



**Security Guide
for Cisco Unified Contact Center Domain Manager**

Release 9.0(1)

August 2012

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

Copyright 2012 Cisco Systems, Inc. All rights reserved.



Contents

| | |
|--|-----|
| Contents | i |
| Preface | iii |
| Purpose | iii |
| Audience | iii |
| Organization..... | iii |
| Related Documentation..... | iv |
| Product Naming Conventions | iv |
| Conventions | v |
| Obtaining Documentation and Submitting a Service Request | vi |
| Documentation Feedback | vi |
| 1. Unified CCDM Security Fundamentals | 1 |
| Security Overview..... | 1 |
| Folders..... | 2 |
| Tasks | 3 |
| Roles..... | 4 |
| Summary | 5 |

2. Managing Roles7

Creating Roles7

 How to Create a Role7

 Default Groups8

3. Creating a Folder Structure9

Managing Folders9

 How to Create a New Folder9

 Policy Roots and Inheriting Permissions10

The Shared Folder12

4. Managing Security14

Creating Users and Groups14

 How to Create a User14

 How to Create a Group16

 Managing Group Memberships16

 How to Add Users to Groups16

 How to Add a Group to Other Groups18

 How to Add Multiple Members to a Single Group19

Assigning Global Permissions19

Assigning Folder-Based Permissions20

 How to Add Folder Permissions to a User or Group20

 Editing Security on Folders That Inherit Permissions22

Appendix A. Roles and Tasks23

Folder-based Tasks23

Global Role Tasks26

Example Usage29



Preface

Purpose

This document explains how to set up and maintain security for the Unified Contact Center Domain Manager (Unified CCDM). It should be read in conjunction with the security section of the *User Manual for Cisco Unified Contact Center Domain Manager*, which describes the entities and operations involved in greater detail.

Audience

This document is intended for administrators responsible for the commissioning and ongoing maintenance of the Unified Contact Center Domain Manager. All users responsible for managing security should have access both to this document and to any records of the exact system setup chosen.

Organization

The sections of this guide are as follows:

| | | |
|------------|------------------------------------|--|
| Chapter 1 | Unified CCDM Security Fundamentals | Contains an overview of CCDM security and the main concepts. |
| Chapter 2 | Managing Roles | Describes how to create and manage CCDM security roles. |
| Chapter 3 | Creating a Folder Structure | Explains how to set up a folder structure to manage security. |
| Chapter 4 | Managing Security | Describes how to create users and groups and to assign permissions to them. |
| Appendix A | Roles and Tasks | Describes the security task permissions available in CCDM and how they relate to the default security roles. |

Related Documentation

Documentation for Cisco Unified ICM/Contact Center Enterprise & Hosted, as well as related documentation, is accessible from Cisco.com at:

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

- Related documentation includes the documentation sets for Cisco CTI Object Server (CTIOS), Cisco Agent Desktop (CAD), Cisco Agent Desktop - Browser Edition (CAD-BE), Cisco Unified Contact Center Domain Manager, Cisco Unified Customer Voice Portal (CVP), Cisco Unified IP IVR, Cisco Unified Intelligence Center, and Cisco Support Tools.
- For documentation for these Cisco Unified Contact Center products, go to <http://www.cisco.com/cisco/web/psa/default.html>, click **Voice and Unified Communications**, then click **Customer Contact**, then click **Cisco Unified Contact Center Products** or **Cisco Unified Voice Self-Service Products**, then click the product/option you are interested in.
- For troubleshooting tips for these Cisco Unified Contact Center products, go to <http://docwiki.cisco.com/wiki/Category:Troubleshooting>, then click the product/option you are interested in.
- Documentation for Cisco Unified Communications Manager is accessible from: <http://www.cisco.com/cisco/web/psa/default.html>.
- Technical Support documentation and tools are accessible from: <http://www.cisco.com/en/US/support/index.html>.
- The Product Alert tool is accessible from (sign in required): <http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice>.
- For information on the Cisco software support methodology, refer to *Software Release and Support Methodology: ICM/IPCC* available at (sign in required): http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/prod_bulletins_list.html.

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

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

Product Naming Conventions

In this release, the product names defined in the table below have changed. The New Name (long version) is reserved for the first instance of that product name and in all headings. The New Name (short version) is used for subsequent instances of the product name.

Note This document uses the naming conventions provided in each GUI, which means that in some cases the old product name is in use.

| Old Product Name | New Name (long version) | New Name (short version) |
|---|---|--------------------------|
| Cisco IPCC Enterprise Edition | Cisco Unified Contact Center Enterprise | Unified CCE |
| Cisco IPCC Hosted Edition | Cisco Unified Contact Center Hosted | Unified CCH |
| Cisco Intelligent Contact Management (ICM) Enterprise Edition | Cisco Unified Intelligent Contact Management (ICM) Enterprise | Unified ICM |
| Cisco Intelligent Contact Management (ICM) Hosted Edition | Cisco Unified Intelligent Contact Management (ICM) Hosted | |
| Cisco CallManager/Cisco Unified CallManager | Cisco Unified Communications Manager | Unified CM |

Conventions

This document uses the following conventions:

| Convention | Description |
|----------------------|--|
| boldface font | <p>Boldface font is used to indicate commands, such as entries, keys, buttons, folders and submenu names. For example:</p> <ul style="list-style-type: none"> • Choose Edit > Find • Click Finish |
| <i>italic font</i> | <p>Italic font is used to indicate the following:</p> <ul style="list-style-type: none"> • To introduce a new term; for example: A <i>skill group</i> is a collection of agents who share similar skills • For emphasis; for example: <i>Do not</i> use the numerical naming convention • A syntax value that the user must replace; for example: IF (<i>condition, true-value, false-value</i>) • A book title; for example: Refer to the <i>Cisco CRS Installation Guide</i> |
| window font | <p>Window font, such as Courier, is used for the following:</p> <ul style="list-style-type: none"> • Text as it appears in code or that the window displays; for example: <pre><html><title>Cisco Systems, Inc. </title></html></pre> |

| | |
|-----|---|
| < > | Angle brackets are used to indicate the following: <ul style="list-style-type: none">• For arguments where the context does not allow italic, such as ASCII output• A character string that the user enters but that does not appear on the window, such as a password |
|-----|---|

Obtaining Documentation and Submitting a Service Request

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

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

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

Documentation Feedback

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

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.



1. Unified CCDM Security Fundamentals

Unified Contact Center Domain Manager (Unified CCDM) provides a flexible and fine-grained security model which enables administrators to align access rights for individual business users with their specific business accountability. It allows users to operate with complete security in their individual areas of responsibility without impacting other parts of the virtual enterprise.

Resources within Unified CCDM, such as Agents, Users, Skill Groups and Reports, are stored in folders as part of a hierarchical folder structure that is typically modeled on the organizational structure of the business. Users and groups of users can be given permission to perform a variety of tasks on the resources in a folder. For example, a user with the *Manage Users* permission in a particular folder can view and edit users in that folder, but cannot view and edit users in any folder where they do not have that permission.

By separating resources into different folders and granting users different permissions on those folders, a security model can be constructed that gives access to business users to the resources that are relevant to their organizational role with the appropriate degree of management capability.

This section gives an overview of how security in Unified CCDM works and describes the individual components of the security model.

Security Overview

The basic components for configuring security in Unified CCDM are *Users*, *Tasks* and *Folders*. A Task is a discrete operation such as 'Browse Folders' or 'Manage Dimensions'. A Unified CCDM User can be given permission to perform a task within the scope of a particular Folder in the Unified CCDM folder tree.

Applying each task to each user on every folder in a complex tree would be cumbersome. To simplify the process, Unified CCDM provides a mechanism to group together a collection of tasks into a *Role*. This role can then be given to a user (within the context of a folder) to enable them to carry out a number of different tasks.

To further simplify the management process, Unified CCDM allows users to be collected together as a *Group*. In the same way that a user is given permission to perform a role within a folder, a Group can be given rights to perform a role within a folder. All of the users who are members of the group receive those permissions through their group membership. This means that future changes to permissions can be managed by applying them to a group, rather than repeating the change for each user, and new users who require the same rights can simply be added to the group.

To simplify security management further still, Unified CCDM allows permissions on a folder to be inherited from its parent folder. This means that permissions can be set at the highest level folder and are cascaded down to lower level folders that require the same settings, without an administrator needing to apply them to each ‘child’ folder.

As well as folder based partitioning, Unified CCDM also provides a mechanism for managing access to features and functionality at a ‘global’ level. Global security is used to manage access to features while folder based security can be used to determine where, and with which resources those features can be used. For example, access to the System Manager tool is something that a user either can or cannot do, it is a global task. A folder based task determines whether or not the user has the right to edit reports in a particular folder.

The relationships between the security components are ‘many-to-many’:

- A *user* can belong to many *groups*
- A *group* can belong to many other groups
- A *role* is comprised of many *tasks*
- A *task* can belong to many different *roles*

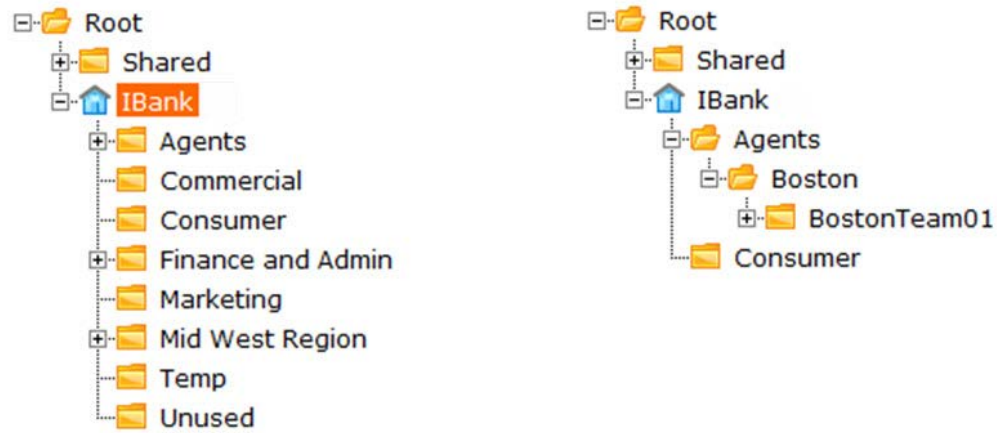
Using the basic building blocks, a sophisticated and fine-grained security model can be constructed.

This guide describes how to configure Unified CCDM’s security and offers guidance on best practice for setting up a security framework.

Folders

Folders in Unified CCDM are organized in a hierarchical tree and access to them can be partitioned, so that individual users have access to different sets of folders. Figure 1.1 shows a view of a Unified CCDM tenant, called IBank, from the perspective of two different users; one of whom is permitted to view many of the folders in IBank, the other who has restricted access to the Consumer and BostonTeam01 folders.

Figure 1.1 The IBank Tenant Folder, Viewed with Two Different Permissions



A folder may inherit its security settings from its parent folder, or may have separate security settings from its parent folder. A folder that does not inherit its security setting from its parent is called a *policy root*. It has its own security settings (the policy) and it is a root folder from which its child folders can inherit their security. See Chapter 3, Policy Roots and Inheriting Permissions for more information about policy roots.

Tasks

A *Task* is an individual permission applied to a user, or group of users, that enable them to carry out particular operations, such as browsing resources or managing information notices within a specified folder or accessing a particular tool. Tasks are either folder-based or global.

Folder-based Tasks

Folder-based task permissions are allocated to folders, and allow a user to do that task in any folder which has that permission.

In general, Unified CCDM provides two types of folder-based task:

- **Browse** tasks allow a user to view items of a specified type. For example, enabling the Browse Dimensions task allows a user to examine resources in that folder using the System Manager tool.
- **Manage** tasks allow a user to move, add, change and delete items of a specified type within a folder. For example a user with the Manage Information Notices task permission can create information notices in the specified folder via the Information Notices and System Manager tools.



You cannot separate out the Manage task permissions any further. For example, you cannot allow a user to change an item but not delete it. If you want users to be able to manage some resources but only to browse others, you should place these resources in separate folders.

Global Tasks

Global tasks give the user permission to carry out various operations, for example, the *Security Manager* task permission allows the user to run the Security Manager tool and the *Provision Agent* task permission allows the user to provision agents.

For most operations, the user will require one or more folder-based task permissions as well as the global task permission. For example, a user with the Security Manager global task permission must also have the Manage Security permission on the folder for which they want to manage the security.

Roles

A *role* is a collection of tasks which define the permitted actions for a particular user or group of users. A role such as ‘Basic User’ has a different set of tasks enabled, to that of ‘Supervisor’ allowing each type of user access to the resources and functionality which is appropriate to their remit. Within Unified CCDM, you can create new roles, change the sets of tasks which make-up existing roles, and apply roles to groups of users.

There are two types of role, folder-based roles and global roles.

Folder-based Roles

Folder-based roles specify the folder tasks which may be performed within specific folders, for example the ability to manage users within a specific folder. These roles apply to a user (or group) only within the specified folder, where they have been applied, and within any subfolders that inherit their security permissions from that folder.

Roles (composed of tasks) are applied to users and groups of users with permission to perform those tasks on the resources in specific folders. Sub-folders can inherit the same security permissions if necessary, granting the same group of users the same permissions on those folders. For more information on inheritance, see Chapter 3, Policy Roots and Inheriting Permissions.

Figure 1.2 Roles, Tasks and Folders









Global Roles

Global Roles are comprised of global tasks which provide the ability to perform certain kinds of action system-wide. Global tasks, and hence global roles are not folder specific. For example, the ability to access Security Manager is a global task. The ability to manage security on a particular folder is a folder-based task. Global roles applied to a user (or group of users) are effective across the entire system.

Summary

Users, folders and roles form the basic components of Unified CCDM Security. With these building blocks defined, the process of implementing a security model in Unified CCDM can be summarized as follows:

-  **Identify and create the security roles you need** to allow you to distribute permissions appropriately. From a management perspective it makes sense to keep the number of roles as low as you can, while still delivering the partitioning you need.
-  **Configure default groups and roles.** Unified CCDM allows you to specify *default groups* that are automatically created when a new folder is added. These groups then have predefined security settings on the new folder. Using this feature can speed up the process of managing security a great deal, so it is worth understanding and leveraging it.
-  **Construct a folder tree** in which resources can be stored. Try and keep it simple. Aim for the minimum number of folders required in order to partition access to resources appropriately. If you need to restrict access to agent resources on a team-by-team basis for reporting purposes, then a folder will be needed for each team. Typically the folder tree will mirror the organizational structure. It's worth noting that in very large installations, folder depth (the number of levels between the root folder and the lowest leaf level folder) can have an impact on system performance. As a rule try and keep to a maximum folder depth of seven folders, not including the tenant folder.
-  **Define Inheritance.** When planning the folder structure, determine which folders can inherit their security from a parent folder and which need their own specific security settings (policy roots). The more folders that inherit security, the less administrative activity required. However, you may need different configurations of security permissions on a variety of folders to meet business requirements for access control.

-   **Create users and assign permissions.** Assigning permissions to users through their group memberships can simplify security management. Give the permissions required for a particular role (global and folder-based) to a group and then add the users who need those permissions to that group. If a single group, or a small number of groups, already have all the permissions a user needs, all you have to do to set up a particular user's access permissions is add them to the appropriate groups.

The rest of this document describes each of these steps in detail.



2. Managing Roles

Roles are collections of tasks, which can be grouped together and applied to users or groups. Like tasks, roles can be folder-based, containing a collection of folder-based tasks, or global, containing a collection of global tasks.

Folder roles always apply to folders. A user that has a particular folder role in a folder is able to do all the tasks in that role on the items in that folder. A user that has been given a global role is able to do all the tasks in that global role.

This section describes how to create new roles. It also describes how default groups and roles are automatically assigned to simplify the process of managing security.

Creating Roles

Unified CCDM comes with a number of pre-configured global and folder-based roles. You can choose to use these roles as they are, or edit them and create additional roles to suit your needs.

For a complete list of all the global and folder-based tasks available, and the preconfigured roles to which they apply, see Appendix A.



To manage folder-based roles, use the **Role Manager** link in the Security Manager. To manage global roles, use the **Global Security Manager** link in the Security Manager.

How to Create a Role

1. From the **Security Manager** on the **Tools** Page select the **Role Manager** link to create folder role, or the **Global Security Manager** link to create a global role. A list of existing roles is displayed.
2. Click **New** on the menu bar. The Create New Role page is displayed, showing a list of tasks with blank check boxes.
3. Enter the **Name** and **Description** of the role.

4. Select the check boxes of the tasks you want to enable for the role. A complete list of tasks is given in Appendix A.
5. Click **Save**. The new role is added to the list of roles.

**Note**

When creating global roles that allow access to the System Manager, Information Notices or other tools, you will also need to include the **Advanced User** global task to allow access to the Tools page.

Default Groups

Every time a policy root folder is created, up to three groups will be created automatically within the folder. These groups will have a default role applied to them for the folder. You can configure and use these groups to simplify security management. Ideally these groups will align with the security profiles required by the majority of users.

The following default groups and roles are used:

- **Basic Users Group**, with **Basic** role
- **Supervisor Users Group**, with **Supervisor** role
- **Advanced Users Group**, with **Advanced** role

**Note**

The default Advanced users group is also given the global security role of **Global Advanced** when a new folder is created. See Chapter 1, Global Roles for more information.

You can change the groups you want to be added to each new policy root, and the role you want to apply to each group on the folder.

To change the default groups and their roles:

1. Click **Settings** from the top right menu.
2. Select **Security Settings** from the left menu panel.
3. The Security Settings page is displayed, showing **Groups to create when removing inheritance**.
4. Select which groups you want to be added to new policy root folders.
5. For each group, select a folder role from the drop-down menu.
6. Click **Save**.

New users are also added to the **Everyone** group, which is given the **Basic** role by default and the **Basic** folder-based role on the Shared folder.

The Security Settings page allows you to apply folder-based roles only to default groups. It is not currently possible to change the global roles associated with the default groups.



3. Creating a Folder Structure

This section describes how to set up a folder structure in Unified CCDM. A folder represents the lowest level at which security can be managed within Unified CCDM; you cannot give a user rights to edit a particular item, but you can grant access to manage items within a particular folder.

It is recommended that you read through this entire document before planning your folder structure.

Managing Folders

System Manager enables you to create, edit, move and remove folders from the tree structure.

How to Create a New Folder

1. Click **Tools > System Manager > Select Create a Folder**.
2. The folder tree-structure is displayed in the left panel with the create-new-folder screen to the right.
3. Select the location of your new folder in the tree. For example, click on a folder which will act as the new folder's parent.
4. Enter the new folder's Name and Description.



Note

It is not possible to edit the name of a folder once it has been created.

5. Clear the **Inherit Permissions** check box if you require the new folder to have a different set of security permissions to those of its parent folder. If *all* users who can see the parent folder and perform tasks within it will be able to perform the same tasks in the new folder then you can leave the check box selected so that security settings will be inherited.

6. Click **Save**. The new folder is created in the selected location in the hierarchical tree structure.



You can create several folders in the same location. Select the **Create Another** check box to repeat the process.

Unified CCDM allows you to create any number of folders and any number of folder levels within the hierarchical tree. It is recommended however, for optimal performance and ease of maintenance, that you do not create any more than seven levels of folder beneath the tenant folder.

Policy Roots and Inheriting Permissions

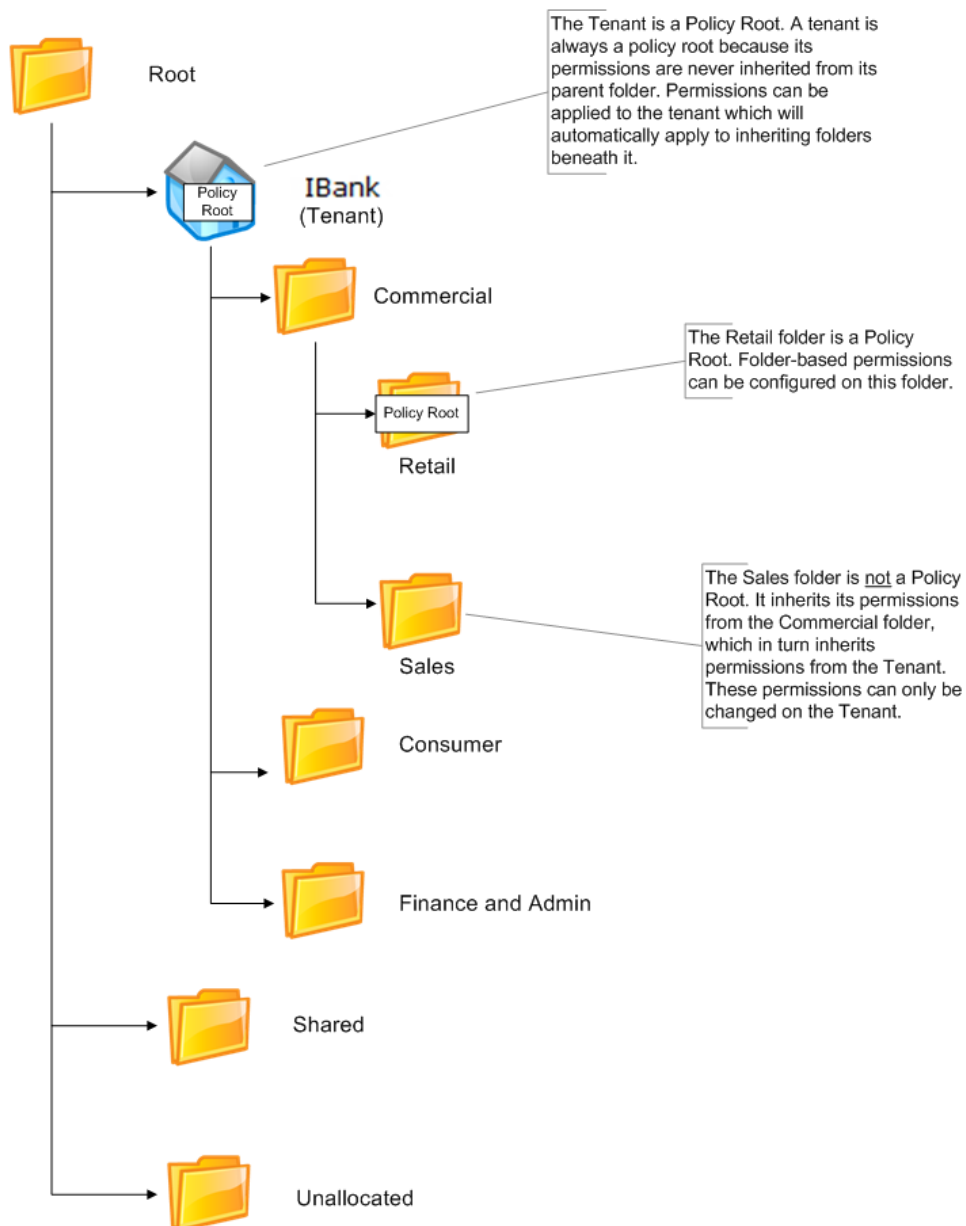
When creating a folder, the default behavior is for the folder to inherit the security settings of its parent. The security settings applied to the parent folder will also apply to the new folder. Any changes made to those roles and security settings are then cascaded down the folder-tree to all inheriting folders. Subsequently, it is not possible to change the security on an inheriting folder.

Alternatively, you can enable a folder to begin a new set of permissions, which its sub-folders may also inherit. A folder which does not inherit its security settings is referred to as a *Policy Root*. By definition, the Root folder and the tenant folder are always Policy Roots. Figure 3.1 shows a typical folder-tree with policy roots labelled.

Policy Roots enable you to create a new configurable set of permissions on a folder. Inheriting folders carry identical security permissions to their parent policy root folders, unless this chain of inheritance is 'broken' (by creating a Policy Root).

Note that the policy root labels shown here are for illustrative purposes only these labels do not appear in the Unified CCDM user interface.

Figure 3.1 Policy Roots and Inheriting Folders



You can use the Security Manager tool to determine whether a folder is a policy root. Click **Security Manager**, and navigate to the folder you want to look at. The right-hand panel displays folder security information. Under the **Permissions** tab, the permitted users and their roles are displayed, along with a check box indicating whether or not that folder inherits permissions from its parent. Additionally, the security roles are displayed dimmed for folders that inherit permissions and are not policy roots. These permissions cannot be changed at this level.

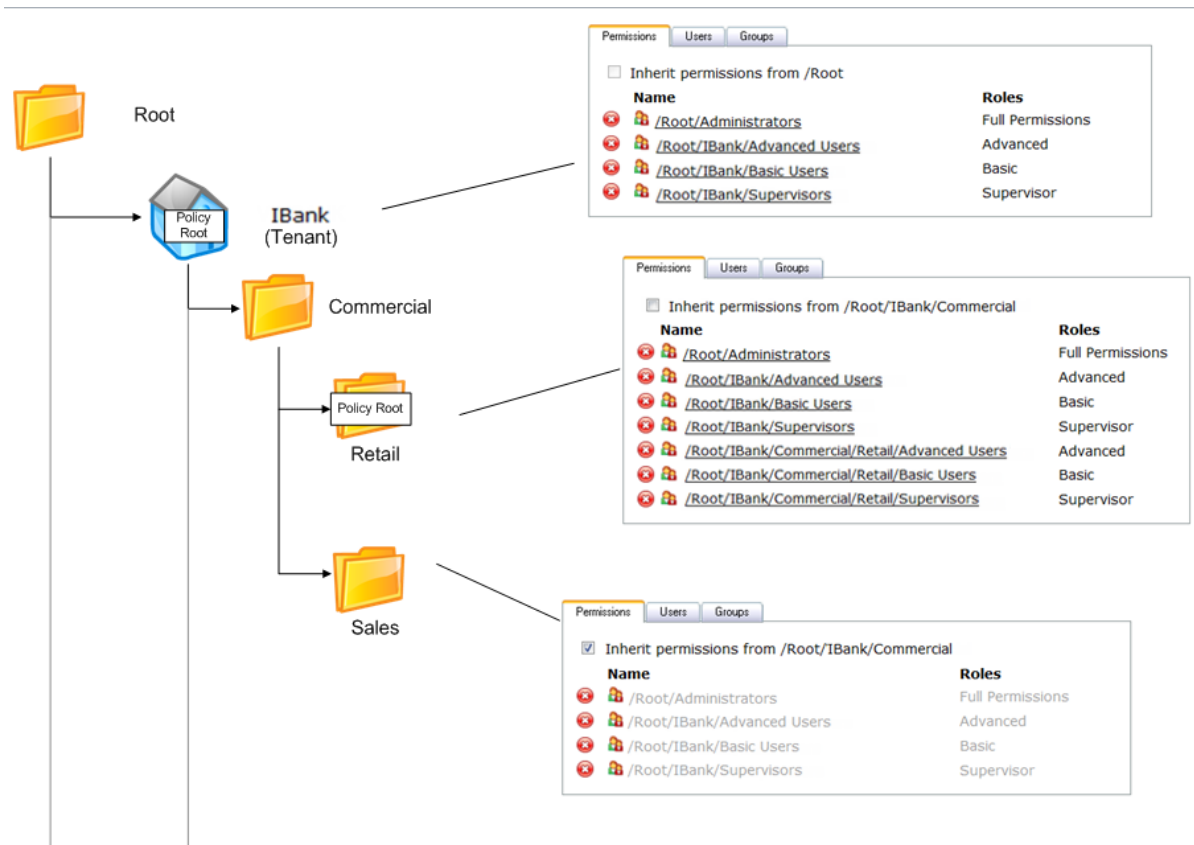
To create a new policy root, clear the **Inherit Permissions** checkbox to break inheritance for the selected folder. To set a folder to inherit its security settings, select the **Inherit Permissions** checkbox on the Permissions tab in Security Manager.



When inheritance is broken, and a new policy root folder is created, any permissions that were previously applied to that folder (by inheritance) will be explicitly applied to the folder so that existing users' permissions on that folder are not affected.

Figure 3.2 shows the folder tree structure with the **Permissions** tab displayed for some of the folders. Note that the roles are dimmed on the Sales folder. This is because you cannot edit the roles on a folder that inherits its permissions from another folder.

Figure 3.2 *Inherited Folders and Policy Roots*



The Shared Folder

The **Shared** folder is a unique folder which, by default, is accessible to everyone on the system. This is achieved by the automatic inclusion of all new users to the **Everyone** group, which, by default, has the basic folder-role on the Shared folder.

The Shared folder can be managed in the same way as any other folder on the system. You can create folders within the Shared folder and indicate whether or not security settings are inherited. In this way you can create and distribute resources within the Shared folder, restricting access to certain users or groups.



4. Managing Security

Creating Users and Groups

Security in Unified CCDM operates on the basis of roles, which are applied to users, giving them a set of tasks, either on a specified folder, or globally across the system. Rather than setting a role for each individual user, you can also apply a role to a collection, or **group** of users.

Groups can be user-defined and located within a folder, or created automatically when a new policy root folder is added to the system. These default groups enable security to be set up quickly, providing permissions that users will most commonly require on their specified folders.

How to Create a User

Unified CCDM treats user accounts in a similar way to resources. That is, each user account is contained within a specific folder, and users with appropriate permissions enabled on that folder can change the user's properties (such as the password) or move or delete the account.

Each user has a home folder that they can use to store their own reports and parameter sets. The home folder is usually the default selected folder when a user opens a Unified CCDM tool which contains a folder tree.



Note

The home folder can be a different folder to that which contains the user account. For example, you might create a user in the folder `Users/Atlanta`, but set their home folder to be `Resources/Atlanta`

To create a new user:

1. Click **Tools>Security Manager > User Manager**. The folder-tree structure is displayed in the left panel, with details of users in the selected folder displayed to the right.

2. Select the folder in which your new user's account will be stored. Existing users are displayed with their **Name, Description, Last Logged In** time and **Last Modified** time.
3. Click **New** on the menu bar.
4. The **Create a new user page** will be displayed. Enter the user's details
 - **Login Name:** username.
 - **First Name:** user's first name.
 - **Last Name:** user's last name.
 - **Email:** user's email address.
 - **Description:** any explanatory text.
 - **Advanced Mode:** select if the user is to be assigned global roles, providing access to advanced mode tools such as System Manager.
 - **Enabled:** account enabled. The user will be stored in Unified CCDM but will be unable to login until the enabled check box is selected.
 - **Text Only Mode:** displays Unified CCDM in text-only mode.
 - **User must change password at next login:** prompts user to change password after first login.
 - **Password Never Expires:** password is assigned indefinitely. The user will not be prompted to change it.
 - **User cannot change password:** prevents the new user from changing their password. The password can still be changed by an administrator.
 - **User Home Folder:** location of the user's home folder. The user will start here when logging in. If the User Home Folder field is left blank, the folder in which the user is created will become the home folder by default. Use the **Browse** button to locate the correct folder, or enter the path.

**Tip**

Select the **Create a new folder for this user** check box to create a new folder for the user's home folder. The user is given the role of 'My Reports' on this folder by default. A different default home folder role can be configured on the **Settings > Security Settings** page.

- **Password:** user's initial password.
 - **Confirm Password:** user's initial password.
5. Click **Save** to create the new user.

How to Create a Group

The procedure for creating a group is very similar to creating a user.

1. Click **Tools > Security Manager > Group Manager**. The folder-tree structure is displayed in the left panel, with the groups belonging to the currently selected folder displayed on the right.
2. Select the folder in which you want to create the new group.
3. Click **New** in the menu bar. The Create a new user group page is displayed.
4. Enter the **Name** and **Description** of the group.
5. Click **Save**. The group is added to the selected folder.



You can create several groups at a time. Select the **Create Another** check box to repeat the process.

Managing Group Memberships

Groups are a useful mechanism to quickly apply a collection of permissions to a user or another group. Managing security in this way means that you need only change the permissions for the group to update the permissions of all the group's members.

There are three ways to manage group memberships in Unified CCDM:

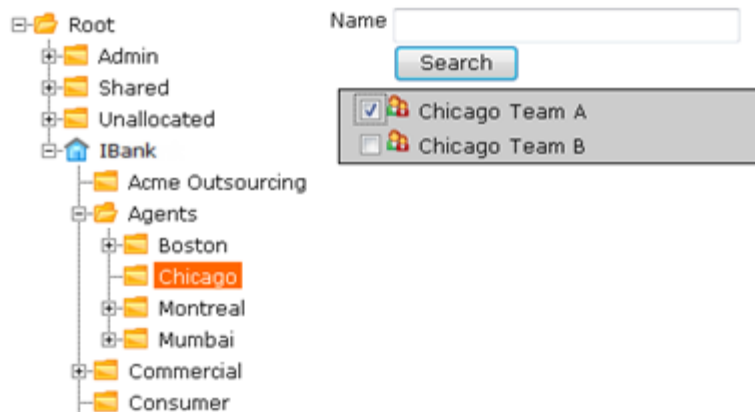
- Add users to groups using the User Manager when you want to add a single user to one or more groups.
- Use the Group Manager when you want to add a single group to one or more groups.
- You can also add multiple users and groups to a single group using the Group Manager.

How to Add Users to Groups

1. Click **Tools > Security Manager > User Manager**. The folder-tree structure is displayed in the left panel, with the details of users in the currently selected folder displayed on the right.
2. Select the required folder.
3. Select the user name of the user you require from the list.
4. The user's details are displayed.
5. Click the **Groups** tab. A list is displayed showing all the groups the selected user already belongs to (see Figure 4.1). In this example, the user belongs only to the Everyone group, to which all new users are automatically added.

Figure 4.1 *The Groups to which a User Belongs*


6. Click **Add to Group**. A dialog box is displayed, showing the selected folder in the tree-structure, and the groups available for the user to join. In this example the selected user is being added to the group Chicago Team A (in the Chicago folder) by selecting its check box.

Figure 4.2 *The Groups a User Can Join*

7. Use the folder tree to find the folder containing the group to which you wish to add your user. Select the checkbox of the required group. You can add the user to several groups if required. Use the folder tree to change location if you want to add the user to groups in other folders.

8. Click **Close**. The group memberships you have chosen to create will be listed for review.



Use the remove button  to cancel any of the pending group memberships.

9. Click **Save** to finalize the changes.

How to Add a Group to Other Groups

In addition to being able to add users to groups, you can also add groups to other groups. This can be useful if you wish to create a group that has a subset of permissions which it derives from another group.

To add group A to group B.

1. Click **Tools > Security Manager > Group Manager**. The folder-tree structure is displayed on the left, with group details displayed in the right panel.
2. Select the folder of the group you want to add (A).
3. The groups belonging to the selected folder are displayed with their Details and Last Modified dates.
4. Click the group you require (A).
5. The group's details are displayed under three tab headings: Details, Members and Groups.
6. Click the **Groups** tab.
7. The group's membership of other groups is displayed along with an Add to Group button.
8. Click **Add to Group**.
9. A dialog box is displayed, showing the folder-tree structure and groups corresponding to the folder selected in the tree.
10. Select the folder of the group you wish to add to (B). The list of groups is displayed.
11. Select the check box of group B.
12. Click **Close**. The group of which group A is now a member (group B) is displayed in the membership list.
13. Click **Save** to finalize the changes.



You cannot add a group to a group which is already a member of the first group, or any of its associated groups. In other words, if group B is a member of group A (or group A's existing groups), you cannot add group A to B. The Group Manager tool displays a message indicating that a *violation check constraint* has been encountered.

How to Add Multiple Members to a Single Group

In addition to being able to assign a user to a particular group or groups, you can also navigate to the group and add members to it using Group Manager.



To add multiple members to a group:

1. Click **Tools > Security Manager > Group Manager**. The folder tree structure is displayed on the left with groups in the selected folder displayed in the right panel.
2. Locate the folder in which your group is stored.
3. The groups within the selected folder are listed.
4. Click the required group. Group details are displayed with Details, Members and Groups tabs.
5. Click the **Members** tab. Existing members of the group are listed (including users and groups)
6. Click **Add Members**. A dialog box is displayed, showing the folder-tree structure and users/groups in the selected folder.
7. Find the folder in which your user (or group) is located using the folder structure.
8. Users and groups within the selected folder are displayed.
9. Select the users you want to add to the group using the check boxes. You can repeat step 6 and 7 to add multiple users.
10. Click **Close**. The new users (and groups) are added to the list of members.
11. Click **Save** to finalize the changes.

Assigning Global Permissions

In addition to the permissions that can be applied to a user or group to perform a task within the context of a specific folder, Unified CCDM also has permissions that are global in nature. For example, a user can be given access to a tool such as System Manager or Security Manager.

To apply a global role to a user or group:

1. Click **Tools>Security Manager> Global Security Manager**. The list of global roles is displayed.
2. Click the role you wish add a user or group to. Details of the selected role are displayed with Details, Tasks and Members tabs.
3. Click the **Members** tab. A list is displayed, showing all the users  and  groups currently assigned with the selected role.
4. Click the **Add Members** button. A dialog box displays the folder-structure on the left and users and groups on the right.
5. Select the folder in which your user or group is located.
6. The available users and groups correspond to the selected folder.

**Tip**

Use the **Name** field and **Search** button to find the user or group you require. You can also use the Type drop-down to filter your search to just **Users**, just **Groups** or both **Users and Groups**.

7. Select the checkbox adjacent to the groups or users you require.
8. Click **Close**. The new user or group is added to the list.
9. Click **Save** to finalize the changes.

**Caution**

If you want to delegate user creation and some elements of security management to other users, but you do not want to allow them to manage global security, you can achieve this by creating a group that is a member of the relevant global roles and allowing the user to add members to that group, rather than allowing them to manage global security directly. This avoids the situation where a user who needs to create new users with the System Advanced role also has the capability to grant users other global roles and tasks such as Manage Site.

Assigning Folder-Based Permissions

Whereas global roles affect users' activity across the system, folder roles are applied to groups or users, and impact the activity of users within specific folders.

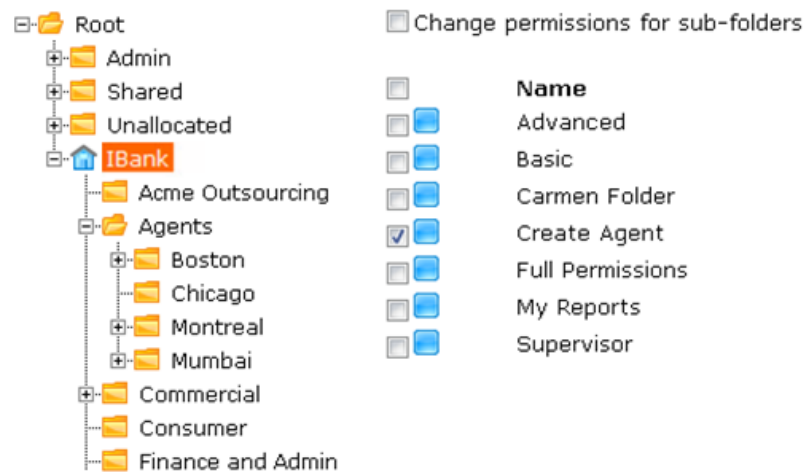
Each folder has a set of configured permissions either inherited from its parent folder, or applied to the folder itself as a policy root.

How to Add Folder Permissions to a User or Group

Folder roles apply to the user or group only within a specific folder. This folder is selected during the process of applying the role as shown below.

1. Click **Tools > Security Manager**. The folder-tree is displayed in the left panel, with security details displayed to the right, corresponding to the selected folder.
2. Select the folder in which your user or group is located. The folder's security details are displayed under the Permissions, Users and Groups tab.
3. If you are applying the role to individual users, select the **Users** tab. If you are applying the role to a group (or groups) of users, select the **Groups** tab. All the users or groups in the folder are displayed.
4. Select the checkbox of the user(s) or group(s) you want to apply the role to. The Clear Selections and Change Permissions buttons are activated.
5. Click **Change Permissions**. A dialog box is displayed showing the folder-structure and roles available for the selected folder (see Figure 4.3). The dialog box displays available roles with check boxes, enabling you to select any number of roles to apply to your users/groups on the selected folder.

Figure 4.3 Applying Roles to Users and Groups



6. Select the folder on which you want to apply the role.
7. Select the checkbox of the role you wish to apply to the user/group.
8. You can repeat steps 6 and 7 if you want to apply several roles on different folders.
9. When you have finished setting roles for your user or group, click **Save**. The dialog box displays the changes you have made to the security role settings.
10. If you are happy with the configuration, click **Confirm**.

Editing Security on Folders That Inherit Permissions

The example in Figure 3.2 above shows a folder tree with both inheriting and policy root folders, with the roles applied to each using Security Manager. You cannot apply a new folder role to a folder which inherits permissions from another folder. You can either apply the desired permission to the policy root folder or you can ‘break inheritance’ and make the folder a policy root itself.

If you attempt to edit security settings on a folder that inherits permissions from a parent, you will see the message in Figure 4.4.

Figure 4.4 Security Settings Error Message

This folder is currently inheriting permissions. To edit permissions on this folder select the button below.

Clicking **Edit Item Security** will allow you to make the folder you have selected a policy root, enabling you to edit security on the folder. Any sub-folders will now inherit their permissions from the new policy root, and any previously inherited permissions will automatically be applied explicitly to the folder. See Chapter 3, Policy Roots and Inheriting Permissions for more information.



Appendix A. Roles and Tasks

Roles are a collection of tasks which can be carried out by a user of Unified CCDM. This section describes the function of each of the available tasks.

Folder-based Tasks

Roles can be applied to a specific folder; so that users assigned the folder-based role have access to the task-based permissions specified only for that folder. The following table lists the tasks available to create a folder-based role, using **Security Manager > Role Manager**. The **B**, **S**, and **A** columns indicate whether the task is enabled by default for these pre-configured roles in Unified CCDM. The roles in your Unified CCDM system may differ from the list here if they have been edited since the system was installed. Some tasks may not be licensed for use in your Unified CCDM system.

Note that a folder task permission allows the user to perform a task on a folder, but, in most cases a global role is also required to provide access to a tool with which to perform the task. For example, the Manage Dimensions folder task permission allows the user to manage dimensions in a folder, but the global task permission, System Manager, is also needed to allow the user to locate the required dimension and perform the update.

| Task Name | Comments | B | S | A |
|------------------------|--|---|---|---|
| Folder Settings | | | | |
| Browse Folders | Allows the user to see a folder in the folder tree. For example, when creating a parameter set, a user needs Browse Folders to navigate to the location of their resources, and Browse Dimensions on the folder where the resources are located. | ✓ | | ✓ |
| Manage Folders | Allows the user to edit, create and remove folders in the specified folder. | | | ✓ |

| Task Name | Comments | B | S | A |
|---------------------------|---|---|---|---|
| Users and Security | | | | |
| Browse Users | Allows the user to view the details of all users in the specified folder. For example, if the user has access to the Security Manager/User Manager tool, the Browse Users task allows them to view users and their details in a particular folder. | ✓ | | ✓ |
| Manage Users | Allows the user to modify settings of users within the specified folder. For example, if the user has access to the Security Manager/User Manager tool, the Manage Users task allows them to view and edit users in a particular folder. | | ✓ | ✓ |
| Reset Passwords | Allows the user to reset the passwords of other users within the specified folder. For example, if the user has access to the System Manager tool and access to Browse Users in a particular folder, the Reset Passwords task allows them to reset the password of those users, but not edit other user details such as Username. | | | ✓ |
| Manage Tenants | Allows the user to manage tenant items within the specified folder. | | | |
| Manage Security | Allows the user to modify security permissions on the selected folder. Access to the Security Manager tool is also required. | | | ✓ |
| Reporting | | | | |
| Browse Reports | Allows the user to browse, select and run reports in the specified folder. Requires access to the Reports page which is available to all users by default. If the user has access to the System Manager tool then Browse Reports will also allow them to view report objects in folders that they can access in the System Manager folder tree. The Basic Mode interface displays a flat list of all reports that the user has Browse Reports access to in folders beneath the /Shared folder. | ✓ | | ✓ |

| Task Name | Comments | B | S | A |
|--------------------------------|---|---|---|---|
| Manage Reports | Allows the user to create, modify and delete reports within the specified folder. For example if the user has access to the System Manager tool then they can move, delete and edit the properties of reports they can access via the System Manager folder tree. | ✓ | | ✓ |
| Browse Parameter Sets | Allows the user to browse and select parameter sets in the specified folder, when running reports or via the Report Manager and System Manager tools | ✓ | | ✓ |
| Manage Parameter Sets | Allows the user to create, modify or remove Parameter Sets in the specified folder, using either the Reports tool or via System Manager. | ✓ | | ✓ |
| Dimensions and Prefixes | | | | |
| Browse Dimensions | Allows the user to list system resources (Agents, Skill Groups, Call Types etc.) in the specified folder. For example, this permission is necessary for a user to see dimension items in order to create Parameter Sets. When viewing an item in System Manager, such as an Agent, Browse Dimensions is required on the folder in which the Agent is located. Items to which the agent has a membership, such as a Skill Group or Agent Team will be visible in the Agents detail tabs, even if the user does not have Browse Dimensions on their location as the Browse Dimension permission allows a user to see an item's memberships. However, if the user does not have Browse Dimension permission on the location of the membership items, they will not be able to click through using the Go To button to view details of those items. | ✓ | | ✓ |
| Manage Dimensions | Allows the user to edit, move and delete dimensions, such as Agents, Agent Teams or Skill Groups, in the specified folder using System Manager. The user will not be able to delete or reskill an Agent if the Agent has memberships to an item in another folder (on which the user does not have permissions). | | ✓ | ✓ |
| Manage Dimension Memberships | Allows the user to add, modify and delete dimension memberships. | | | |
| Clone Dimensions | Allows the user to copy agents. | | ✓ | |

| Task Name | Comments | B | S | A |
|----------------------------|--|---|---|---|
| Browse Prefixes | Allows the user to browse automatic resource movement prefixes in the specified folder on the Prefix details tab of a Tenant item in the System Manger tool | | | ✓ |
| Manage Prefixes | Allows the user to add and remove automatic resource movement prefixes in the specified folder, using the Prefixes tab of a Tenant item in the System Manger tool | | | |
| Information Notices | | | | |
| Browse Information Notices | Allows the user to list and view information notices within the specified folder via the Information Notices and System Manager tools. If a user has Browse Information Notices permissions on their home folder then notifications for currently active information notices located in their home folder and every parent folder up to and including the tenant folder will be displayed on the user's home page. | ✓ | | ✓ |
| Manage Information Notices | Allows the user to create information notices (for users in the specified folder) via the Information Notices and System Manager tools. Information notice options are displayed on the user's homepage, provided they have been given the global permission to access Information Notices. | | | ✓ |
| Uploading | | | | |
| Upload Media | Allows the user to upload files to the specified folder through System Manager. | | | ✓ |
| Uploading | | | | |
| Manage Search Folders | Allows the user to create, modify and delete search folders and searches. | | | |

Global Role Tasks

Global roles, such as Basic, Advanced, Host and System Administrator are applied to users or groups of users, enabling them to access the same set of functions on all the folders to which they have access. The following table displays a list of all available tasks configurable for a global role, accessed through **Security Manager > Global Security Manager**.



The **Basic (B)** and **Advanced (A)** columns indicate the default settings for these roles in a new installation of Unified CCDM.

| Global Task Name | Comments | B | A |
|------------------------|---|---|---|
| Information Notices | Displays the Information Notices tool on the tools page. | | ✓ |
| Reports | Displays the Reports tool and Report options on the user's tools page. | ✓ | ✓ |
| Security Manager | Displays Security Manager and Security Manager options on the user's tools page. | | ✓ |
| Service Manager | Displays Service Manager on the tools page. | | ✓ |
| System Manager | Displays System Manager on the tools page. | | ✓ |
| Advanced User | Displays a checkbox on the user settings page, enabling access to Advanced User mode, which displays the tools page on start-up. | | ✓ |
| Manage Site | Allows the user to save system settings, security settings, reporting settings and provisioning settings on the Settings page. | | |
| Self Skill | Allows users to view and edit their own skill groups. | | |
| Browse Roles | Allows the user to view folder-based roles within Role Manager and Security Manager. | | ✓ |
| Manage Roles | Allows the user to create, modify and delete folder-based roles within Security Manager > Role Manager. | | |
| Browse Global Roles | Allows the user to view global roles in Global Security Manager. | | ✓ |
| Manage Global Roles | Allows the user to add, modify and delete global roles using Global Security Manager. | | |
| Browse Global Security | Enables Global Security Manager within the Security Manager tool on homepage. Access is view only. Roles are unable to be edited. | | ✓ |

| Global Task Name | Comments | B | A |
|----------------------------------|---|---|---|
| Manage Global Security | Displays the Global Security Manager option within Security Manager tool on the tools page, enabling the user to view and edit global security roles. | | |
| Browse Dimension Types | Allows the user to select dimension types (such as Agent or Call Type) from an Item Type drop-down, when creating a Parameter Set in Reports. | ✓ | ✓ |
| Bulk Import Dimensions | Allows the user to upload csv files containing dimensions such as agents, through the upload menu on the items panel in System Manager. | | ✓ |
| Provision Agent | Allows the user to create and manage an Agent via System Manager, or Agent Team Manager, provided the user has also been granted permission to Manage Dimensions on the specified folder, and Browse Connected Systems is enabled. | ✓ | ✓ |
| Provision Agent Desktop | Allows the user to add an Agent Desktop, through the New > Resource Items menu within System Manager, provided the user has also been granted permission to Manage Dimensions on the specified folder, and Browse Connected Systems is enabled. | | ✓ |
| Provision Agent Team | Allows the user to add an Agent Team item to a folder, through the New > Resource Items menu within System Manager. | ✓ | ✓ |
| Provision Call Type | Allows the user to add a new Call Type to a folder via the System Manager, New > Resource Items menu. | | ✓ |
| Provision Device Profile | Allows the user to manage device profiles. | | ✓ |
| Provision Dialed Number | Allows the user to provision new Dialed Numbers. | | ✓ |
| Provision Directory Number | Allows the user to provision new directory numbers. | | ✓ |
| Provision Enterprise Skill Group | Allows the user to provision new Enterprise skill groups. | | ✓ |
| Provision Expanded Call Variable | Allows the user to create an Expanded Call Variable and manage its settings and active dates, through System Manager > New Resource. | | ✓ |

| Global Task Name | Comments | B | A |
|-------------------------|---|---|---|
| Provision IP Endpoint | Allows the user to provision IP endpoints from the remote equipment. | | ✓ |
| Provision Label | Allows the user to create Labels for specific label creation through System Manager > Resource Folder > Resource Item. | | ✓ |
| Provision Person | Allows the user to provision a Person via System Manager or Service Manager, provided the user has also been granted permission to Manage Dimensions on the specified folder, and Browse Connected Systems is also enabled. | ✓ | ✓ |
| Provision Service | Allows the user to provision and manage a service, including setting Service Level Type, associated Skill Groups and peripherals, using System Manager. | | ✓ |
| Provision Skill Group | Allows the user to manage skill groups using System Manager, Skill Group Manager (within Service Manager) provided the user has also been given permission to Manage Dimensions on the folder where the skill group is located. | ✓ | ✓ |
| Provision User Variable | Allows the user to provision a user-defined variable, using System Manager. | | ✓ |

Example Usage

This section describes combinations of folder-based and global security tasks required to carry out some typical usage scenarios within Unified CCDM.

| Scenario | Task | Where? | Why? |
|-----------------|-----------------------------------|---|--|
| Create an Agent | System Manager or Service Manager | Global | To access to the create agent menus. |
| | Manage Dimensions | Folder in which the new Agent is to be created. | In order to create the Agent in the specific folder |
| | Provision Agent | Global | In order to provision the Agent to UCCE |
| | Browse Dimensions | Folders containing items which need to be associated with the | In order to allow the creation of the Agent's memberships. |

| Scenario | Task | Where? | Why? |
|---|-----------------------------------|--|---|
| | | agent, for example, Peripherals, Teams, Skill Groups and Agent Desktops. | |
| Create a user and allocate non-default permissions | System Manager | Global | To access the functionality to create users. |
| | Manage Users | Folder in which new user is to be created. | To create the new user in the specific folder. |
| | Security Manager | Global | To access the functionality to change permissions for the new user. |
| | Manage Security | Folder in which new user is to be created. | To change the permissions for the new user. |
| | Browse Global Roles | Global | To access the permissible global roles. |
| | Browse Roles | Global | To access the permissible folder roles. |
| Reskill-only permissions (for example, for a supervisor user) | System Manager or Service Manager | Global | To access System Manager or Skill Group Manager tool. |
| | Browse Folders | Folder containing agent and folder containing skill group to be assigned to agent. | To access agent and new skill group. |
| | Manage Dimensions Memberships | Folder containing agent and folder containing skill group to be assigned to agent. | To modify the agent and skill group details. |
| | Provision Agent | Global | To provision the agent change to UCCE. |
| | Provision Skill Group | Global | To provision the skill group change to UCCE. |