to which destination number (label)

**Row**
In a table, a row is a horizontal line of cells spanning the columns. Each row supplies values from a certain set of data that relate to the context described by the column header. See also Column, Field
Scroll
To display a new area of text within the current document or web page. This is normally accomplished using scrollbars that appear at the side or bottom of the window and indicate the user's location within the text.

Security
Any process which prevents the data held in the data mart from being viewed by unwanted users, while at the same time enabling permitted users to access the data they require.

Security Group
A collection of users who are associated with particular resources and perform particular functions according to the permissions granted to the group by the applicable user, such as creating, deleting or viewing reports.

Security Tree
A hierarchical tree in which security groups and their associated users are organized. In the Management Portal all system resources, users and groups are stored in folders in the tree.

Session
A single period during which a user is logged into the system.

Settings
Functions that define the manner in which the user interacts with the system.

Skill Group
An organizational association of contact center agents sharing common talents such as technical or language abilities, or skills in dealing with customer complaints. Skill groups are associated with a particular peripheral and allow the ICM to route calls to the most appropriate available agent. Several skill groups at different contact centers are served by different peripherals and may be collectively combined in an enterprise skill group.

Spreadsheet
A document which displays data numerically in fields organized into rows and columns.

State
An item's provisioning status. There are five states: Synchronise, Error, Ready, Delete Pending and Deleted.
Subset
A subset of data is a portion of the data that when calculated together creates a summarized value

Summary
A high level view of data; the sum of underlying data values

Supervisor
A person responsible for a team of agents. A supervisor can add and remove agents and view statistics for the team that they supervise. A supervisor may also be an agent. See also Agent Team

System Administrator
The highest level of user in the management system, who is responsible for creating more users and granting user permissions and access rights

Table
A matrix consisting of fields, separated into rows and columns, which display values

Tagged Image File Format (TIFF)
A standard image file format. The TIFF format supports multiple images and data in the same file, images of multiple pages and other options

Task
An action that a user is allowed to perform. Tasks are collected together to create a Role

Team
See Group, Agent Team

Tenant Folder
A folder exclusive to a particular tenant. It is the same as a system folder except that a tenant folder does not and cannot inherit the security permissions of a parent folder and is a stand-alone entity (compare with Folder)

Threshold
A limit defined on the application server and applied to report data. Data values breaching the threshold are displayed in a manner that easily differentiates them from other data values

TIFF
See Tagged Image File Format
**Toolbar**
A list of links above the report view panel. These links are used to access the various functions and options available to the user.

**Total Field**
Totals fields display a value which represents a total or summary of all of the available data selected for analysis.

**Uniform Resource Locator (URL)**
The global address of a document or site on the World Wide Web (such as www.cisco.com).

**Uniform Resource Name (URN)**
A means of identifying resources on the Internet. An URN is a unique and unchangeable name (compare with Uniform Resource Locator).

**URL**
See Uniform Resource Locator.

**User**
An individual granted access to the application.

**User Group**
Users who share the same role assignments (security permissions).

**View**
How an item (such as a report) is displayed.

**Voice Response Unit (VRU)**
A device capable of routing a call automatically using a customer's replies to a series of prompted messages. A VRU may respond directly to a customer's voice or to a sequence of dialed digits. Also called IVR (Interactive Voice Response Unit) or ARU (Audio Response Unit).

**Web Archive**
A stand alone HTML file with the extension .mhtml, which contains report data in HTML code.

**Web Browser**
An application that allows a user to access the World Wide Web or locally held web pages. Web browsers include a graphical interface that lets users interact with and navigate through web pages.
Web Server
The web server obtains data directly from the data mart in response to user queries.

Wrap
A call state in which activities such as paperwork or consultations arising as a direct result of, and associated with, a customer call are completed. Also called Post-Call Processing (PCP) or After-Call Work (ACW). An agent is not available to take calls during wrap up activities.

WYSIWYG
What You See Is What You Get. Typically used to describe a text editor that displays formatted text

XML
See Extensible Markup Language
| Manage Resources | 57, 59, 100 |
| Manage Roles | 118 |
| Manage Security | 111 |
| Manage Settings | 31 |
| Manage Telephones | 57, 92, 96, 100 |
| Manage the System | 51 |
| Manage Users | 123 |
| New Report | 44, 46 |
| New Role | 32, 118, 123, 127 |
| New Schedule | 46 |
| New System Notice | 39 |
| Online Help | 13, 14, 15, 17, 21, 43, 44 |
| Parameter Sets | 46, 49 |
| Parent/child | 54, 55, 122 |
| Password | 15, 20, 35, 72, 123, 126 |
| Permissions | 111, 114, 122 |
| Persons | 68 |
| Prefixes | 14 |
| Print | 44, 46 |
| Properties | 32, 46, 55, 118, 123, 127 |
| Ready | 60 |
| Real Time reports | 43 |
| Reports | 43 |
| Historical Reports | 43 |
| Managing Reports | 43, 44, 46, 49 |
| Real Time reports | 43 |
| Report Exception Thresholds | 49 |
| Report Parameters | 43, 46 |
| Resources | 31 |
| Disabled | 55, 57, 59 |
| Roles | 32, 114, 118 |
| Global Roles | 32, 114, 118 |
| Non-Global Roles | 114, 118 |
| Security | 32, 111, 114 |
| Settings | 20, 31, 32, 35, 37, 79 |
| Skillgroups | 28, 87 |
| Skills | 28, 87, 90 |
| Synchronize | 60 |
| System | 51 |
| Tasks | 118 |
| Teams | 25, 72, 84 |
| Telephones | 57, 59, 92, 96, 100 |
| TIFF | 44 |
| Tree Structures | 14, 54, 55 |
| Tutorial | 114 |
| Understand Reports | 43, 44 |
| Upload | 61, 105 |
| User | 14, 55, 111, 118, 122, 126, 131 |
| Managing Users | 15, 31, 32, 35 |
| Settings | 106 |
| View | 17, 21, 44 |
| VRU Script | 105 |
| WAV file | 105 |
| Welcome | 13, 14, 17 |