Staging Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.6(1)

First Published: 2021-05-14

Americas 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: 408 527-0883

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 1994–2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface ix

Change History ix

About This Guide ix

Audience x

Related Documents x

Communications, Services, and Additional Information x

Field Notice x

Documentation Feedback xi

Conventions xi

CHAPTER 1

Active Directory and ICM/CCE 1

Active Directory for Unified ICM/CCE 1

Active Directory Support by Unified CCE 2

Benefits of Active Directory 2

Support for Corporate Domain Installations 2

No Domain Administrator Requirement 2

Flexible and Consistent Permissions 2

Streamlined Administration 2

Standard Windows Naming Conventions 3

Active Directory and Microsoft Windows Server 3

Active Directory Domain Services 3

RWDC Authentication 3

RWDC LDAP Read 3

Restartable Active Directory Domain Services 3

Single Sign On (SSO) Support 4

CHAPTER 2 **Domain Requirements and Supported Topologies** 5

Microsoft Active Directory Tools 5

Run dcdiag.exe 6

Run repadmin.exe 7

Domain Requirements 8

Requirements for Group Policy in AD 8

Group Policy Overview 9

Group Policy Settings 9

Unified ICM Server Domain Requirements 9

Block Policy Inheritance 10

Prevent Use of Improper Policies 10

Install the Administration Client on a Different Domain in a Single Forest 10

DNS Requirements 11

Global Catalog Requirements 11

Supported Topologies 12

Multiple Forests Not Supported 13

Single Forest, Single Tree, and Single Domain Benefits and Usage Scenarios 13

Single Domain Model 13

Advantages of Single Domain Model 14

Single Domain Topology Design 14

Single Tree Multiple Child Domains 16

When to Add Additional Domains 16

Multiple-Tree Topology 19

Multiple Tree Forests 19

Multiple Trees in a Single Forest Model 20

Business Requirements 20

When to Choose a Multiple Tree Domain Model 20

Additional Considerations for Topology Design 21

Single Domain 21

Single Tree, Multiple Domains 21

Single Forest, Multiple Trees 22

Additional Considerations 22

Domain Name System 22

Configure Active Directory Sites 23
Assign Global Catalog and Configure Time Source 24

CHAPTER 3 Organization Units 27
What Is an OU? 27
OU Hierarchies 27
Cisco Root OU 28
Facility OU 29
Instance OU 29
Unified ICM Instance OU 29
Security Groups 30
Security Groups and OUs 30
Security Groups Described 30
Security Group Names and Members 31
Config Security Group 32
Setup Security Group 32
OU Hierarchies and Security 33
Service Security Group 36

CHAPTER 4 User Migration Tool 39
User Migration Tool Prerequisites 39
User Migration Tool Features 40
Migration Scenarios 40
Internationalization (I18n) and Localization (L10n) Considerations 41
Security Considerations 41
User Migration Steps 41
Export Users from the Source Domain 42
Import Users into the Target Domain 42
Change Domain Name 43
User Migration Tool Modes 43
Mode Considerations 45
Export Mode 45
Import Mode 46
Verify Mode 47

Content Parameter Descriptions 47
Users from Trusted Domains 48
User Migration Tool Troubleshooting 49
User Migration Tool Error Messages 49

CHAPTER 5 **Service Account Manager 51**
Service Account Management 51
Other Considerations 51
Permissions 51
Domain Restriction 51
Local Group Update Failures 52
Logging 52
Service Account Manager End User Interfaces 52
Service Account Manager GUI Dialog Boxes 52
Service Account Manager – Main Dialog Box 52
Service Account Manager – Edit Service Account dialog box 58
Command Line Interface for Service Account Manager 58
Silent Setup for Default Service Accounts 58
Service Account Manager 59
Update Existing Account for Single Service 59
Update existing account for more than one Service 60
Fix Account Displaying Adverse Health State 60

CHAPTER 6 **Prepare to Work with Active Directory 61**
Perform Preliminary Steps 61
Domain Manager and OU Hierarchy 61

CHAPTER 7 **Domain Manager 63**
Domain Manager Tool Functionality 63
Open the Domain Manager 64
Domain Manager Window 64
View Domains 67
Add Domain to a View 68
Remove Domain from a View 69

Create or Add Cisco Root 69
Remove Cisco Root 71
Create or Add Facility OU 72
Remove Facility OU 72
Create Instance OU 73
Remove Instance OU 74
Security Groups 74
Add Users to Security Group 76
Remove Members from Security Group 78
Organizational Unit Validation Errors Dialog Box 78

CHAPTER 8 **Local Machine Authorizations** 81
UcceService Group 81
UcceConfig Group 81
Local Administrators Group 81

CHAPTER 9 **Staging Prerequisites** 83
System Design Specification 83
Platform Hardware and Software 84
Set Staging Environment 85

CHAPTER 10 **Microsoft Windows Server Staging** 87
Drive Partition Guidelines 87
Logger or Administration and Data Server Partition Guidelines 87
Partition Guidelines for Other Contact Center Components 88
Windows Setup Guidelines 88
Enable SNMP Management on Microsoft Windows Server 89
Join Standalone Servers to Domain in Microsoft Windows Server 89
Set Persistent Static Routes 90
Collect Existing SNMP Properties 90
Display Settings 92
System Properties 92
Configure Event Viewer 93
Connectivity Validation 93

APPENDIX A **Domain Controller Installation on MS Windows Server** 95
Install Domain Controller on Microsoft Windows Server 95

APPENDIX B **Moving the Cisco Root OU** 97
Introduction 97
Definitions 97
Cisco Root OU 97
Domain Manager 97
Requirements and Prerequisites 97
Preparatory Steps 98
Transfer Cisco Root OU to Another OU 98

Preface

- Change History, on page ix
- About This Guide, on page ix
- Audience, on page x
- Related Documents, on page x
- Communications, Services, and Additional Information, on page x
- Field Notice, on page x
- Documentation Feedback, on page xi
- Conventions, on page xi

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

Changes	Section	Date
Initial Release of Document for 12.6(1)		May, 2021

About This Guide

This document contains system diagrams, staging steps and sample test cases for supported models of Unified ICM/CCE. The supported models are:

- Dedicated Forest/Domain Model
- Child Domain Model

Note This document is for individuals responsible for staging deployments of Cisco contact centers. Individuals must be trained on the use and functions of Unified ICM/CCE as well as Microsoft Windows Server, Active Directory (AD), and DNS. This document does not provide detailed Cisco Unified Intelligent Contact Management Enterprise (Unified ICM) or Microsoft Windows Server specific information. You can find this information elsewhere in specific documentation from Cisco or Microsoft.

Audience

Individuals utilizing this document must have knowledge and experience with the following tools/software/hardware to stage the system software as described in this document:

- Cisco Unified ICM Scripting and Configuration Tools
- Third-party software (if installed)
- Microsoft Windows Server and Windows Active Directory administration
- Microsoft SQL Server administration

Related Documents

Document or Resource	Link
Cisco Unified Contact Center Enterprise Installation and Upgrade Guide	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices
- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at https://cway.cisco.com/mynotifications.

Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

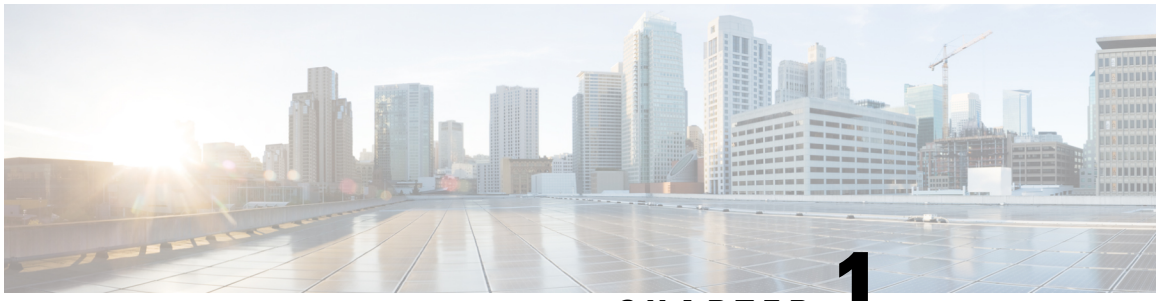
Conventions

This document uses the following conventions:

Table 1: Conventions

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • A syntax value that the user must replace. Example: IF (*condition*, *true-value*, *false-value*) • A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.

Convention	Description
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems, Inc. </title></html>`
`< >`	Angle brackets are used to indicate the following: • 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.



CHAPTER 1

Active Directory and ICM/CCE

- Active Directory for Unified ICM/CCE, on page 1
- Active Directory Support by Unified CCE, on page 2
- Benefits of Active Directory, on page 2
- Active Directory and Microsoft Windows Server, on page 3
- Single Sign On (SSO) Support, on page 4

Active Directory for Unified ICM/CCE

Microsoft Windows Active Directory (AD) is a Windows Directory Service that provides a central repository to manage network resources. Based on the registry settings, Unified ICM uses AD to control user access rights to perform setup, configuration, and reporting tasks. AD also grants permissions for different components of the system software to interact; for example, it grants permissions for a Distributor to read the Logger database.

This document provides details of how the system software uses AD.

Note This document does not provide detailed information on AD. Unified ICM administrators must be familiar with the Microsoft AD. See Microsoft documentation for details on Microsoft AD.

Note This guide uses the term “Unified ICM” to generically refer to Cisco Unified Contact Center Enterprise (Unified CCE) and Cisco Unified Intelligent Contact Management (Unified ICM). You can use either Unified CCE or Unified ICM for advanced call control, such as IP switching and transfers to agents. Both provide call center agent-management capabilities and call scripting capabilities. Scripts running in either environment can access Unified CVP applications.

Note Unified CCE no longer creates or deletes Active Directory user accounts. You can manage these user accounts within their active Directory infrastructure.

Active Directory Support by Unified CCE

Unified ICM/CCE supports active directory on Windows Server. For detailed information on supported versions for Unified ICM, see:

- *Virtualization for Unified Contact Center Enterprise* at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html
- *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html

Benefits of Active Directory

Support for Corporate Domain Installations

Use the existing AD functionality in your network to control access to Unified ICM functions by co-locating Unified ICM in an existing Windows domain (except the domain controller). Control access to functions in an existing Windows domain, including the corporate domain, and utilize the AD functionality your network already supports. Decide where to place the collocated resources in your Organizational-Unit (OU) hierarchy.

Related Topics

What Is an OU?, on page 27

No Domain Administrator Requirement

You only need to be a local machine administrator to belong to the setup group for any VM for which you are installing a component.

You can determine which users in your corporate domain have access rights to perform specific tasks with the Domain Manager.

For more information, see the chapter Domain Manager.

Flexible and Consistent Permissions

The OU hierarchy allows you to define a consistent set of permissions for users to perform configuration, scripting, and reporting tasks.

You can grant these privileges to any trusted AD user.

Streamlined Administration

Unified ICM uses AD to control permissions for all users so that administrators do not need to enter redundant user information. Unified ICM relies on AD for setup, configuration, and reporting permissions.

Standard Windows Naming Conventions

AD supports standard Windows naming conventions.

By default, there are no specific naming requirements for the Unified ICM usernames or the domain name. Certain features, like SSO, can impose requirements. For more information on the feature, see the *Cisco Unified Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html

Active Directory and Microsoft Windows Server

Unified ICM/CCE supports Active Directory on Microsoft Windows Server. Unified ICM/CCE does not support Read Only Domain Controller (RODC) in its deployments.

See Microsoft documentation for details on setting up Windows Server.

Active Directory Domain Services

Active Directory Domain Services form the core area for authentication of user configuration information. Active Directory Domain Services also hold information about objects stored in the domain.

RWDC Authentication

The Unified ICM/CCE application user must be authenticated if the client machines are connected to Read Write Domain Controller (RWDC).

RWDC LDAP Read

Unified ICM/CCE must perform the LDAP read operation successfully when the client is connected to RWDC. LDAP Read operations happen when Unified ICM/CCE Configuration applications read the data from the Active Directory. Unified ICM/CCE issues LDAP ADSI calls to perform this.

Restartable Active Directory Domain Services

You can stop and restart the Active Directory Domain Services without restarting the domain controller.

Currently, appropriate error messages are not shown because we do not check the running of Active Directory Domain Services and its dependent services before performing the Active Directory related operations.

Because Unified ICM/CCE does not use the Microsoft Windows Server LDAP library, no error displays when you restart Active Directory Domain Services.

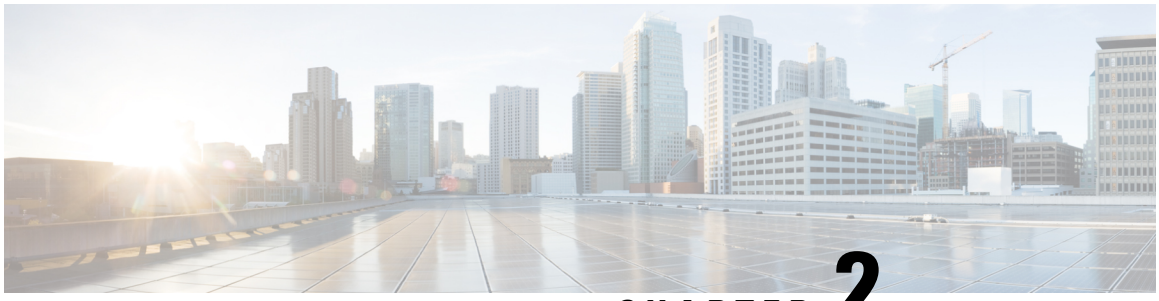
Single Sign On (SSO) Support

Note Unified CCE no longer creates or deletes Active Directory user accounts. You can manage these user accounts within thier Active Directory infrastructure.

Single sign-on (SSO) is an authentication and authorization process. (Authentication proves that you are the user you say that you are, and authorization verifies that you are allowed to do what you are trying to do.) SSO allows users to sign in to one application and then securely access other authorized applications without a prompt to reenter user credentials. As an agent or supervisor, when you login to a Unified CCE solution web component using a username and password, SSO provides a security token that allows you to securely access all other web based application and services without providing your login credentials repeatedly from the same web browser instance. By using SSO, Cisco administrators can manage all users from a common user directory and enforce password policies for all users consistently. If you move to a different browser you need to re-authenticate the SSO.

To enable SSO, the Unified CCE Solution requires an Identity Provider (IdP) to interface with Microsoft Active Directory (AD). The IdP stores user profiles and provides authentication services to support SSO sign-ins to the contact center solution. However, the IdP does not replace AD. Irrespective of the IdP used to interface with the identity source, the Active Directory infrastructure is a mandatory component for SSO because AD is still required to support Unified CCE administrator sign-ins.

For detailed information about SSO in the contact center solution, see the *Cisco Unified Contact Center Enterprise Features Guide*.



CHAPTER 2

Domain Requirements and Supported Topologies

- Microsoft Active Directory Tools, on page 5
- Run dcdiag.exe, on page 6
- Run repadmin.exe, on page 7
- Domain Requirements, on page 8
- Requirements for Group Policy in AD, on page 8
- DNS Requirements, on page 11
- Global Catalog Requirements, on page 11
- Supported Topologies, on page 12
- Domain Name System, on page 22
- Configure Active Directory Sites, on page 23
- Assign Global Catalog and Configure Time Source , on page 24

Microsoft Active Directory Tools

Before you install Unified ICM in a new or existing AD environment, ensure that the environment is stable. As a rule, for all domain controllers in a forest, monitor replication, server, and AD health daily using the Microsoft System Center Operations Manager or an equivalent monitoring application. For information about using Operations Manager to monitor AD, see the *Operations Manager Monitoring Scenarios* for the current version of Operations Manager on the Microsoft TechNet website.

Microsoft provides several tools that you can use to ensure AD health and connectivity and that your environment is ready for Unified ICM. Some of the tools which you can use to check the health are as follows:

- dcdiag
- repadmin

Table 2: Microsoft AD Tools

Tool	Purpose	Command Line
dcdiag.exe	• Generates a report on AD health. • Verifies connectivity, replication, topology integrity, inter-site health, and trust verification. • Checks Network Card (NC) head security descriptors, net logon rights, and roles. • Locates or gets the domain controller.	`dcdiag /v /e /f:dcdiag.txt` **Note** Run this tool on the enterprise domain.
repadmin.exe	• Retrieves the replication status of all domain controllers in a spreadsheet. • Verifies DNS infrastructure, Kerberos, Windows time service (W32time), remote procedure call (RPC), and network connectivity.	`repadmin /showrepl * /csv >showrepl.csv`

Note Your network administrator or a qualified AD expert (for example, Microsoft Support Services), should evaluate the reports that these tools generate.

After you install the tools, run the following setups:

- dcdiag.exe
- repadmin.exe

Run dcdiag.exe

Procedure

Step 1 Choose **Start** > **Run**.

Step 2 Type **cmd**.

Step 3 Press **Enter**.

A command console opens.

Step 4 At the prompt, enter **dcdiag.exe /e /v /f:dcdiag.txt**.

Note If you use the /e option, run dcdiag.exe at the root level. If you do not use the "/e" option, run dcdiag.exe on each individual domain controller.

The application creates the text file dcdiag.txt in the folder containing dcdiag.exe.

Step 5 Open the text file and note any items that are prefaced with "Warning" or "Error."

Step 6 Correct all the issues, then rerun dcdiag.exe to ensure that no issues remain.

Run repadmin.exe

Procedure

Step 1 Choose **Start** > **Run**.

Step 2 Type **`cmd`**.

Step 3 Press **Enter**.

A command console opens.

Step 4 At the prompt, enter **`repadmin.exe /showrepl * /csv >showrepl.csv`**.

Step 5 Open Excel and choose **File** > **Open**.

Note Depending on your version of Excel, the menu cascades may be slightly different.

Step 6 In the "Files of type" section, click **Text Files (*.prn;*.txt;*.csv)**.

Step 7 In the "Look in" section, navigate to *showrepl.csv*, then click **Open**.

Step 8 In the Excel spreadsheet, right-click the column heading for showrepl_COLUMNS (column A), then click **Hide**.

Step 9 In the Excel spreadsheet, right-click the column heading for Transport Type, then click **Hide**.

Step 10 Select the row just under the column headings, then choose **Windows** > **Freeze Pane**.

Step 11 Click the upper-left corner of the spreadsheet to highlight the entire spreadsheet. Choose **Data** > **Filter** > **AutoFilter**.

Step 12 In the heading of the Last Success column, click the **`down arrow`**, then click **Sort Ascending**.

Step 13 In the heading of the Source DC column, click the **`down arrow`**, then click **Custom**.

In the Custom AutoFilter dialog box, complete the custom filter as follows:

a. Under Source DC, click **does not contain**.

b. In the corresponding text box, enter **`del`** to filter deleted domain controllers from the spreadsheet.

Step 14 In the heading of the Last Failure column, click the **`down arrow`**, then click **Custom**.

In the Custom AutoFilter dialog box, complete the custom filter as follows:

a. Under Last Failure, click **does not equal**.

b. In the corresponding text box, enter `0` to filter for only domain controllers that are experiencing failures.

For every domain controller in the forest, the spreadsheet shows the following:

- Source replication partner
- The time that replication last occurred
- The time that the last replication failure occurred for each naming context (directory partition)

Step 15 Use Autofilter in Excel to view the replication health for the following:

- Working domain controllers only
- Failing domain controllers only
- Domain controllers that are the least, or most recent

You can observe the replication partners that replicate successfully.

Step 16 Locate and resolve all errors.

Step 17 Rerun repadmin.exe to ensure that no issues remain.

Domain Requirements

Warning The Domain Controller and DNS servers can not be co-located on any Unified ICM component and must be installed on a separate server.

Warning The UCCE servers should be in the same domain, and multiple domains are not supported.

Unified ICM Requirements for AD:

- Authenticated users require credentials of a domain account with write privileges to the ICM OU.
- Microsoft AD tools or Domain Manager are the only supported tools for provisioning AD.
- You cannot create Unified ICM servers in the Unified ICM OU hierarchy.
- You can only apply the Unified ICM group policy template to OUs containing the Unified ICM servers.
- Single-label DNS domain names (such as “ICM”) are not supported when you use them with Unified ICM/CCE. Multi-part names such as ICM.org, ICM.net, ICM.com, or sales.ICM.org are acceptable.

Note For additional information, see Information about configuring Windows for domains with single-label DNS names.

- Requires no AD schema changes. Authenticated users require read access to the contents of AD.

Requirements for Group Policy in AD

Group Policy plays a pivotal role in AD management. Group Policy directly affects the function of distributed applications like Unified ICM. This section explains Group Policy and defines requirements to ensure proper functioning of your Cisco applications related to Unified ICM servers.

Group Policy Overview

Administrators can manage computers centrally through AD and Group Policy. Using Group Policy to deliver managed computing environments allows administrators to work more efficiently because of the centralized, 'one-to-many management' it enables. Group Policy defines the settings and allows actions for users and computers. It can create desktops that are tailored to user job responsibilities and level of experience with computers. Unified ICM uses this centralized, organized structure to help ease the administrative burden and create an easily identifiable structure for troubleshooting. However, some settings can adversely affect Unified ICM and the Unified ICM servers ability to function. Therefore, you must control the OU structure for Unified ICM components and ensure adherence to a standard.

Group Policy Settings

Administrators use Group Policy to define specific configurations for groups of users and computers by creating Group Policy settings. These settings are specified through the Group Policy Object Editor tool (known as GPedit.msc) and are present in a Group Policy Object (GPO), which is in turn linked to AD containers (such as sites, domains, or OUs). In this way, Group Policy settings are applied to the users and computers in the AD containers. For more information on Group Policy management, see *Group Policy Management Console* at https://technet.microsoft.com/en-us/library/cc753298(v=ws.11).aspx.

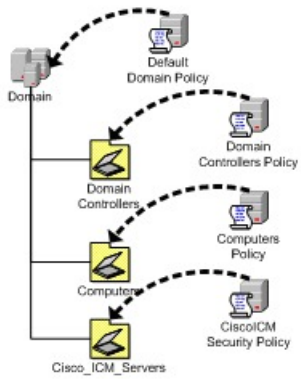
Caution Do not perform group policy updates during production hours as it may impact CVP/UCCE services.

Unified ICM Server Domain Requirements

You can move all Unified ICM servers into a separate OU to ensure proper functioning of the Unified ICM application and to improve security. You must clearly identify the OU as Cisco_ICM_Servers (or a similar clearly identifiable name) and documented in accordance with your corporate policy.

Note Create this OU either at the same level as the computer or at the Cisco ICM Root OU. If you are unfamiliar with AD, engage your Domain Administrator to assist you with Group Policy deployments.

Figure 1: Group Policy Deployments



After you apply the Group Policy to the OU, you must prevent propagation of default or custom Group Policies to this OU. You can use block inheritance to prevent this propagation. For details, see Block Policy Inheritance, on page 10.

Verify that a global Enforced policy is not applied in the domain. For details, see Prevent Use of Improper Policies, on page 10.

You cannot block enforced GPO links from the parent container.

Block Policy Inheritance

You can block inheritance for a domain or organizational unit. Blocking inheritance prevents Group Policy objects (GPOs) that are linked to higher sites, domains, or organizational units from being automatically inherited by the child-level. If a domain or OU is set to block inheritance, it appears with a blue exclamation mark in the console tree.

Procedure

Step 1 In the Group Policy Management Console (GPMC) console tree, double-click the forest containing the domain or organizational unit (OU) for which you want to block inheritance for GPO links.

Step 2 To block inheritance for an OU, double-click **Domains**, double-click the domain containing the OU, and then right-click the OU.

Step 3 Choose **Block Inheritance**.

Prevent Use of Improper Policies

You must prevent improper policies from being propagated. If the Enforced option is selected in a Group Policy Object being applied to a Cisco OU, a parent object enabled the option, which takes precedence over block policy inheritance. You must uncheck the Enforced option on all parent OUs or Group Policy Objects.

Procedure

Step 1 Select a parent OU or Group Policy Object from the Group Policy Management console tree.

The Default Domain Policy opens in the right pane.

Step 2 In the **Links** section, locate the domain, and note whether the **Enforced** option is enabled (**Yes** if enabled, **No** if not).

Step 3 If the option is enabled, right-click on **Yes** and deselect the **Enforced** option.

Install the Administration Client on a Different Domain in a Single Forest

You can install the Administration client on a different domain other than the Central Controller domain within a single forest.

Before you begin:

- A transitive trust must exist between the Administration client domain and Central Controller domain.
- An ICM domain user from the Central Controller domain must be granted local administrator privilege on the Administration client machine.

Note The following steps are only required when the AdminClientInstaller is in a different domain than the Central Controller.

Procedure

Step 1 Log in to the Administration client machine using the credentials from the Central Controller domain user, which is a part of local administrators group.

Step 2 Find the fully qualified domain name of the Central Controller domain.

Step 3 Install the Administration client.

Step 4 Launch the Administration client setup.
The Log in page appears.

Step 5 Log in with your Active Directory user name and password.
The log in fails because you are attempting to log in from a non-UCCE domain.

Step 6 Log in again with your Active Directory user name and password and the fully qualified UCCE domain name that you obtained in step 2.
You will now be able to log in to the Administration client.

DNS Requirements

The following are DNS requirements:

- AD Integrated Zone for both forward and reverse lookup zones.
- Enterprise level Standard Secondary Zone for the Unified ICM Child Domain model or the Unified ICMH Domain model.
- Manually add all additional addresses (high, privates, private highs, and so forth) to the forward lookup zone in DNS along with associated PTR records.
- Corporate DNS servers have forwarding enabled to the AD servers (if using Corporate DNS servers as opposed to the Domain Controllers for name resolution).

Global Catalog Requirements

In a multi-domain forest, a Global Catalog is required at each AD site. The Global Catalog is a central repository of domain information in an AD forest. A significant performance degradations and failure happen without

the local or Global Catalog. It is important for every AD query to search each domain in the forest. The multi-site deployments are required to query across WAN links.

Contact center enterprise solutions use the Global Catalog for Active Directory. All domains in the AD Forest in which the Unified CCE Hosts reside must publish the Global Catalog for that domain. This includes all domains with which your solution interacts, for example, Authentication, user lookup, and group lookup.

Note This does not imply cross-forest operation. Cross-forest operation is not supported.

Supported Topologies

Unified ICME systems support the following AD topologies:

- Single Domain
  - Unified ICM in the Corporate domain
  - Unified ICM in a child domain of the Corporate domain
  - Unified ICM as a standalone domain
  - Unified ICM as a tree root

A forest is a collection of AD domains that provide a namespace and control boundary within AD.

systems support the following AD topologies:

- Single Domain
  - Customer HDSs in a single domain
- Single Forest, Single Tree
  - You can have an Administration client in a different domain from the Unified ICM/CCE instance in the same tree.
- Single Forest, Multiple Tree

Note You can have an Administration client in a different domain from the Unified ICM/CCE instance in the same tree.

Use the following example to determine how your domain structure looks before installing the Domain Controller.

This information is intended for the individuals responsible for:

- Configuring the AD Domain and Forest Topologies
- Staging new deployments of on Microsoft Windows Server

You must train the administrators of your system on the use and functions of:

-
- Microsoft Windows Server
- AD
- DNS

This section does not provide detailed Unified ICME or Microsoft Windows Server specific information. You can find this information elsewhere in Cisco and Microsoft documentation. Individuals using this document must have at least intermediate knowledge and experience with AD.

The ability to integrate Unified ICM into existing infrastructures is one of the premises of Unified ICM. You can mitigate the impact that the unique environments in these existing infrastructures have on Unified ICM with minor adjustments to the support schema.

For more information, see the chapter Organizational Units.

Multiple Forests Not Supported

"Multiple forests" means two or more forests in a given environment that share resources through manually created trust relationships. All Unified CCE nodes, services, and users must reside in the same AD forest.

For additional information, see Security Guide for Cisco Unified ICM/Contact Center Enterprise.

Use Microsoft Services or third-party Microsoft partner professional services to mitigate any Microsoft specific issues that might arise, as domain topologies vary.

Single Forest, Single Tree, and Single Domain Benefits and Usage Scenarios

The following are the benefits of using Single Forest, Single Tree, and Single Domain:

- Benefits
    - Simple setup
    - High stability
    - Smallest AD footprint
    - Least deployment-to-complexity ratio
    - Easiest support profile
- Sample usage scenarios
    - Enterprise Deployment

Single Domain Model

This type of domain structure has one major advantage over the other models: simplicity. A single security boundary defines the borders of the domain and all objects are located within that boundary. You do not need to establish trust relationships between other domains, so you can easily run Group Policy.

When designing the new Active Directory structure from a multiple domain NT style structure, it was generally believed you could not consolidate on a single domain model. AD changes this. The capacity to span multiple domains in a single forest is improved and simplified.

Advantages of Single Domain Model

The single domain model is ideal for many Unified ICM deployments. The first advantage of a single domain structure is simplicity. When you add unnecessary complexity to a system architecture you introduce potential risk, and make it difficult to troubleshoot. A simpler, single AD domain structure reduces the administration costs and minimizes setbacks.

Another advantage is centralized administration. Organizations with a strong central IT structure want the capability to consolidate their control over their entire IT and user structure. Because NT domains were not able to scale to these levels, the central control that organizations wanted was not available. Now, AD and the single domain model allow for a high level of administrative control, including the capability to delegate tasks to lower sets of administrators.

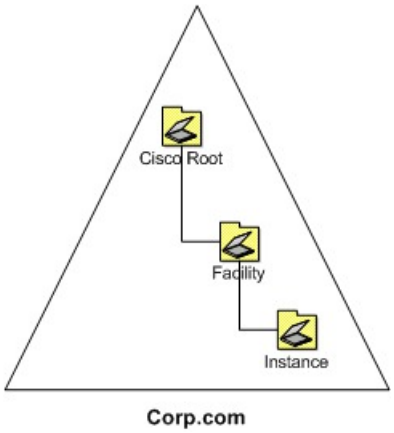
Unified ICM benefits from this design because AD traversal queries are limited to the single domain. As a result, request processing time is reduced. AD controls access and provides security which dramatically improves the overall performance of Unified ICM.

Single Domain Topology Design

Design is the most important aspect of any AD deployment. Follow Microsoft planning and design technical documentation to ensure a smooth transition.

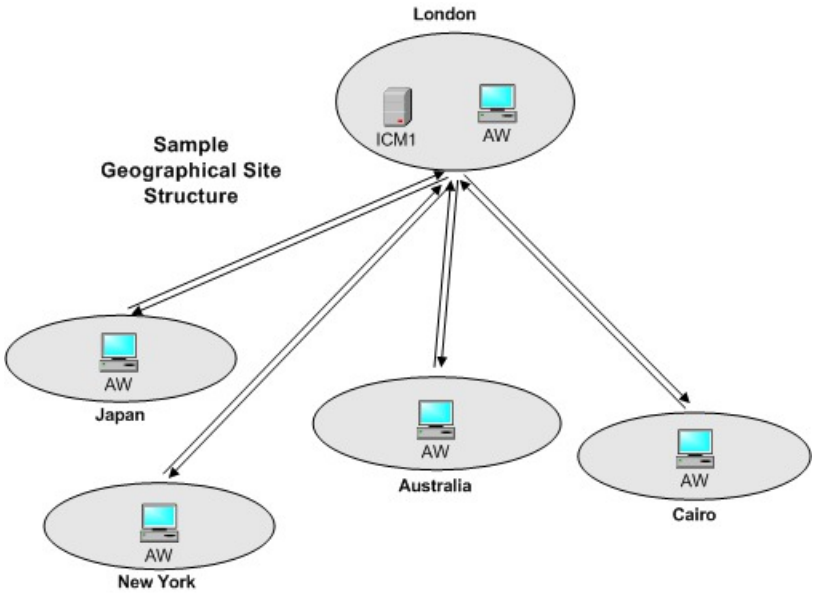
Delegation of password-change control and other local administrative functions can be granted to individuals in each specific geographical OU. The delegation of administrative functions provides administrators with permissions specific to the resources within their own group while maintaining central administrative control in the root OU.

Figure 2: Sample Single Domain Layout



You can create several AD sites to control the frequency of replication. Position a site to correspond with a separate geographical area, creating a site structure similar to the one shown in the following figure.

Figure 3: Site Organization by Geographical Location

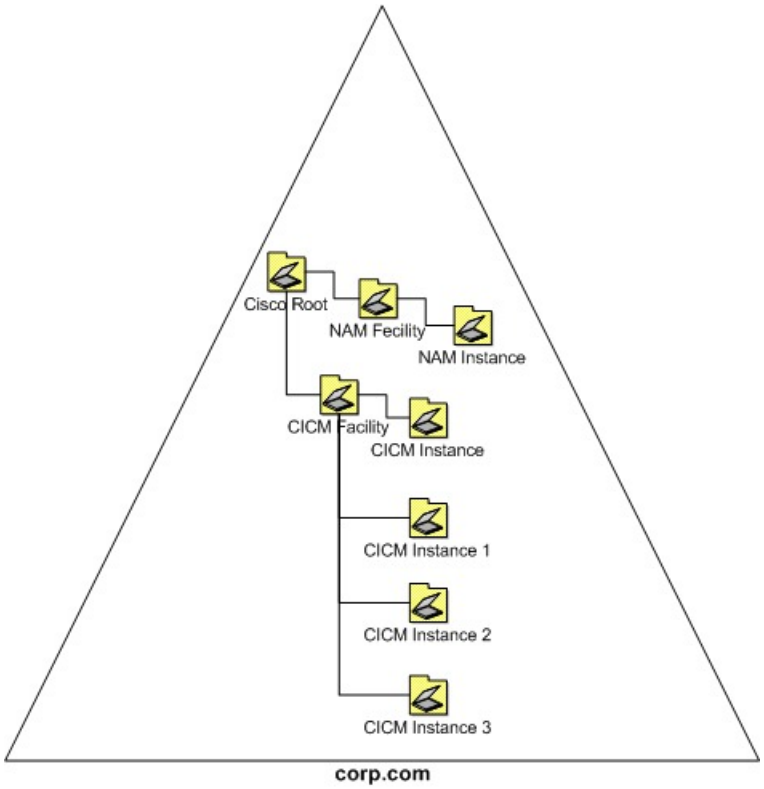


Create separate sites to help throttle replication traffic and reduce the load placed on the WAN links between the sites. For more details about site links and replication, see How Active Director Replication Topology Works.

This type of single domain design is ideal for both large and small organizations. Multiple domain use is reduced as delegation of administration is now accomplished by using OUs and Group Policy objects, and the throttling of replication is accomplished through AD sites.

Hosted scenarios have many instances deployed in various ways (such as geographically, client size, or however this model fulfills your needs). The following figure shows an example domain layout.

Figure 4: Hosted OU Structure for Single Domains



A single-domain design enables AD to manage access to the domain using Group Policies, Kerberos, and ACLs. This greatly simplifies administrative overhead and provides an increased return on investment for the entire organization.

For more information, see the chapter Organizational Units.

Single Tree Multiple Child Domains

Some deployments of systems require Unified ICM to be installed in more than one domain. Sometimes the addition of one or more child domains into the forest is necessary. Keep in mind that a Unified ICM system must be in a single domain, even when you install ICM in more than one domain. When adding a domain to the forest, consider the particular characteristics of multiple domain models.

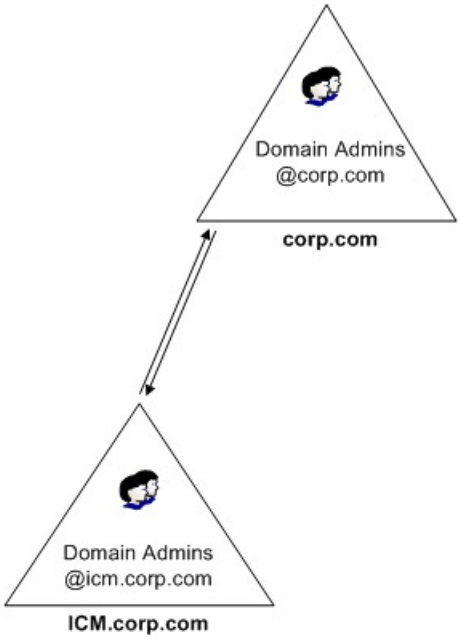
By default, two-way transitive trusts exist between the child domain and the parent domain in AD. However, this two-way transitive trust does not mean that resource access is automatically granted to members of other domains. For example, a user in the child domain is not automatically granted any rights in the parent domain. Explicitly define all rights by using groups. Understanding this concept helps to determine the requirements of domain addition.

When to Add Additional Domains

Begin design with a single domain and only add domains when necessary. If your infrastructure needs decentralized administration, you may need to add child domains to your existing domain structure. Multiple interconnected domains may be useful if your organization requires its own IT structure to manage Unified ICM, and there are no plans to consolidate the domains into a centralized model. A domain acts as a security

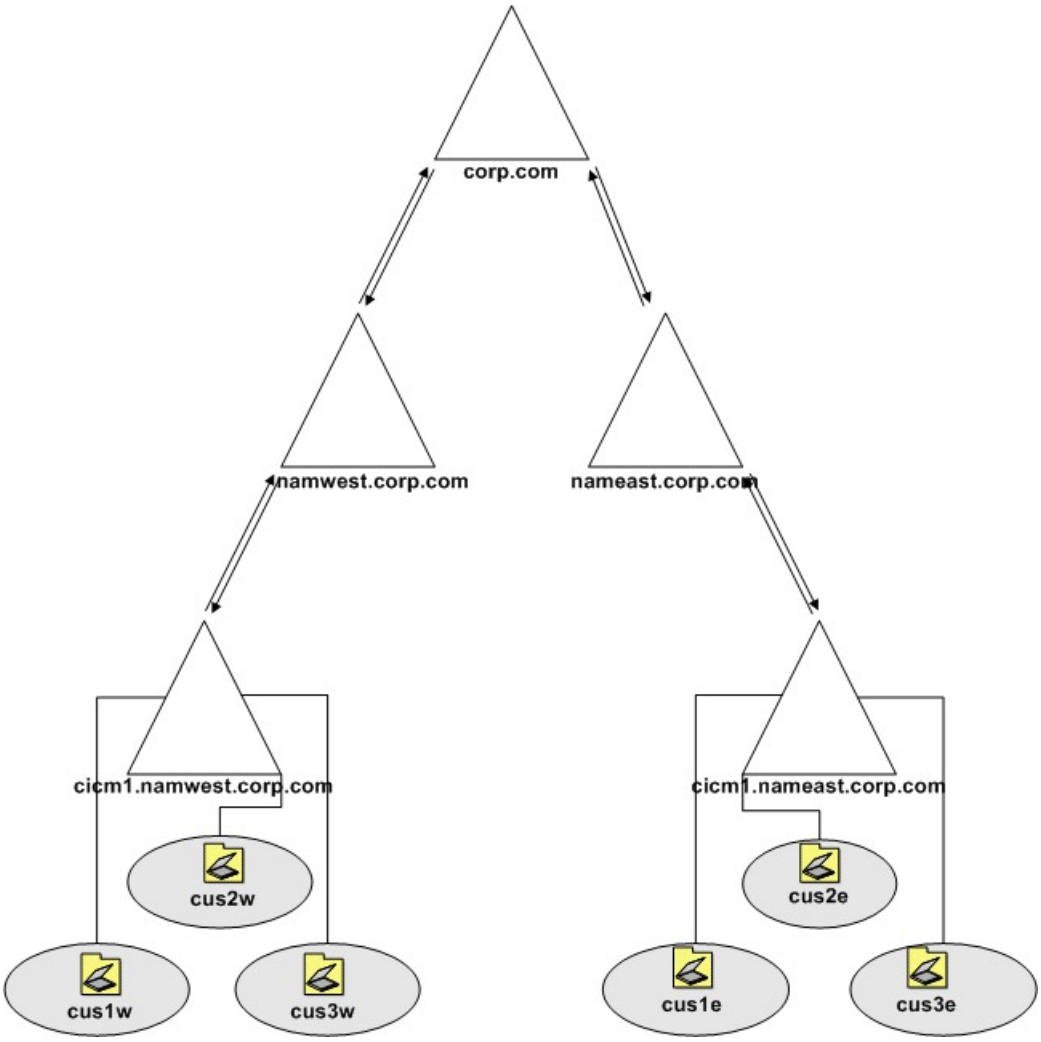
boundary for most types of activities and blocks administration from escaping the boundaries of the domain. NT domains inherit many of their associated limitations. This design approach operates in much the same way. Try to centralize administration before you deploy AD because you gain more AD advantages. AD advantages include centralized management, a simpler deployment model, simplified user and group management, and enhanced operability. The following figure demonstrates the default boundary in this topology. Assign the rights to give the user access to resources in the parent domain.

Figure 5: Active Directory Boundaries



If geographic limitations (such as extremely slow or unreliable links), segment the user population into separate groups. This segmentation helps to limit replication activity between domains and makes it easier to provide support during working hours in distant time zones. AD sites throttle replication across slow links. Slow links by themselves do not mean you must create multiple domains. Administrative flexibility is the main reason to create a domain for geographical reasons. For example, if you experience a network problem in Asia, a local administrator has the power and resources to administer the Asia domain. You do not need to contact a North American administrator.

Figure 6: Regional Domains

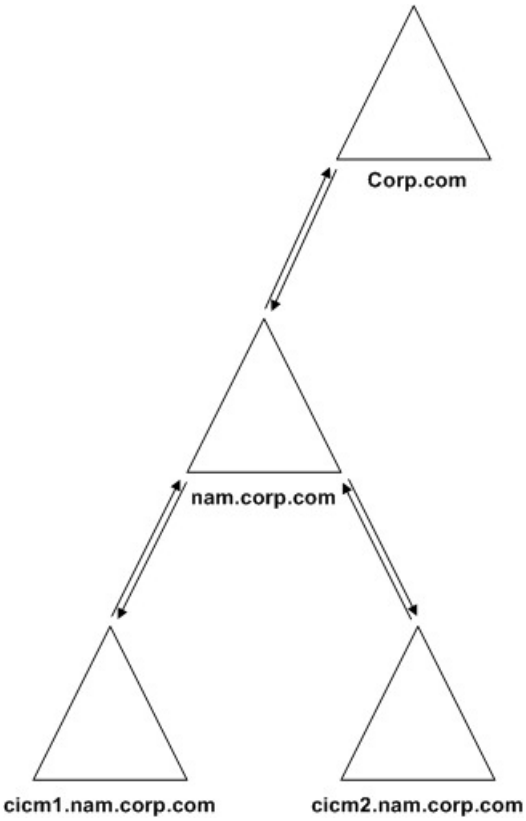


The single tree multiple child domain model allows each region to perform its own administration, creating an easily distributed and flexible topology. This domain model allows for a wide support base with immediate incident response. It also keeps the deployment clean and logical.

For Unified ICM, the addition of multiple child domains retains some of the old familiarity of NT4 topologies but gives an ease of delegation. This topology appeals to some service providers.

The single tree multiple child domain topology provides a contiguous namespace where the DNS domain names relate to the naming convention.

Figure 7: Contiguous Namespace



The flexibility in this model is apparent. However, you must be familiar with your organization requirements for a distributed, collaborative application such as Unified ICM. Use the simplest possible topology that meets your requirements.

Related Topics

Domain Name System, on page 22

Multiple-Tree Topology

A single forest with multiple trees and disjointed namespaces is a complex AD topology. This configuration can consist of one or more root domains, and one or more child domains.

Multiple Tree Forests

A forest is established when you create the first AD domain. This domain is known as the forest root. In a forest, any domains sharing a contiguous namespace form a tree. After a tree is established in a forest, any new domains added to an existing tree inherit a portion of its namespace from its parent domain.

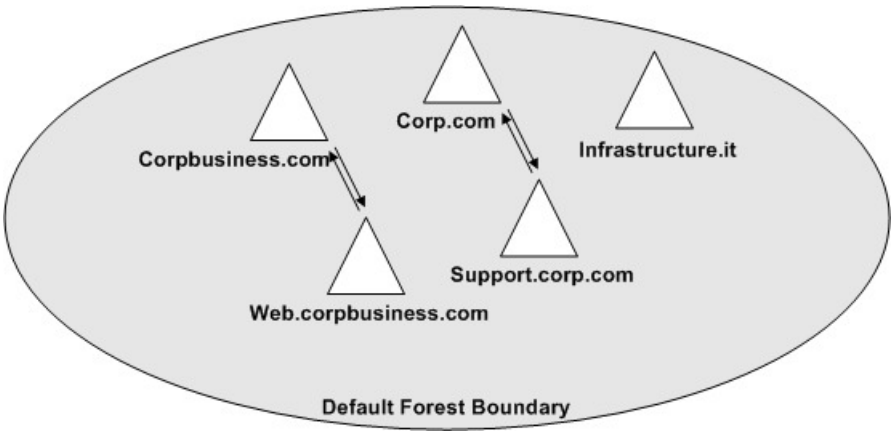
Any domain added to the forest that maintains a unique namespace form a new tree in the forest. An AD forest can consist of one or many trees in a single forest. In some instances, multiple trees are required so that a company can meet its business requirements.

Multiple Trees in a Single Forest Model

If your organization moves to an AD environment and uses an external namespace for its design, then you can integrate the external namespace into a single AD forest. Use multiple trees in a single forest to accommodate multiple DNS namespaces.

One of the most misunderstood characteristics of AD is the difference between a contiguous forest and a contiguous DNS namespace. You can integrate multiple DNS namespaces into a single AD forest as separate trees in the forest as indicated by the following figure.

Figure 8: Simple Multiple Tree Topology



Only one domain in this design is the forest root (Corp.com in the preceding figure). Only this domain controls access to the forest schema. All the other domains shown (including the subdomains of Corpbusiness.com, and the domains occupying different DNS structures) are members of the same forest. All trust relationships between the domains are transitive, and the trusts flow from one domain to another.

Business Requirements

Ensure that you plan a simple domain structure. If a business does not require multiple trees, do not increase the difficulty by creating an elaborate multiple-tree structure. However, sometimes multiple trees are required and this requirement is decided only after a thorough assessment of the business. When considering a multiple tree structure, keep the following requirements in mind:

DNS Names

If a business comprises of different subsidiaries, or has partnered with other businesses that maintain their distinct public identities as well as separate (noncontiguous) DNS names, you might have to create multiple trees in a single forest.

When to Choose a Multiple Tree Domain Model

If your organization currently operates multiple units under separate DNS namespaces, consider a multiple tree design. If you simply use multiple DNS namespaces, you are not automatically a candidate for this domain design. For example, suppose that you own five separate DNS namespaces. Then you decide to create an AD structure based on a new namespace that is contiguous throughout your organization. When you consolidate your AD under this single domain, you simplify the logical structure of your environment and keep your DNS namespaces separate from AD.

If your organization extensively uses its separate namespaces, consider the following design. Each domain tree in the forest can then maintain a certain degree of autonomy, both perceived and real. This type of design often satisfies branch office administrator needs.

The preceding domain design is logically more convoluted. Technically this domain design carries the same functionality as any other single forest design model. You set up all the domains with two-way transitive trusts to the root domain and share a common schema and global catalog. The difference is that they all use separate DNS namespaces. Reflect the separate DNS namespace use in the zones that exist on your DNS server.

Additional Considerations for Topology Design

The preceding sections provide a general overview of the considerations necessary when you choose a topology for Unified ICM in a corporate environment. Other considerations might arise, depending on a corporation's internal directives. The following topics include additional considerations for topology design.

Single Domain

In general, a Windows domain structure must be as simple as possible. The simplest approach is to create just one domain.

A single domain approach benefits:

- Most straightforward design
- Requires the least replication traffic
- Provides a minimum of administrative complexity
    - Requires the fewest domain administrators
    - Requires the fewest domain controllers
    - Allows administrative control at low levels in the domain by creating OUs and OU-level administrators—does not require a domain administrator to perform most tasks

Single Tree, Multiple Domains

A more complex structure is a root domain with domains beneath it.

Single tree, multiple domain approach provides the following benefit: the domain administrator of the root domain has complete power over the AD tree.

However, consider the following drawbacks when you use the single tree, multiple domain approach:

- More complex than a single domain
- Creates more replication traffic
- Requires more domain controllers than a single domain
- Requires more domain administrators than a single domain
- Setting tree-wide Group Policies requires using site Group Policy Objects (GPOs) or replicated domain/OU GPOs
- Tree could become complex if you create too many child domains

Single Forest, Multiple Trees

If the DNS names are contiguous for all domains in a forest, they can belong to a single domain tree. If their DNS names are not contiguous, create separate domain trees. So, if one domain tree is sufficient, there is no inherent need to create multiple trees.

Before using a single forest, multiple tree approach, consider the following drawbacks:

- Far more complex than a single domain
- Creates substantially more replication traffic
- Requires more domain controllers than a single domain
- Requires more domain administrators than a single domain
- Requires using site Group Policy Objects (GPOs) to set Group Policies

Additional Considerations

Security

Some organizations separate business units to provide security. This perception is a holdover from Windows NT4 where the domain boundary did provide the security. AD, however, provides layers of actual security. These layers are all customizable, and you can set them up in any of the supported topologies.

Corporate Directives

Many organizations have standard policies and procedures that they are accustomed to using as a Global standard. Unified ICM is a robust application and might be sensitive to some of these directives. For instance, some organizations have daily or weekly reboot policies for domain controllers. This situation requires a firm understanding of the effect AD has on the domain structure. If you turn all of the Domain Controllers off simultaneously, anything that relies on AD breaks. To avoid this problem, stagger the Domain Controller reboots so at least one domain controller per domain remains online at any given time.

Many variations and unique policies can impact Unified ICM. The procedures detailed in this guide delineate the best possible methods of deploying and maintaining Unified ICM. Review your company policies and compare them with the requirements established in this guide. If conflicts arise, correct them before deployment.

Domain Name System

AD integrates with the Domain Name System (DNS) as follows:

- AD and DNS have the same hierarchical structure.

  Although separate and run differently for different purposes, an organization namespace for DNS and AD have an identical structure.

- You can store DNS zones in AD.

  If you use the Microsoft Windows Server DNS Server service, you can store primary zone files in AD for replication to other AD controllers.

- AD uses DNS as a locator service, resolving AD domain, site, and service names to an IP address.

To log on to an AD domain, an AD client queries their configured DNS server for the IP address of the Lightweight Directory Access Protocol (LDAP) service running on a domain controller for a specified domain.

Note You can use dcdiag.exe to troubleshoot client computers that cannot locate a domain controller. This tool can help determine both server and client DNS mis-configurations.

While AD is integrated with DNS and shares the same namespace structure, it is important to understand their differences:

- DNS is a name resolution service.

  DNS clients send DNS name queries to their configured DNS server. The DNS server receives the name query and either resolves the name query through locally stored files or consults another DNS server for resolution. DNS does not require AD to function.

- AD is a directory service.

  AD provides an information repository and services to make information available to users and applications. AD clients send queries to domain controllers using the Lightweight Directory Access Protocol (LDAP). An AD client queries DNS to locate a domain controller. AD requires DNS to function.

Follow the Microsoft method for AD to create lookup zones and to configuring DNS servers:

- Select **AD Integrated Zone** for both forward and reverse lookup zones.
- Select the **Allow Dynamic updates** and **Only Secure updates** options.
- Limit zone transfers to trusted servers in and across domains in a forest only.
- Add Unified CCE supplementary addresses manually (high, private, private high) in DNS as a Host record. Always create a PTR record for manually added hosts.
- If you use Corporate DNS servers rather than the Domain Controllers for name resolution, ensure that the Corporate DNS servers have forwarding enabled to the AD servers.

Configure Active Directory Sites

On Unified ICM Root Domain Controller:

Procedure

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **AD Sites and Services**.

Step 2 Rename the default first site name as per AD Site Plan in Unified ICM System Diagram.

a) For a geographically separated DC, right-click **Sites**.
b) Select **New Site**.
c) Enter the site name of the additional domain controller based on the Unified ICM System Diagram.

Step 3 Create subnets for each DC site:

a) Right-click the Subnets folder and select **New Subnet**.
b) Enter the subnet address and mask, respective to the LAN at the Domain Controller Site.
c) Highlight the Site Name associated with that subnet.

Step 4 Expand the Servers folder from the original first site folder.

a) For each Server you need to move to a different site, right-click on server name, select **Move** and highlight the Site you want to move it to.

Step 5 Expand Inter-Site Transport under Sites.

a) Open the IP folder and select **DEFAULTIPSITELINK** from the right pane.
b) Right-click and select **Properties**. Ensure that both sites are added as entries in the Sites in this Site Link window.
c) Change the Replicate Every value to **15 minutes**.

Assign Global Catalog and Configure Time Source

To assign Global Catalogs and configure the time source per your Unified ICM System Diagram and the Unified ICM/CCE System Design Specification for your setup:

Procedure

Step 1 Open **Active Directory Sites and Services**.

Step 2 Connect to the Domain Controller designated as the Global Catalog.

Step 3 Right-click **NTDS Settings** and select **Properties**. Select **Global Catalog**.

Step 4 Move FSMO roles, as indicated in your Unified ICM System Diagram and the Unified ICM/CCE System Design Specification for your setup.

Step 5 The Forest Time Source defaults to the PDC Emulator, which is originally created on the Forest Root Domain Controller.

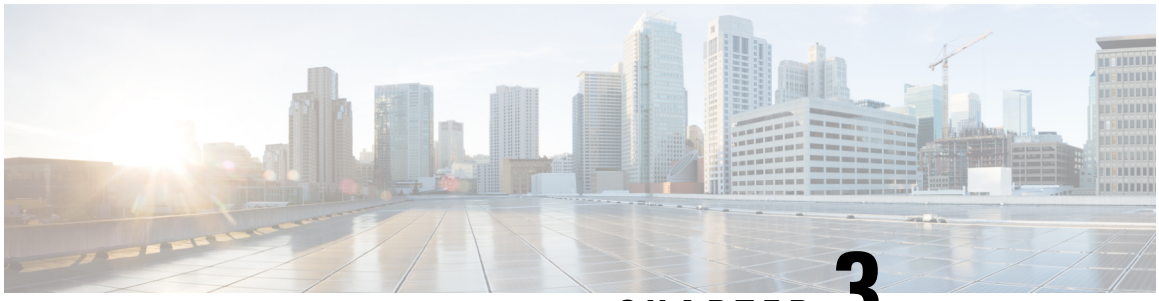
If the PDC Emulator moved to another Domain Controller, redefine the Time Source as either that server, or use an external Time Source.

a) On the Server currently running the PDC Emulator, run the following command: **`Net time /setsntp:<DNS Name of Time Source>`**.
b) To synchronize a Server to the Time source, see the procedure available on the Microsoft Website (http://support.microsoft.com/kb/816042).

Important Windows Server domain controllers that publish their Global Catalogs are required to be used. The preferred DNS servers must not be manually changed. It is important that all the other DNS Servers must have delegation set up with the DNS server of the forest Root Primary Domain Controller.

For detailed information on supported versions for Unified ICM, see:

Contact Center Enterprise Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html



CHAPTER 3

Organization Units

- What Is an OU?, on page 27
- OU Hierarchies, on page 27
- Cisco Root OU, on page 28
- Facility OU, on page 29
- Instance OU, on page 29
- Security Groups, on page 30

What Is an OU?

An OU is a container in the AD domain that can contain other OUs, as well as users, computers, groups, and so on. OUs are a way to organize your objects into containers based on a logical structure. The OU design enables you to assign a flexible administrative model that eases the support and management of a large, distributed enterprise. The OU design is also used for setting up security groups.

AD controls permission to create an OU. Typically, the Domain Administrator has rights to create OUs at the root of the domain, then delegates control of those OUs to other users. After the Domain Administrator delegates a user OU control, the user has permission to create the Cisco Root OU.

Related Topics

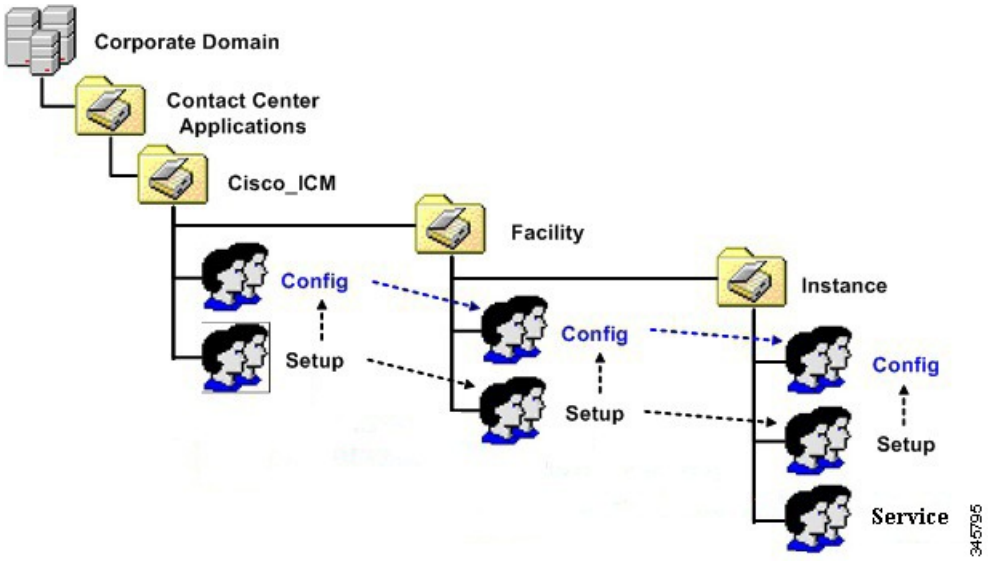
Security Groups, on page 30

OU Hierarchies

Unified ICM uses the following hierarchy of OUs:

- The Cisco Root OU (Cisco_Root)
- One or more Facility OUs
- One or more Instance OUs

Figure 9: Organizational Unit (OU) Hierarchy



All objects that Unified ICM requires are created in OUs on the domain. You can place the OU hierarchy that the Unified ICM creates at the Root of the domain, or in another OU. Servers are not placed in this OU hierarchy. You can place servers in other OUs on the domain.

Note

- The system software always uses a Cisco Root OU named “Cisco_ICM” (see preceding figure).
- The Domain Admin is a member of the Config, and Setup in the Cisco Root OU.
- Installing Unified ICM in the corporate domain is now a supported environment.

Related Topics

Cisco Root OU, on page 28
Facility OU, on page 29
Instance OU, on page 29

Cisco Root OU

You can place the Cisco Root OU at any level within the domain. Software components locate the Cisco Root OU by searching for its name.

The Cisco Root OU contains one or more Facility OUs.

What is the Cisco Root OU?

- Unified ICM always uses a Cisco Root OU named “Cisco_ICM”.
- The OU containing all domain resources created by Unified ICM.
- Defines permissions for all Unified ICM instances.

- Only one Cisco Root OU can exist in each domain

For more information, see Appendix B - Moving the Cisco Root OU.

Related Topics

Create or Add Cisco Root, on page 69

Facility OU

A Facility OU is a group of Instance OUs that are organizationally related or have similar management needs. Permissions defined for a Facility OU propagate to each Instance OU contained in that facility.

The Facility OU provides an administrative separation between Unified ICM instances. For example, you might have different Facility OUs for Lab and Production Unified ICM instances.

A Facility OU inherits the permissions set for the containing Cisco Root OU. You can then specify different user permissions specific to that Facility.

Note Facility OU names must be 32 characters or less.

Related Topics

Instance OU, on page 29
Cisco Root OU, on page 28

Instance OU

An Instance OU inherits the permissions set for the containing Facility OU. You can then specify different user permissions specific to that instance.

Unified ICM Instance OU

A Unified ICM instance is a single installation of the system software. It consists of several components (including the CallRouter, the Logger, Administration & Data Server, and Peripheral Gateways), some of which might be duplexed.

An Instance OU:

- Is the representation of a Unified ICM instance.
  - Each Unified ICM instance has an associated Instance OU.
- Defines permissions for that instance as part of that Instance OU.

  An Instance OU inherits the permissions set for the containing Facility OU; you can then specify different user permissions specific to that Instance.
- Is named by the user according to the following rules:
  - Limited to 5 characters

- Alphanumeric characters only
- Can not start with a numeric character
- Some instance names are reserved (local and sddsn)

Related Topics

Facility OU, on page 29

Security Groups

Security Groups and OUs

Each OU in the OU hierarchy has associated security groups.

Security groups permissions are inherited down the chain in the OU hierarchy. For example, users added to a security group for a Facility OU have the privileges of that security group for all Instance OUs contained in that Facility OU.

Each OU has the following security groups:

- Config Security Group
- Setup Security Group

In addition to the preceding list, Instance OUs also contain the Service Security Group.

Warning Microsoft limits the number of cascading groups in the OU hierarchy. For more information, see Microsoft *Active Directory Maximum Limits - Scalability* article at http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx.

Warning Users who are local administrators for the server automatically can perform configuration tasks. Therefore, only users who are members of the Setup Security Group must be local administrators.

Security Groups Described

A security group is a collection of domain users to whom you grant a set of permissions to perform tasks with system software.

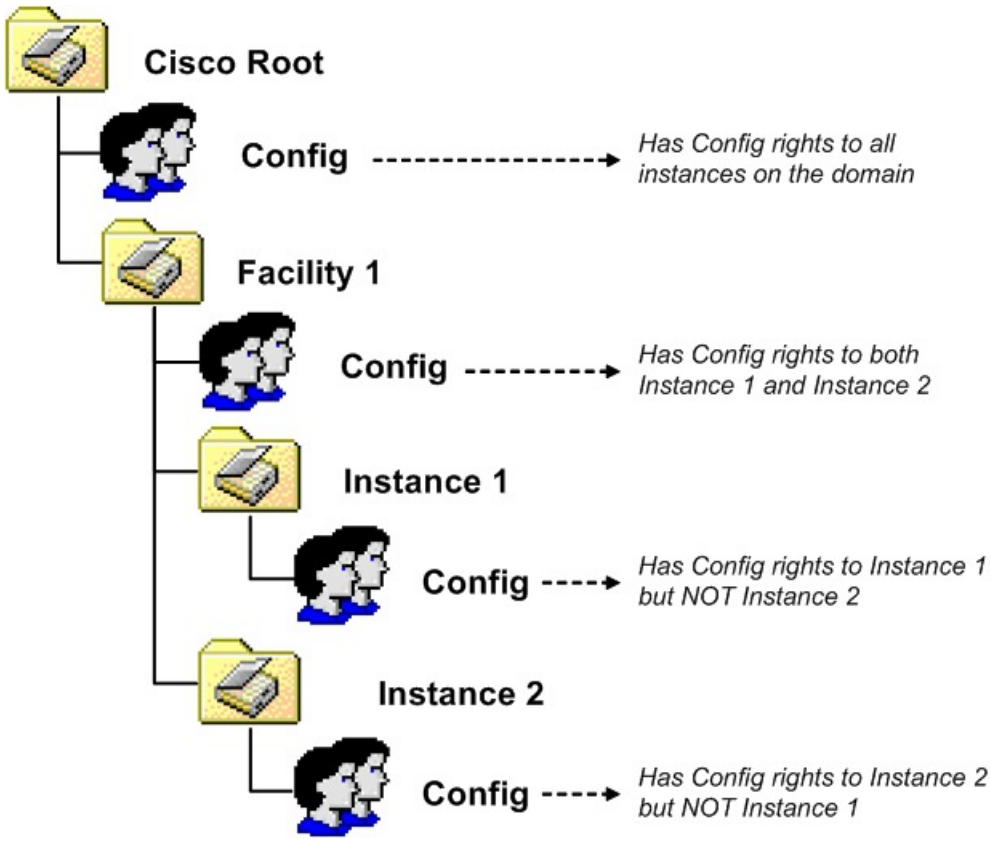
For each security group, you add domain users, who are granted privileges to the functions controlled by that security group. Users are given membership in the security groups to enable permission to the application. You can create these users in other OUs in this domain, or in any trusted domain.

Note The user who creates the Cisco Root OU automatically becomes a member of the Setup Security Group for the Cisco Root OU. In effect, this user is granted privileges to all Unified ICM tasks in the domain.

Security Groups:

- Similar groups at each level of the hierarchy allow users to be granted permission to multiple Instances.
- Are nested so that:
  - A similar group from the Parent OU is a member of each group.

Figure 10: Security Group Nesting



- Use AD Domain Local Security Groups.

Related Topics

Add Users to Security Group, on page 76

Security Group Names and Members

The function names of the security groups are Setup, Config, and Service. Group names must be unique in AD. Combining the names of levels of the hierarchy with the function name helps allow a unique name to be generated.

Names of the security groups created by OUs at various levels include:

- Root: `Cisco_ICM_<function>`
- Facility: `<Facility>_<function>`

- Instance: `<Facility>_<Instance>_<function>`

NetBIOS names truncate if needed and random digits are appended.

Security Group Members:

- You can add any user from a trusted domain to a group.
- Group nesting allows for groups outside the OU hierarchy.

Config Security Group

The Config Security Group controls access privileges to the common Unified ICM configuration tasks.

Domain users whom you added to a Config Security Group have access to the following applications at that point in the OU hierarchy and below:

- Configuration Manager

Note Config users can only perform AD operations using the User List tool (provided they have AD permissions to do so). Members of the Setup Group automatically have the permissions required to use the User List tool.

- Script Editor
- Internet Script Editor
- Database Access
  - SQL Permission granted to the Configuration group instead of to individual users. Database access is given explicitly to the Instance level group. Group nesting gives this access to Facility and Root configuration members.

Added to the GeoTelGroup role on the Administration & Data Server DB.

Note For Administration & Data Server DBs only. Not for Logger DBs and HDSs.

Setup Security Group

The Setup Security Group controls rights to run:

- Installation and Setup Tools
- Configuration Manager

Users who are members of the Setup Security Group can:

- Install instances and software components.
- Add users to security groups.

- Create service accounts.
- Manage OUs, groups, users, and permissions.

Note The Setup Security Group is automatically made a member of the Config for that Unified ICM instance.

The Setup group at each level is given AD permissions to the parent OU.

Figure 11: Setup Security Group permissions

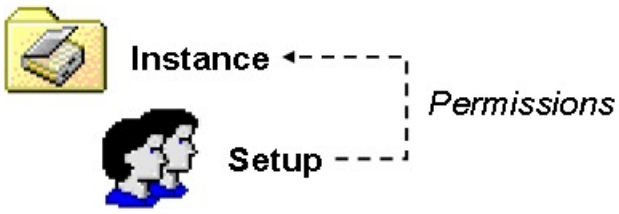


Table 3: Setup Security Group AD permissions

Tasks	OU Hierarchy Level
Delete Subtree	Child objects only
Modify Permissions	Child objects only
Create/Delete OU Objects	This object and all child objects
Create Group Objects	Child objects only
Read/Write Property	Group objects
Special: Create/Delete User Objects	This object and all child objects

For more information see the chapter Service Account Manager.

OU Hierarchies and Security

OUs are nested as described in the preceeding section, with the Root OU containing Facility OUs, which contain Instance OUs. For Unified ICM, the Cisco Root OU is the “Cisco_ICM” OU. As OUs have associated security groups, the nesting of OUs allow the nesting of access rights. Members of a security group have all the access rights granted to that same security group at lower levels in the hierarchy.

Examples:

If you make a user a member the Root Setup security group (see Root Setup Security Group Member Permissions/Access Rights following), that user has the following permissions/access rights:

- Permissions/access rights in the Root Setup security group.

  This also grants permissions/access rights for this user in the:

  - Facility Setup group

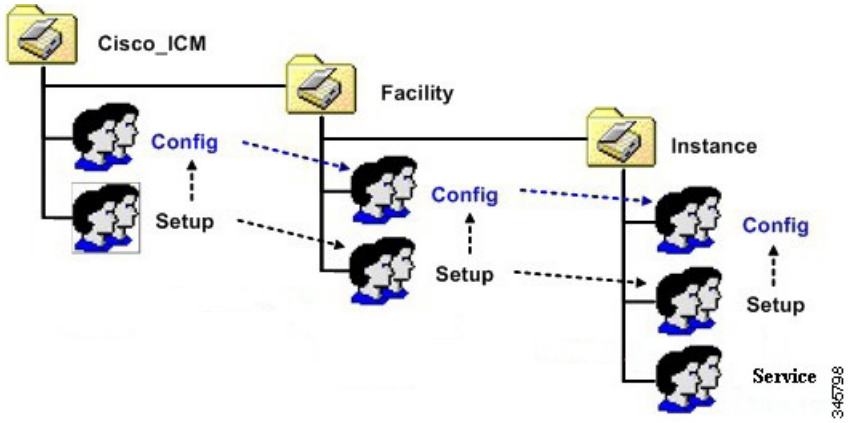
- Instance Setup group

- Permissions/access rights in the Root Config security group.

  This also grants permissions/access rights for this user in the:

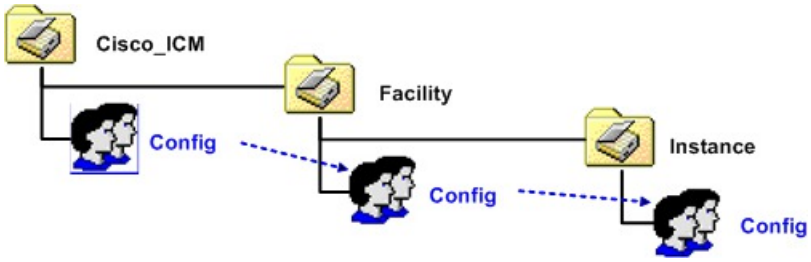
  - Facility Config group
  - Instance Config group

Figure 12: Root Setup Security Group Member Permissions/Access Rights



Making a user a member of the Root Config security group grants permissions/access rights in that security group as well as the Facility and the Instance Config security groups.

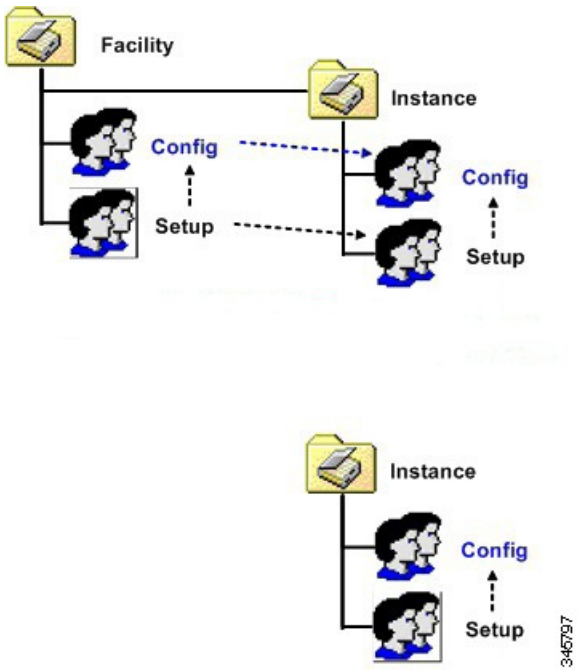
Figure 13: Root Config Security Group Member Permissions/Access Rights



Members of a Facility security group have all the permissions/access rights granted to Instance OUs nested within that Facility. However, members of those Instance OUs security groups do not necessarily have the permissions/access rights granted to their containing Facility OU.

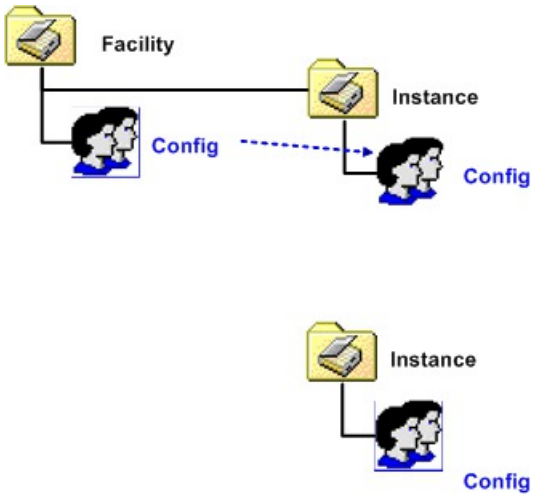
A member of the Instance Setup security group is granted permissions/access rights only to the Instance level security groups (Setup and Config).

Figure 14: Facility/Instance Setup Security Group Member Permissions/Access Rights



In the following illustrations, a member the Facility Config security group has permissions/access rights to that security group and the Instance Config security group. However, a member of the Instance Config security group only has permissions/access rights to that security group.

Figure 15: Facility/Instance Config Security Group Member Permissions/Access Rights



This hierarchy allows you to define security with maximum flexibility. For example, you can grant permissions/access rights at the Facility OU level, so those users have access to a set of instances. You can then define permissions for instance administrators at the Instance OU level, and those users would not have access to the other instances.

Note You cannot move an Instance from one Facility to another.

Related Topics

Instance OU, on page 29

Service Security Group

The Service Security Group is a security group generated automatically for Instance OUs. It exists at the Instance level only. The Service Security Group controls access between the system software components.

Note The Service Security Group is not exposed to users for the Domain Manager. You do not have to perform any tasks related to it.

The group has a SQL login and is a member of the GeoTelAdmin role on the following databases:

- Logger SideA DB
- Logger SideB DB
- Administration & Data Server DB
- HDS
- Outbound Option DB

Service Logon Accounts

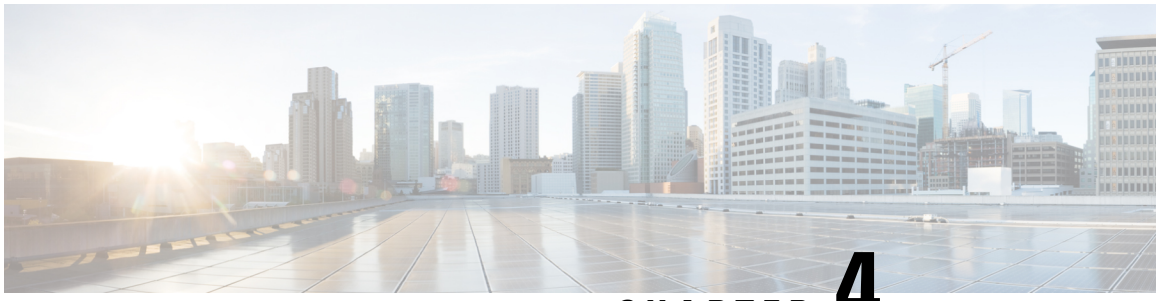
- You do not have to randomly generate passwords. You can provide passwords and save them in AD or on the local machine, or save them on both.
- Passwords are 64 characters long and include:
  - English upper case characters (A..Z)
  - English lower case characters (a..z)
  - Base 10 digits (0..9)
  - Non-alphanumeric characters (! @ # % ^ & * ( ) [ ] { } ` ~ - + ? . , ; : ' < >)
- Are added to local Administrators group.
- Are given rights to Logon as a Service.
- DNS names are comprised of: <*Instance component machine*>

  Possible components are the:
  - Distributor (NetBIOS name is Distrib)
  - LoggerA
  - LoggerB

- Tomcat

- NetBIOS names are comprised of: <*instance component-#####*>

  where ##### is used to represent digits added to ensure the NetBIOS name is comprised of the full 20 characters allowed to help ensure, but not guarantee its uniqueness. The list of possible components is the same as those for the DNS names except as indicated above.



CHAPTER 4

User Migration Tool

- User Migration Tool Prerequisites, on page 39
- User Migration Tool Features, on page 40
- Migration Scenarios, on page 40
- Internationalization (I18n) and Localization (L10n) Considerations, on page 41
- Security Considerations, on page 41
- User Migration Steps, on page 41
- User Migration Tool Modes, on page 43
- Users from Trusted Domains, on page 48
- User Migration Tool Troubleshooting, on page 49

User Migration Tool Prerequisites

You must meet the following prerequisites before you run the User Migration Tool:

- In the target domain, run Domain Manager. Lay out the Unified ICM OU hierarchy and create the Unified ICM security groups for each Unified ICM instance before you run the User Migration Tool.
- Import the exported Unified ICM registry from the source Logger system to the target Logger system.
- Back up the Logger database from the source Logger system and restore it on the target Logger system before you run the User Migration Tool in the target domain.
- If users from an external domain are members of the Unified ICM security groups at the source domain, use the“Active Directory Domains and Trusts” tool to establish the trust relationship. Establish the trust relationship between the target domain and the external domain that corresponds to the trust relationship that existed between the source domain and the external domain.
- If you move the Unified ICM server to a new domain, make sure that the SQL Server migrates to the new domain before you run the User Migration Tool.
- In the source domain, the user who runs the User Migration Tool must be a domain user and a member of the local system administrator group.
- In the target domain, the user who runs the User Migration Tool must have the following privileges:
  - The user must be a member of the local system administrator group.
  - The user must be a domain user.

- The user must have at least one of the following privileges set:
  - a domain administrator
  - a member of the Cisco_ICM_Setup (Root) security group

- Access the external domain to migrate the membership of Unified ICM users who belong to an external domain. Access requires external domain user account credentials with read privileges.

User Migration Tool Features

The User Migration Tool provides the following features:

- Migrates AD user accounts from an old (source) domain to a new (target) domain to the same, or a different, Unified ICM facility.
- Adds the user account in the corresponding Unified ICM security groups in the target domain.
- Updates the Logger database with the Globally Unique Identifier (GUID) of the user account from the target domain.
- Migrates the Unified ICM security group membership of Foreign Security Principals to the new domain.
- Migrates the Unified ICM security group membership of user accounts to another facility in the current domain.

Note User Migration Tool is not applicable for SSO users.

Migration Scenarios

Use the User Migration Tool in the following migration scenarios:

- Technology Refresh upgrades on machines in a target domain.
- Technology Refresh upgrades on machines in a different Unified ICM Facility OU in a target domain.
- Moving machines with pre-installed Unified ICM components to a target domain.
- Moving machines with pre-installed Unified ICM components to a different Unified ICM Facility OU in the target domain.
- Moving machines with pre-installed Unified ICM components to a target domain and performing a Common Ground (CG) upgrade.
- Moving machines with pre-installed Unified ICM components to a different Unified ICM Facility OU in the target domain and performing a Common Ground upgrade.
- Migration of user accounts to a different Unified ICM Facility OU in the same domain.

Internationalization (I18n) and Localization (L10n) Considerations

In the localized version of Unified ICM/CCE, you can store the usernames in non-Western European characters (but not in Unicode) in the Unified ICM/CCE database, but the Active directory Common Name (First, Last, Middle), sAMAccount Name, User Principal Name, Organizational Unit (OU) and domain names are always in Western European character set and must not include Unicode or multi-byte characters.

The User Migration Tool is able to perform user migration for localized systems.

Security Considerations

The User Migration Tool connects to the Logger Database using Windows Authentication.

In the source domain, the user running the User Migration Tool must be a domain user and a member of the local system administrator group.

In the target domain, the user running the User Migration Tool must have the following privileges:

- The user must be a member of the local system administrator group.
- The user must be a domain user.
- In addition, at least one of the following privileges must be set. The user must be:
  - a domain administrator
  - a member of the Cisco_ICM_Setup (Root) security group

Migration of the membership of system users who belong to an external domain with one-way trust, requires credentials of an external domain user account with read privileges (such as a domain user account) to access the external domain.

User Migration Steps

The User Migration Tool first runs in the source domain in Export mode. In this mode, it reads the users from the Logger database and the nine (9) security groups, then exports the user information (such as Username and UserGroupID) and the security group membership from the source AD folder. The UMT looks at the Logger database for each user found and looks at all nine (9) security groups to find the user group memberships (the Setup and Config security groups in the Root, Facility, and Instance OUs). The user information found is added to the flat file.

For users belonging to the external domain, the User Migration Tool needs credentials to connect to the external domain. The UMT looks for the users in the external domain. If the UMT finds them, it determines the security group membership for the user in the source domain and exports the information.

The UMT also looks at the Instance security groups (Setup and Config) to find any user accounts. If the UMT finds user accounts, it adds that user information to the flat file as well.

The User Migration Tool then runs in the target domain in an Import mode. In this mode, it reads the file that was generated during Export mode and does the migration for all the users that belong to the source domain. During this mode, it looks for the users in the target domain and, if they are not found, creates the user accounts

in the Instance OU. It fixes the group membership for the user and updates the database (if necessary) with the target domain name and the user's GUID from the target domain. In order to perform migration of the users belonging to an external domain, the User Migration Tool needs credentials to connect to the external domain. It looks for the users in the external domain and, if they are found, it fixes the security group membership for the user in the target domain.

The following are the steps involved when using the User Migration Tool.

Export Users from the Source Domain

Procedure

Step 1 Back up the Logger database for each Unified ICM/CCE instance using Microsoft SQL Server tools.

Step 2 On the Logger system, for each installed Logger instance, run the User Migration Tool in Export mode.

An output file (umt_<*Facility name*>_<*logger database name*>.bin) is generated in the directory from which the tool is run.

Step 3 In a Technology Refresh upgrade scenario:

a) Copy the output file to the Logger system in the target domain (to the folder from which you run the User Migration Tool on the target system).
b) Back up and export the registry on the source system.
c) Check the log file for any errors.

Import Users into the Target Domain

Procedure

Step 1 If the Unified ICM/CCE services are running, shut them down.

Step 2 If you need to change the domain name in a Common Ground upgrade scenario, see Change Domain Name, on page 43 and proceed to Step 4.

Step 3 In a Technology Refresh upgrade scenario:

a) Make sure that the exported file exists in the Logger system.
b) Restore the Logger database that was copied from the source Logger system using Microsoft SQL Server tools.
c) Import the Unified ICM/CCE registry exported from the source domain.

Step 4 Run the User Migration Tool in Import mode for each Logger instance to migrate users.

Step 5 (Optional) Run the User Migration Tool in verify mode to validate the migration.

Step 6 For duplex Logger systems, run the ICMDBA tool to synchronize sides A and B.

Step 7 Restart the Unified ICM/CCE services if they were previously running.

Change Domain Name

To change the domain for a system, you must have the necessary permissions. To change the domain for all instances on the computer, complete the following steps:

Procedure

Step 1 Open the Web Setup tool.

Step 2 Click the **Instance Management** tab.

Step 3 Delete any instances and facilities that you don't want to use in the new domain.

Step 4 Open the Cisco Domain Manager tool. Ensure that the instances and facilities that are defined match what is actually on the system. A mismatch can cause the Web Setup Change Domain operation to fail.

Step 5 Select the instance that you want to modify, and then click **Change Domain**.

The Change Domain page opens, displaying the currently configured domain and the new domain name of the system.

Step 6 Click **Save**. Confirm whether you want to change the domain.

Step 7 Click **Yes**. If successful, you'll return to the Instance List page.

If the instance doesn't exist, then create it using the Cisco Domain Manager. Be sure to create the instance under the selected facility in the new domain.

Note Make sure that the certificates in the keystore pertain to the fully qualified domain name (FQDN) of the servers. If you have changed the domain name or hostname, be sure to update the certificates in the keystore.

User Migration Tool Modes

The User Migration Tool provides functions in the following modes:

- Export
  - Runs on the Logger system in the source domain.
  - Exports user account details from the Logger database and Instance security groups to a file generated in the same directory in which the tool was run.

    Names the exported file by combining the tool name (umt), the ICM Facility name, and the Logger database name (umt_<*Facility name*>_<*Logger database name*>.bin).

    The exported file contains the source domain name. It also contains Unified ICM instance specific parameters such as the Unified ICM Facility name, Unified ICM instance name, and Logger database name. You do not need to specify these parameters during the Import mode because they are contained in the exported file.

- Import
  - Imports user account details from the exported file.

- Updates AD and the Logger database (if necessary).

Note Due to the need to replicate new user accounts and AD security group memberships, wait 15 minutes after an Import completes before you run the User Migration Tool in Verify mode.

- Verify
  - Runs on the Logger system in the target domain after you perform an Import.
  - Validates the import.

Note Help is available by entering **`usermigration.exe`** with either no arguments or the **`/help`** argument. This command displays the command line syntax, and all modes and parameters are displayed.

The User Migration Tool also generates a report file in the same directory that the tool is run. The name of the report file consists of the name of the exported file suffixed with ".rpt" (umt_<*Facility name*>_<*Logger database name*>.rpt).

The report file contains the following information:

- In the **Export** mode:
  - the name of the user account that is exported
  - all the Unified ICM security groups that the user account is a member of
- In the **Import** mode:
  - the name of the user account that is created in AD
  - all the security groups added to the user account.

In addition, every time the User Migration Tool runs, it generates a log file in `C:\temp`. The name of the log file contains the current time-stamp and is prefixed with "UMT" (for example: UMT2008619141550.log).

The log file contains results in three categories:

- Info
- Warning
- Error

Runtime messages are also displayed in the command window while the User Migration Tool runs.

Related Topics

Import Mode, on page 46
Verify Mode, on page 47

Mode Considerations

The username created can not log on for Internet Script Editor pages, without first logging into the new domain and then changing the password.

Use your Windows logon to login using the AD account. A prompt appears asking to change the password. Provide a new password, then use the Internet Script Editor interface to login.

Export Mode

The Export mode exports the user information from the source domain and external domain into a file.

When you run the User Migration Tool in Export mode, it exports the following information to the file:

- Unified ICM Facility and Instance name
- Logger database name
- AD user account name and the domain name
- Unified ICM security group that the user is a member of
- UserGroupID from the Logger database

The following table provides the command and parameter information for the User Migration Tool operating in Export mode.

Table 4: Export Mode Syntax

Command	Mode Parameter	Content Parameters
UserMigration.exe	/Export	[/DBname <*Logger Database name*>]
		[/Facility <*ICM Facility name*>]
		[/Instance <*ICM Instance name*>]

The Export mode command syntax is: usermigration.exe /Export /DBname <*Logger Database name*> /Facility <*ICM Facility name*> /Instance <*ICM Instance name*>.

Note

- For each external domain, the UMT command-line interface solicits the credential details to connect to that domain. If it fails to connect to the domain, it does not export the users belonging to that domain.
- The parameter names are not case sensitive. The first parameter must always be the Mode Parameter. The order of the content parameters does not matter, as long as you include all of them in the command.

Related Topics

Content Parameter Descriptions, on page 47

Import Mode

The Import mode migrates users from the source domain, and external domain, to the target domain; and then updates the Unified ICM database.

In the Import mode, the User Migration Tool gets the username from the input file, and searches for a user account in the AD, and creates one if not found. The user account is created in the Instance OU using the password supplied in the command-line interface. The password is set to expire to force the user to change the password during the next login.

The User Migration Tool adds the user account to the Unified ICM security group based on the information from the exported file. The Logger database then updates with the user account AD Globally Unique Identifier (GUID) and the target domain name.

The following information imports from the exported file:

- Logger database name
- Unified ICM facility
- Instance name

In the Import mode, you can run the User Migration Tool with an optional /Facility parameter to import the user accounts to a different facility name. If the new facility migration is in the same domain:

- You do not need to create the user accounts or update the Logger database.
- Only the Unified ICM security group membership of the user account updates.

The following table provides the command and parameter information for the User Migration Tool operating in Import mode.

Table 5: Import Mode Syntax

Command	Mode Parameter	Content Parameters
UserMigration.exe	/Import	[/FileName <*Exported file name*>]
		[/SetPassword <*Default password for newly created AD user accounts*>]
		[/Facility <*Different ICM Facility name*>] (Optional.)

The Import mode command syntax is: usermigration.exe /Import /FileName <*Exported file name*> /Setpassword <*Default password for newly created AD user accounts*> /Facility <*Different ICM Facility name*>.

In the Import mode, the User Migration Tool searches for a user account in the AD, and creates a user account if it does not find one. The user account is created in the Instance OU using the password supplied in the command-line interface. The password is set to expire to force the user to change the password during the next logon.

Note The parameter names are not case sensitive. The first parameter must always be the Mode Parameter. The order of the content parameters does not matter, as long as you include them all in the command.

Related Topics

Content Parameter Descriptions, on page 47

Verify Mode

The Verify mode validates the import in the target domain by validating the AD and Unified ICM database migration done in the Import mode.

The User Migration Tool performs the following verification with the data from the exported file:

- Verifies the existence of the user account in AD.
- Verifies the membership of the user in the Unified ICM security groups.
- Validates the user's AD Globally Unique Identifier (GUID) and the domain name with the information in the Logger database (Unified ICM only).

The command and parameter information for the User Migration Tool operating in Verify mode are provided in the following table.

Table 6: Verify Mode Syntax

Command	Mode Parameter	Content Parameters
UserMigration.exe	/Verify	[/FileName <*Exported file name*>]
		[/Facility <*Different ICM Facility name*>] (Optional.)

The Verify mode command syntax is: **`usermigration.exe/Verify/FileName <Exported file name>/Facility <Different ICM Facility name>`**.

Note The parameter names are not case sensitive. The first parameter must always be the Mode Parameter. The order of the content parameters does not matter, as long as they are all included in the command.

Related Topics

Content Parameter Descriptions, on page 47

Content Parameter Descriptions

The following table provides descriptions of the parameters used by the User Migration Tool.

Table 7: User Migration Tool Parameters

Parameter	Description
/DBName	The Logger database name.

Parameter	Description
/Facility	The Unified ICM instance facility name. When you optionally specify this parameter during the import or verify mode, the User Migration Tool migrates users to a different Unified ICM facility.
/Instance	The Unified ICM instance name.
/FileName	The filename that has the user information exported from the source domain.
/SetPassword	The default password used for the user account created in the target domain. The User Migration Tool sets it to "Change password at next logon" so that the user is forced to change the password when they log in for the first time.

Users from Trusted Domains

User accounts from trusted AD domains with authorization in the current domain are possible. These user accounts are authorized in the current domain because the users are members of Unified ICM security group. The User Migration Tool performs migration of Unified ICM security group membership of such user accounts.

For one-way trusted domains, the User Migration Tool needs Domain User credentials from the external domain in order to:

- Connect to the external domain and find a user account.
- Determine the Unified ICM security group membership in the current domain.

The command-line interface to solicit credentials is as follows:

1. Enter username on domain <*DomainName*>.
2. Enter <*password*>.

For users of a trusted domain, the Unified ICM security group membership is migrated only if the user is a direct member of the Unified ICM security group.

For example:

- *ExtUser1* is a user account belonging to the trusted domain *ExtDomainA*.
- *ExtUser1* is a **direct** member of the Cisco_ICM_Setup and Cisco_ICM_Config security groups.
- *ExtUser1* is a member of the security group FOO.

Note This restriction does not exist for users belonging to the current (source) domain.

As a result, when the Unified ICM security group membership of *ExtUser1* is migrated, only the Cisco_ICM_Setup and the Cisco_ICM_Config security groups are selected.

To migrate Unified ICM security group membership of users belonging to a one-way trusted domain, there must be at least one user from that domain in the Logger database. Otherwise, the UMT skips migration for the one-way trusted domain.

The UMT knows that it needs to connect to a one-way trusted domain only if it is referenced in the Logger database. Unless it connects/authenticates to the one-way trusted domain, it cannot determine if users from that domain are a member of the Unified ICM security groups.

User Migration Tool Troubleshooting

This section provides troubleshooting information for the User Migration Tool.

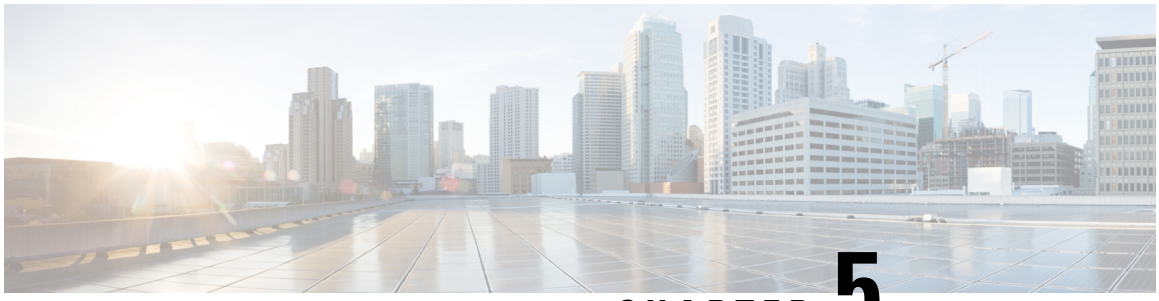
User Migration Tool Error Messages

The following table provides solutions for User Migration Tool error messages.

Table 8: User Migration Tool Error Messages

Error Message	Solution
Cannot connect or authenticate to the Logger database.	Verify that the Logger database exists and that you can authenticate it using Windows authentication.
Cannot connect or authenticate to the Current domain.	Verify that the Domain controller is up and running and the logged-in user is a member of the Domain Users group.
Cannot add the user account to a Unified ICM security group.	Verify that the logged-in user has the required permissions to run in Import mode. The logged-in user must be a Local Administrator and a member of the Setup security group in the domain. The specified password in the /Setpassword parameter must satisfy the domain's password policy requirements.
Cannot create user account in the target domain.	Verify that the logged-in user has the required permissions to run in Import mode. The logged-in user must be a local administrator and a member of the Setup security group in the domain.
The exported binary file is corrupted.	Run the User Migration Tool again on the source system to generate a new export file.
The exported binary file could not be found in the directory where the User Migration Tool is running.	Ensure that the exported file is available in the directory from where the tool is run.
Failure while reading from the Logger database.	Verify that the Logger database is not corrupted.
Failure while updating the Logger database.	Verify that the logged-in user has writable permissions for the database. The logged-in user must be a local administrator and a member of the Setup security group in the domain.

Error Message	Solution
Failure while reading from the exported binary file.	The exported binary file is corrupted. Run the User Migration Tool in Export mode again on the source system to generate a new export file.
Failure while writing to the binary file during export.	Ensure that the logged-in user has write permissions in the current directory.
One or more of the Unified ICM OU is missing in the current domain.	Run Domain Manager tool and create Setup security groups, and re-run the User Migration Tool.
One or more of the Unified ICM security groups do(es) not exist in the current domain.	Run the Domain Manager tool and create the Setup security groups, then re-run the User Migration Tool.
The logged-in user has insufficient credentials.	The logged-in user must be a Local Administrator. The logged-in user must be a member of the Domain Users group in the current domain. For import, the logged-in user must be a member of Cisco_ICM_Setup security group.
The Logger database is corrupted.	Fix the Logger database and re-run the User Migration Tool.
The system is either running stand-alone, or in a workgroup.	The User Migration Tool must be run on a system that is in a domain.
Mismatch of version between the User Migration Tool and the exported file.	You must use the same version of the User Migration Tool for both modes of the migration.
The User Migration Tool could not disable configuration changes.	Disable the configuration changes manually, then run the tool.
Incorrect usage of the User Migration Tool.	You cannot run the User Migration Tool in Import mode under the same Unified ICM facility and domain that it was exported from. You must run it under a different Unified ICM facility in the same domain, or on a different domain.
The Router system is not reachable for remote registry access.	Ensure the hostname or IP address of the router is correct.



CHAPTER 5

Service Account Manager

- Service Account Management, on page 51
- Service Account Manager End User Interfaces, on page 52
- Service Account Manager GUI Dialog Boxes, on page 52
- Service Account Manager – Main Dialog Box, on page 52
- Service Account Manager – Edit Service Account dialog box, on page 58
- Command Line Interface for Service Account Manager, on page 58
- Service Account Manager, on page 59

Service Account Management

The Service Account Manager allows you to use existing AD accounts as Unified ICM/CCE service accounts.

Other Considerations

Permissions

You must have the correct privileges to associate the accounts in the local machine. Typically, a Domain User with local administrator privilaege performs this task.

Domain Restriction

The following conditions are mandatory when adding or editing a service account using the Service Account Manager Tool or Websetup:

- The service account must be in the same domain as the Unified ICM server.
- The UPN (User Principal Name) must be set for the account in the Active Directory.
- ensure that the account user login name set for UPN is same as the NETBIOS pre-windows 2000 login name (SAM Account Name).

Special Case: If the distributor service Account and logger service account are different then add the distributor service account in the logger.

Local Group Update Failures

If Service Account Manager fails to add the user in the local administrators group and local UCCE service account group then add the user to above mentioned groups manually.

Logging

The application maintains its own log file, when you invoke it as a standalone application. If you invoke it through the Web Setup tool, logs write to the Websetup log files only.

Service Account Manager End User Interfaces

The Service Account Manager has two user interfaces:

- The Graphical User Interface consisting of the following dialogs boxes:
  - Main
  - Edit Service Account
- The Command Line Interface

Related Topics

Service Account Manager GUI Dialog Boxes, on page 52
Service Account Manager – Main Dialog Box, on page 52
Service Account Manager – Edit Service Account dialog box, on page 58
Command Line Interface for Service Account Manager, on page 58

Service Account Manager GUI Dialog Boxes

You can find a shortcut to the application in Windows **Start** > **Programs** > **Cisco Unified ICM-CCE Tools** folder.

The Service Account Manager has two dialog boxes:

- Main
- Edit Service Account dialog box.

Related Topics

Service Account Manager – Main Dialog Box, on page 52
Service Account Manager – Edit Service Account dialog box, on page 58

Service Account Manager – Main Dialog Box

You can use the Service Account Manager as a standalone application for Cisco Unified ICM/CCE Installer.

The Main Service Account Manager dialog box is the application's primary interface. It consists of the *Services Requiring User Logon Accounts* section (which contains the *Service Name*, *Service Logon Account Name*,

Logon Account Health, *Password Expiration*, *State*, and *Startup* fields), the **Facility/Instance** drop-down; and the **Select All**, **Edit Service Account**, **Fix Group Membership**, **Refresh**,**Close**, and **Help** buttons.

The following table provides a description for each field and button in this dialog box.

Field/Button/ Drop-down	Description
Service Name	A list of all relevant services. If there are no relevant services on the server, such as a Administration & Data Server, or Logger; the field displays the message "This instance does not have any service that requires a service account."
Service Logon Account Name	Displays the service account name for the list of relevant services.

Field/Button/ Drop-down	Description

Logon Account Health	The Service Account Manager has an account health check mechanism. When the application starts, it scans all relevant Unified ICM services and flags them as indicated below.
	• Green
	  • Healthy Account: the service account state is active.
	• Yellow
	  • Password Warning: the password is due to expire in less than 7 days.
	• Red
	  • *Invalid Account*: service has an invalid account associated with it.
	  • *Password Expired*: service account password has expired.
	  • *Group Membership Missing*: service account is missing from the required local security groups.
	  • *Account not associated with service*: service account created but not replicated, hence not associated yet.
	  • *Account is locked out in domain*: service has a locked out account associated with it.

Field/Button/ Drop-down	Description
	The following messages could appear in the Health column. • Healthy • Only applies to the service account, not the service itself. • The account is a member of the required UcceService local service and local admin groups. • The account has been validated to start a service. • If the account password is changed outside of the Service Account Manager application, *Healthy* would be displayed even though the service might not actually be healthy because this application cannot detect the change. • Need to create service account • The Service Account Manager must be used to associate a service account for each service. • Account not a member of the UcceService local group • The Service Account Manager then places the account in the required UcceService local service group and local admin group, and sets the required permissions. • Account Disabled • In AD, an account can be enabled or disabled. This message indicates that the account is disabled in the domain. • Password Expired • • Account is locked out in domain • In AD, an account can be locked out because of domain policies. • Central Controller (sideA) Domain name is unknown (Administration & Data Server only) • Administration & Data Servers can be in a different domain than the Central Controller. When **Fixed Group** is selected, you are queried for the domain name of the Central Controller if it is different than that of the Administration & Data Server. • Central Controller (sideA) Domain is not trusted or trust is not two-way (Administration & Data Server only) • There must be a two-way trust between the Central Controller and the Administration & Data Server. SAM detects the lack of the trust relationship and displays this message. SAM might detect this issue, but

Field/Button/ Drop-down	Description
	is unable to fix it. • Account not a member of LoggerA Domain Service Group (Administration & Data Server only) • If the Administration & Data Server is on a different domain than the Central Controller, it applies the Administration & Data Server's Domain Service Group to both itself and the Central Controller. • Central Controller (sideB) Domain name is unknown (Administration & Data Server only) • Administration & Data Servers can be in a different domain than the Central Controller. When **Fixed Group** is selected, you are queried for the domain name of the Central Controller if it is different than that of the Administration & Data Server. • Central Controller (sideB) Domain is not trusted or trust is not two-way (Administration & Data Server only) • There must be a two-way trust between the Central Controller and the Disributor. SAM detects the lack of the trust relationship and displays this message. SAM might detect this issue, but is unable to fix it. • Account not a member of LoggerB Domain Service Group (Administration & Data Server only) • If the Administration & Data Server is on a different domain than the Central Controller, it applies the Administration & Data Server's Domain Service Group to both itself and the Central Controller. • Account not associated with service • When SAM associates an account with a service it might run into replication issues. Use **Edit** and select **Associate the account with a service** rather than selecting editing from the beginning. • Service not validated for starting • When SAM validates a service it might run into replication issues. Use **Validate** to successfully start the service. • Password About To Expire • Check the **Password Expiration** option to determine the validity period of the password. The Service Account Manager can then be used to reset the password for this pre-existing account.

Field/Button/ Drop-down	Description
	A service has an *Invalid Account* health state immediately after creation because no domain account is assigned to it yet. This is expected behavior. A service can have a *Missing Group Membership* problem due to a prior AD related failure. The Service Account Manager is capable of fixing this issue by providing an interface that re-attempts placing the account in the relevant local security groups. **Note** SAM health reporting might be inaccurate for the period of time while AD replication is in progress. The previous health state might be indicated during this time.
Password Expiration	**Note** • Any service with an account password that expires in seven (7) days is yellow flagged by the application. • You own the responsibility to refresh the passwords before they expire. If you do not, the system services fail to function.
State	The current state of the service (Stopped, Start/Stop Pending, or Running).
Startup	Displays how the service is started (Manual or Automatic).
Facility/Instance	Drop-down displaying the “Facility/Instance” name. In case of multiple instances, the default “Facility/Instance” selected in the drop-down is the last instance edited by Setup. Select a specific instance. The Service Account Manager lists all relevant services with their account information, account health, password expiration and startup state for the selected instance. If there are no relevant services on the server (such as a Administration & Data Server, or Logger) the Service Account Manager displays the message: *This instance does not have any service that requires a service account.*
Select All	Click to select all listed services.
Edit Service Account	To fix any account issues, edit one, a few, or all accounts at the same time by selecting them and clicking this button. When the dialog box appears, the Service Account Manager prompts you to try to use the account recently created, as it keeps track of it. The application never stores the password.
Fix Group Membership	Available ONLY if an account with the *Group Membership Missing* health state is selected.
Refresh	Refreshes all information in the Service Account Manager Main dialog box.
Close	Closes the Service Account Manager dialog box.
Help	Select to access the online help for the Service Account Manager.

Service Account Manager – Edit Service Account dialog box

The **Edit Service Account** dialog allows you to use an existing account . From the **Edit Service Account** dialog, you can also modify the existing user account or password. The status bar at the bottom of the dialog box displays status messages as needed.

The following table provides a description for each field, button, and check box for this dialog box:

Field/Button/check box	Description
Service(s)	Displays the name of the service to be edited.
Service account(s)	Displays the account name for the selected service.
Account Domain	Displays the server domain. (Read Only)
Password	Enter the password associated with the account name.
Apply	Click to apply any changes on this dialog box.
Close	Click to close this dialog box. Whenever this dialog box is closed, the Service Account Manager determines if a valid domain account is associated with the services or not. If the account is associated, the services must start automatically. **Note** If the services do not start automatically, you must start it manually using the CCE Service Control Tool. If the Service Account Manager finds that you did not successfully associate a valid domain account with a service, it warns you that the service fails to function until you use the Service Account Manager to associate a valid domain account with the service.
Help	Select to access the online help for the Service Account Manager.

Command Line Interface for Service Account Manager

Silent Setup for Default Service Accounts

Web Setup uses the command line interface to silently associate service accounts.

Setup passes the following three arguments to the Service Account Manager:

/Instance <InstanceName>

- The InstanceName argument specifies the Unified ICM instance name for which the service is being setup.

/Service <ServiceType>

- The Service argument specifies the type of the service whose account name and password are being created.

  For example: /Service Distributor

  Service types to use are:

  - Distributor
  - LoggerA – Use when on Side A of the logger or for All-In-1 ICM/CCE
  - LoggerB – Use when on Side B of the logger only

/Log <Path\LogFileName>

- The Log argument specifies the log file name and the path where the log is appended. Typically, Web Setup and Cisco Unified ICM/CCE Installer passes their own log file name to append the logs. The Service Account Manager also maintains its own log file in the temp folder.

Note

- If any one of the arguments is missing or incorrect, the Service Account Manager returns an error to Setup.
- If Setup needs to create accounts for more than one service, it invokes the Service Account Manager multiple times using the command line interface.

/domainUser <Service Account>

- The domainUser argument provides the Service Account that needs to be associated with the service.

/domainPassword <Password>

- The domainPassword argument provides the Service Account password for the Service Account that needs to be associated with the service.

Service Account Manager

Update Existing Account for Single Service

Procedure

Step 1 Select a single service from Main Service Account Manager dialog box.

Step 2 Click **Edit Service Account**.

The Edit Service Account dialog box opens.

Step 3 Enter a password.

Step 4 Click **Apply**.

The Service Account Manager places the account in required UcceService local group and local admin group, and sets the required permissions.

Update existing account for more than one Service

Procedure

Step 1 Select multiple services or click **Select All** on the Main Service Account Manager dialog box.

Step 2 Click **Edit Service Account**.

The Edit Service Account dialog box opens.

Step 3 Enter an account name.

Step 4 Enter a password.

Step 5 Click **Apply**.

The Service Account Manager then places the account in the required UcceService local group and local admin group, and sets the required permissions.

Fix Account Displaying Adverse Health State

Fix Group Membership is only enabled when an account that is in an adverse health state, is selected. The health state is displayed by a message such as “Group Membership Missing” or “Account not a member of UcceService local group”

Procedure

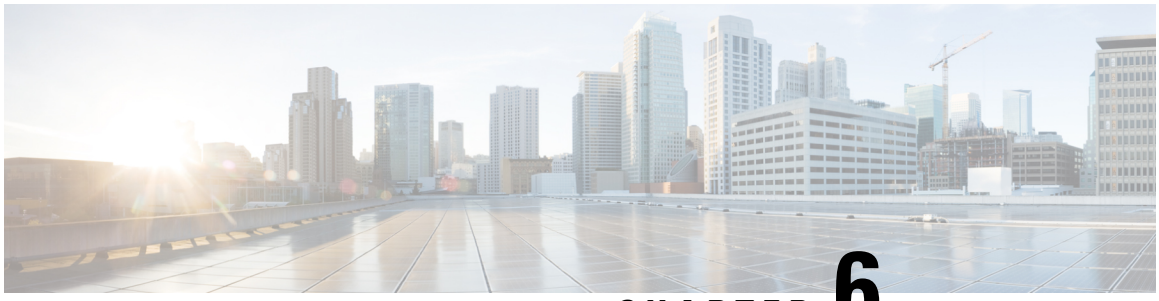
Step 1 Select the unhealthy accounts displaying a state such as the "Group Membership Missing" or "Account not a member of UcceService local group" state.

Step 2 Click **Fix Group Membership**.

Step 3 Click **Apply**.

The Service Account Manager then places the account in the required `UcceService` local service group and local admin group, and sets the required permissions.

Note If the Service Account Manager fails to place the accounts in the groups, it provides an appropriate error.



CHAPTER 6

Prepare to Work with Active Directory

- Perform Preliminary Steps, on page 61
- Domain Manager and OU Hierarchy, on page 61

Perform Preliminary Steps

Perform the following steps before beginning to work with Active Directory.

Warning The Domain Administrator must first create the root OU “Cisco_ICM”. You need not be a Domain Administrator to create the Cisco Root OU if that OU is going to be created in a nested OU (for example, Applications -> Voice Applications…), the Domain Administrator can create a parent OU with delegated rights to create Cisco_ICM Root OU.

Procedure

Step 1 Review the system software staging guidelines.

Step 2 Ensure that you have installed Microsoft Windows.

Step 3 If you are installing a Logger or Distributor/HDS Administration & DataServers, ensure that you have already installed Microsoft SQL Server.

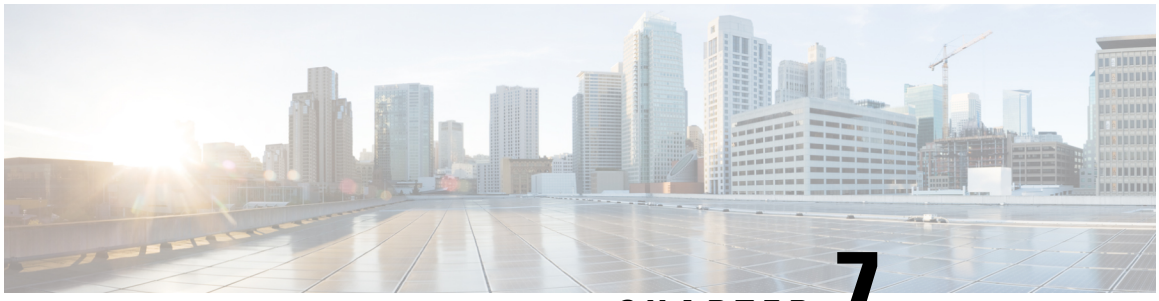
Domain Manager and OU Hierarchy

- The Instance is not just a name in the registry.
- Adding an Instance only requires selecting a Facility and an Instance OU from the domain.
  - First, create the OU hierarchy when you install or upgrade the first server.
  - Then, choose an existing Instance from that hierarchy.

Note When you add an instance, you add that instance's Setup security group to the local Administrators group on that machine. When you remove an instance, it also removes this security group.

- Integrated use of the Domain Manager

When Domain Manager creates Instance OUs, user accounts in old Unified ICM/CCE security groups are automatically copied to new security groups in the new instance OU. The old groups are not modified.



CHAPTER 7

Domain Manager

- Domain Manager Tool Functionality, on page 63
- Open the Domain Manager, on page 64
- Domain Manager Window, on page 64
- Security Groups, on page 74
- Add Users to Security Group, on page 76
- Remove Members from Security Group, on page 78
- Organizational Unit Validation Errors Dialog Box, on page 78

Domain Manager Tool Functionality

The Domain Manager Tool performs the following functions:

- Creates a Cisco Root OU named Cisco_ICM in the domain. After Domain Manager creates this root OU, it also creates two domain local security groups:
  - Cisco_ICM_Config
  - Cisco_ICM_Setup
- Creates a facility OU under the Cisco Root OU, and creates two domain local security groups:
  - <*Facility name*>_Config
  - <*Facility name*>_Setup

  The Domain Manager adds the <*Facility name*>_Setup group to the <*Facility name*>_Config group. The Domain Manager also adds security groups as follows:
  - Adds Cisco_ICM_Config group to <*Facility name*>_Config
  - Adds Cisco_ICM_Setup group to <*Facility name*>_Setup
- Creates an instance OU under each facility OU, and creates three domain local security groups:
  - <*Facility name*>_<*Instance name*>_Config
  - <*Facility name*>_<*Instance name*>_Setup
  - <*Facility name*>_<*Instance name*>_Service

The Domain Manager also performs the following operations:

- Adds <*Facility name*>_<*Instance name*>_Setup to <*Facility name*>_<*Instance name*>_Config, because the setup group needs the permissions for the config group.
- <*Facility name*>_Config group to <*Facility name*>_<*Instance name*>_Config
- <*Facility name*>_Setup group to <*Facility name*>_<*Instance name*>_Setup

The config security group has domain read write permission, so that the user in that group can create a users group as well as OUs in the domain.

For more information, see the chapter Organizational Units.

Open the Domain Manager

To run the Domain Manager, you must be a Domain admin or a domain user who has domain read write permission, so you can create OUs and groups.

Procedure

You can open the Domain Manager in the following ways:

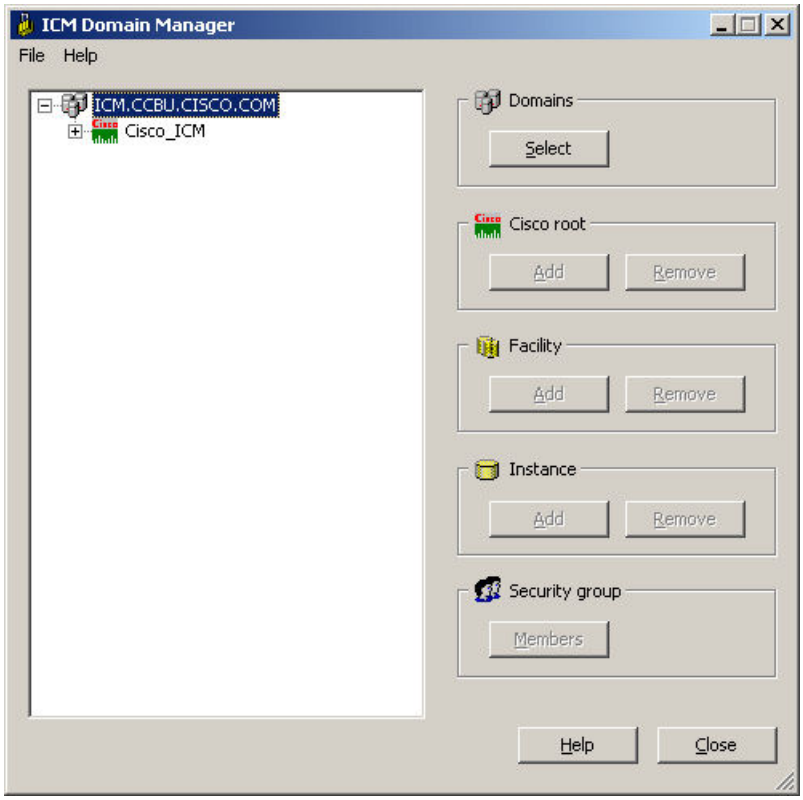
- Open the Domain Manager application from the Cisco Unified Tools folder.
- Access through **Start** > **Programs** > **Cisco Unified CCE Tools** > **Domain Manager**.

Note When the Domain Manager dialog box opens, multiple domains might display in the domain tree in the left pane of the dialog box. The default domain displayed is the domain the current user is logged into.

Domain Manager Window

The Domain Manager dialog box displays the current domain and the Cisco Unified ICM related OUs contained in the domain.

Figure 16: Domain Manager Dialog Box



Domain Manager Tree

The Domain Manager tree display provides a quick view of the Unified ICM created AD OUs and groups in the selected domains. You can display Multiple domains in the tree. The default domain displayed is the current machine domain. When you first expand a domain node, it is validated. The OU Validation Errors dialog box appears only if the error is due to missing or incorrect OU hierarchy information.

A context menu displays when you right-click any object in the Domain Manager tree. These menus provide additional functionality specific to the following level:

- Domains
  - Add Cisco Root
  - Refresh
- Cisco Root
  - Remove Cisco Root
  - Add Facility
  - Security Information
  - Properties
- Facility

- Remove Facility
- Add Instance
- Security Information

- Instance
  - Service Log On Properties
  - Security Information
  - Remove Instance

- Security group
  - Security Group Members
  - Properties

Table 9: Domain Manager Dialog Box Properties

Property	Description
Domains	To add or remove a domain from the Domain Manager tree, click **Select**. The **Select Domains** dialog box appears. For more information, seeView Domains, on page 67.
Cisco Root	To add the Cisco Root when you select a domain that does not already have the Cisco Root, click **Add**. The **Select OU** dialog box appears (for more information, seeCreate or Add Cisco Root, on page 69). To remove the selected Cisco Root and all of its facilities and instances, click **Remove**.
Facility	To add a new facility, select the Cisco Root OU then click **Add**. The **Enter Facility Name** dialog box appears (for more information, seeCreate or Add Facility OU, on page 72). To remove the selected facility and all of its instances, click **Remove**.
Instance	To add an instance, select a facility in the Domain tree display, then click **Add**. The **Add Instance** dialog box appears (for more information, seeCreate Instance OU, on page 73). To remove the selected instance, click **Remove**.
Security group	Click **Members** to display the **Security Group Members** dialog box (for more information, seeAdd Users to Security Group, on page 76) where you assign users to security groups.

Related Topics

View Domains, on page 67
Add Domain to a View, on page 68
Remove Domain from a View, on page 69
Create or Add Cisco Root, on page 69

Create or Add Facility OU, on page 72
Remove Facility OU, on page 72
Create Instance OU, on page 73
Remove Instance OU, on page 74
Add Users to Security Group, on page 76
Remove Members from Security Group, on page 78

View Domains

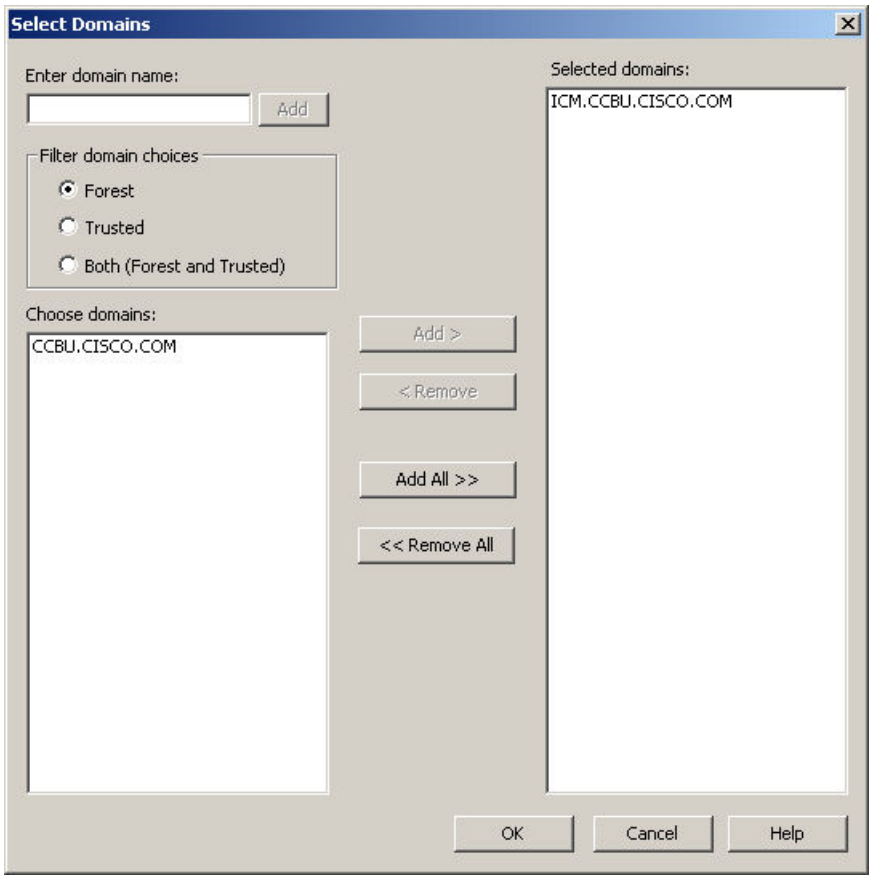
Procedure

Step 1 Open the Domain Manager.

Step 2 In the right top pane of the Domain Manager, click **Select**.

The Select Domains dialog box opens.

Figure 17: Select Domains Dialog Box



You can now add or remove domains for use with the system software.

Table 10: Select Domain Dialog Box Properties

Property	Description
Enter domain name:	Allows you to enter fully qualified domain name. After you enter the qualified domain name, click **Add**. The domain appears in the Choose domains list.
Filter domain choices	• **Forest** – Filters the Choose domains list to display only domains in the same forest. • **Trusted** – Filters the Choose domains list to display only trusted domains. • **Both** – Filters the Choose domains list to display both forest and trusted domains.
Choose domains:	Choose a domain from the displayed list: • **Add >** — Adds domains selected in the Choose domains list to the Selected domains list. • **< Remove** — Removes selected domains from the Selected domains list. • **Add All >>** — Adds all the domains in the Choose domains list to the Selected domains list. • **<< Remove All** — Moves all the domains from the Selected domains list to the Choose domains list.
Selected domains:	Displays a list of all the selected domains.

For more information, see the chapter Domain Manager.

Related Topics

Remove Domain from a View, on page 69

Add Domain to a View

You can add domains by using the controls in the Select Domains dialog box. Follow these steps to add a domain:

Procedure

Step 1 In the left pane under Choose domains, select one or more domains.

Step 2 Click **Add >** to add the selected domains, or click **Add All >>** to add all the domains.

You can also manually type in a domain to add to a view instead of clicking.

Step 3 In the field under Enter domain name, enter the fully qualified domain name to add.

Step 4 Click **Add**.

Step 5 Click **OK**.

The added domains now appear in the Domain Manager dialog box. You can then add the Cisco Root OU.

Related Topics

View Domains, on page 67
Create or Add Cisco Root, on page 69

Remove Domain from a View

You can remove domains by using the controls in the Select Domains dialog box. Follow these steps to remove a domain:

Procedure

Step 1 In the Select Domains dialog box, in right pane under **Selected domains:**, select one or more domains.

Step 2 Click **<Remove** to remove the selected domains, or click **<<Remove All** to remove all the domains.

Step 3 Click **OK**.

The removed domains no longer appear in the Domain Manager dialog box.

Create or Add Cisco Root

You can create the Cisco Root OU either in the domain root, or beneath another OU in the domain.

Note The user who creates the Cisco Root OU automatically becomes a member of the Setup Security Group for the Cisco Root OU. In effect, this user is granted privileges to all Unified ICM tasks in the domain.

Procedure

Step 1 Select the domain you want to add.

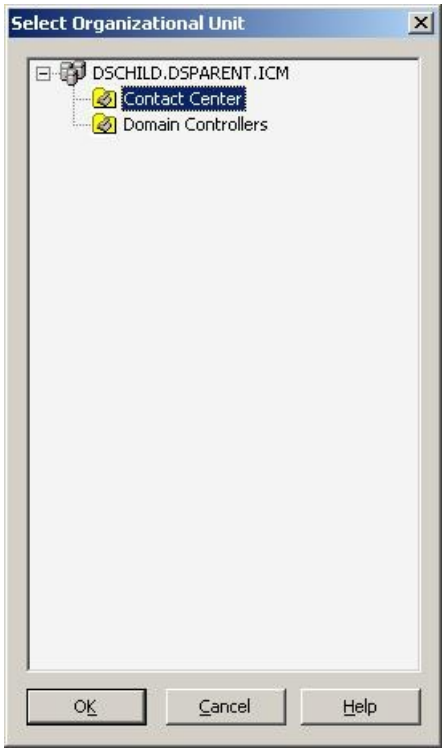
If the current domain, which the Domain Manager loads by default, is not the domain to which you want to add a root, then add a domain to the view.

Step 2 Click the **Cisco Root Add** button. This displays the Select OU dialog box.

Step 3 Click **Add** to add the Root.

The Select Organizational Unit dialog box appears.

Figure 18: Select OU Dialog Box



Step 4 Select the OU under which you want to create the Cisco Root OU, then click **OK**.

When you return to the Unified ICM Domain Manager dialog box, the Cisco Root OU appears either at the domain root, or under the OU you selected in step 3. You can now add facilities and configure security groups.

Note The Domain Administrator is made a member of the Setup group as well.

To access the Cisco Root Properties, right-click the Root node in the main dialog box and select **Properties**. **Add** is disabled if the Root already exists.

Related Topics

Create or Add Facility OU, on page 72
Add Users to Security Group, on page 76

Remove Cisco Root

Note Only users with administrative control at the level above the Cisco Root OU can delete the Cisco Root OU.

Procedure

Step 1 Open the Domain Manager.

Step 2 Select the root in the tree.

Step 3 In the right pane under Cisco Root, click **Remove**.

You are prompted to confirm the removal of the Cisco_ICM OU.

Warning All Unified ICM instances in this domain will no longer work properly if the OU is removed. All users, groups, and other objects in this OU will also be deleted.

Step 4 Click **OK** to confirm the removal.

Create or Add Facility OU

You create a Facility OU to group one or more Instance OUs.

Note You must create at least one Facility OU before you can create a Unified ICM instance.

You must create the Cisco Root OU for the domain before you can create a Facility OU.

Procedure

Step 1 Open the Domain Manager.

Step 2 In the tree view in the left pane, select the Cisco Root OU under which you want to create the Facility OU.

Step 3 In the right pane, under Facility, click **Add**.

The **Enter Facility Name** dialog box opens.

Figure 19: Enter Facility Name Dialog Box

Step 4 Enter the name for the facility.

Note Facility OU names must be 32 characters or less, and cannot contain the characters # , + " < > ; / \ [] : ? *

Step 5 Click **OK**.

The Facility OU is created in the OU tree and shown in the left pane, beneath the Cisco Root OU.

Remove Facility OU

Note Only users with administrative control at the level above the Facility OU might delete the Facility OU.

Procedure

Step 1 Open the Domain Manager.

Step 2 In the tree view in the left pane, navigate down the tree to find and select the Facility OU you want to delete.

Step 3 In the right pane, under Facility, click **Remove**.

You are prompted to confirm the removal.

Warning All Unified ICM instances in this facility will no longer work properly if the OU is removed. All users, groups, and other objects in this OU will also be deleted.

Step 4 Click **OK** to confirm the removal.

The Facility OU is removed from the tree.

Create Instance OU

You can create an Instance OU while creating a Unified ICM instance, or before you create the Unified ICM instance.

Procedure

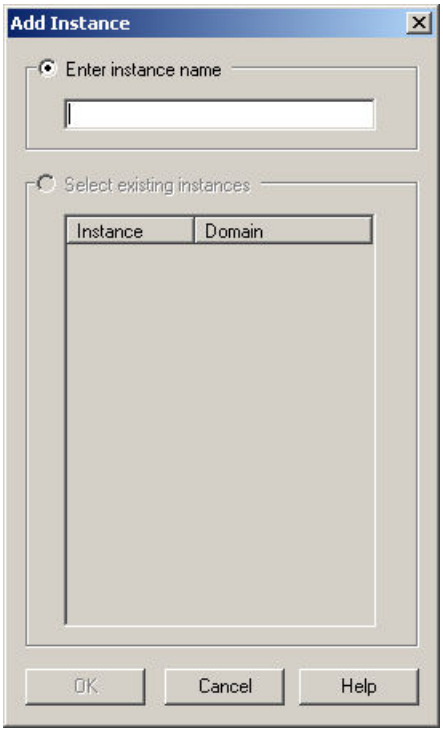
Step 1 Open the Domain Manager.

Step 2 In the tree view in the left pane, navigate to and select the Facility OU under which you want to create the Instance OU.

Step 3 In the right pane, under Instance, click **Add**.

The Add Instance dialog box opens.

Figure 20: Add Instance (Organizational Unit) Dialog Box



Step 4 At this point, you have two options:

a) If you are installing Unified ICM on the current computer for the first time, under the **Enter instance name** radio button, enter the instance name.

Note The Instance OU name must be five alpha-numeric characters or less, cannot begin with a numeric character, and cannot be a reserved name such as local or sddsn.

b) If you are upgrading an existing Unified ICM instance, the instance is listed under the **Select existing instances** radio button. In this situation, select **Select existing instance**, then select the Unified ICM instance from the list.

Step 5 Click **OK**.

The Instance OU is added below the selected Facility OU.

Remove Instance OU

Procedure

Step 1 Open the Domain Manager.

Step 2 In the tree view in the left pane, navigate down the tree to find and select the Instance OU you want to delete.

Step 3 In the right pane, under Instance, click **Remove**.

You are prompted to confirm the removal.

Warning This Unified ICM instance will no longer work properly if the OU is removed. All users, groups, and other objects in this OU will also be deleted.

Step 4 Click **OK** to confirm the removal.

The Instance OU is removed from the tree.

Security Groups

A security group is a collection of domain users to whom you grant a set of permissions to perform tasks with the system software.

For each security group, you add a set of domain users who are granted privileges to the functions controlled by that security group. The Security Group Members dialog box displays the list of groups that are members of the security group selected in the Domain Manager main dialog box. You can add and remove users from the selected group using this dialog box.

Figure 21: Security Group Members Dialog Box

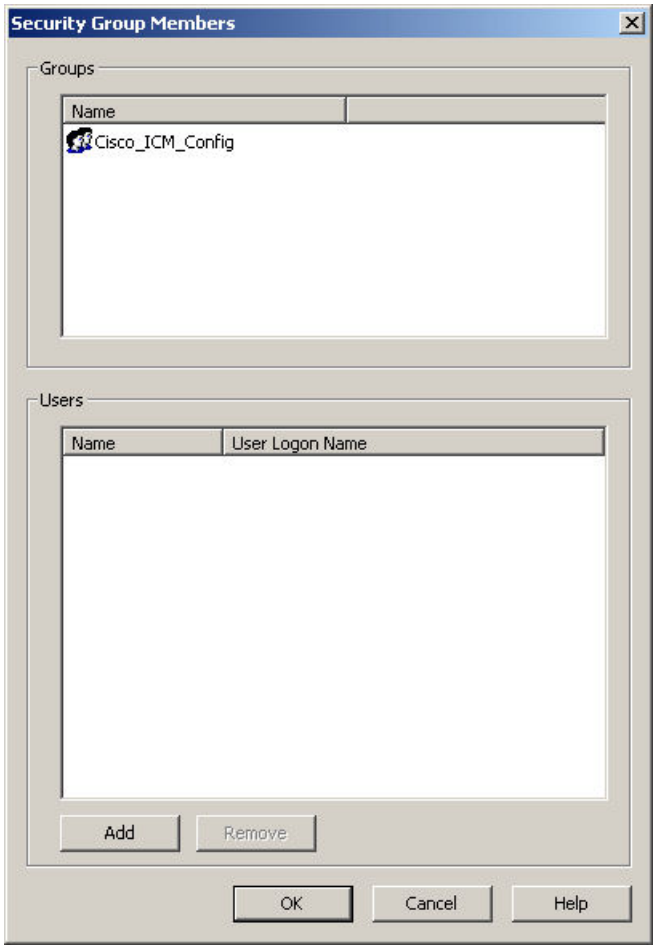


Table 11: Security Group Members Dialog Box Properties

Property	Description
Groups	Displays groups that are members of the security group selected in the Domain Manager main dialog box
Users	Displays the name and user login name of the user.
Add	Use this option to add members to the Security Group.
Remove	Use this option to remove members from the Security Group.
OK	Use this option to save changes and return to Domain Manager.

Related Topics

Add Users to Security Group, on page 76

Add Users to Security Group

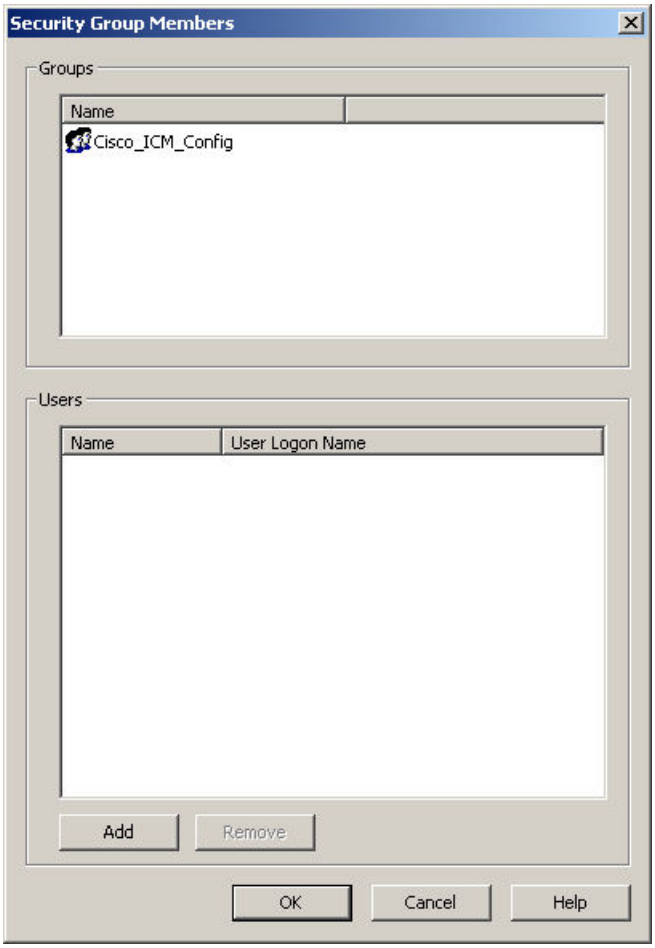
Procedure

Step 1 In the Domain Manager, select the Security Group you want to add a user to.

Step 2 Click **Member** in the Security Group pane of the ICM Domain Manager.

The Security Group dialog box appears.

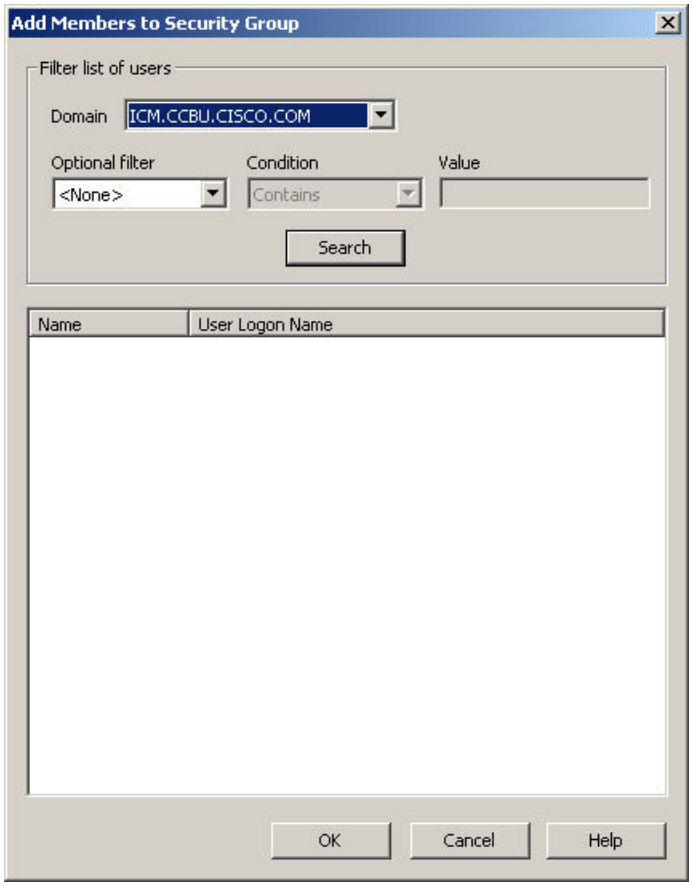
Figure 22: Security Group Members Dialog Box



Step 3 In the Users pane, select **Add**.

The Add Members to Security Group dialog box appears.

Figure 23: Add Members to Security Group Dialog Box



Step 4 Select the filters that are used to create a list of users to select from.

- **Domain** – Select the domain you want to add as a member to the Security Group.
- **Optional filter**

  Select the optional filter you want to use:

  - **<None>** – No additional filter selections applied, Condition and Value inaccessible.
  - **Name** – Continue and search the appropriate Condition and Value. This filter is based on the username of the user.
  - **User Login Name** – Continue and search the appropriate Condition and Value. This filter is based on the username of the user.

- **Condition**

  Select the condition to facilitate your search for the member you want to list:

  - **Contains** – find and list members containing the entered Value.
  - **Starts with** – find and list members whose name or user login name starts with the entered Value.
  - **Ends with** – find and list members whose name or user logon name ends with the entered Value.

- **Value**

  Enter the appropriate value to search on, for example, enter the first name of the user you want to add. This value provides a list of members with that name for you to choose from.

Step 5 Select the member you want to add to the Security Group from the displayed list.

Step 6 Click **OK** to add the selected member to the Security Group.

Remove Members from Security Group

Procedure

Step 1 In the Domain Manager, select the Security Group from which you want to remove members.

Step 2 In the Security Group pane of the Domain Manager dialog box, select **Members**.

The Security Group dialog box appears.

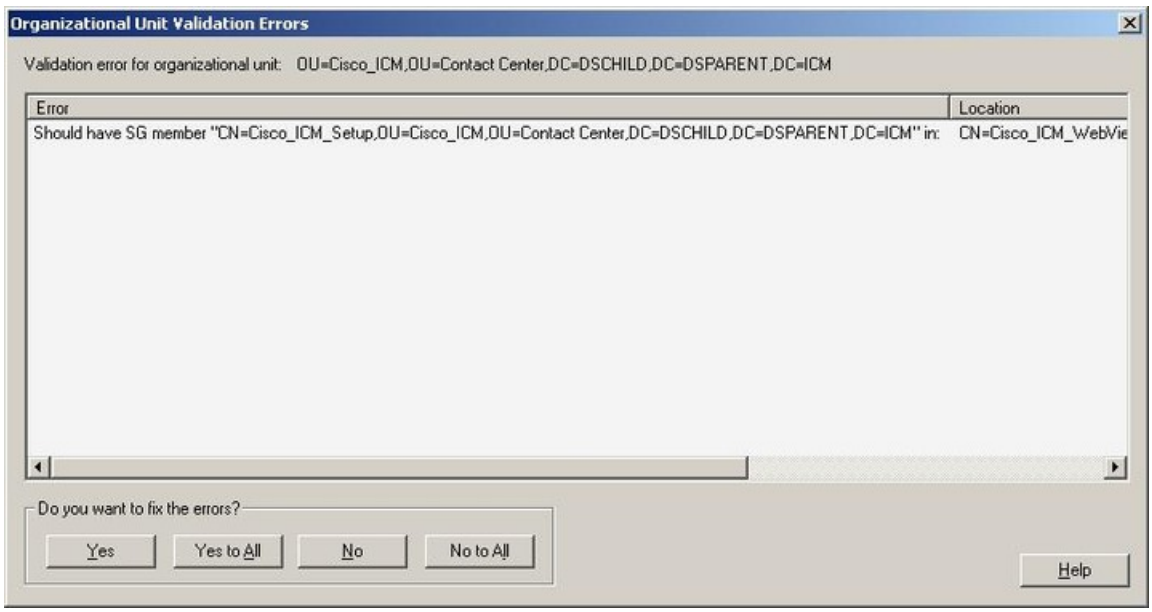
Step 3 In the Users pane, select the member you want to remove from the Security Group.

Step 4 Click **Remove**.

Step 5 Click **OK** to remove the selected member from the Security Group.

Organizational Unit Validation Errors Dialog Box

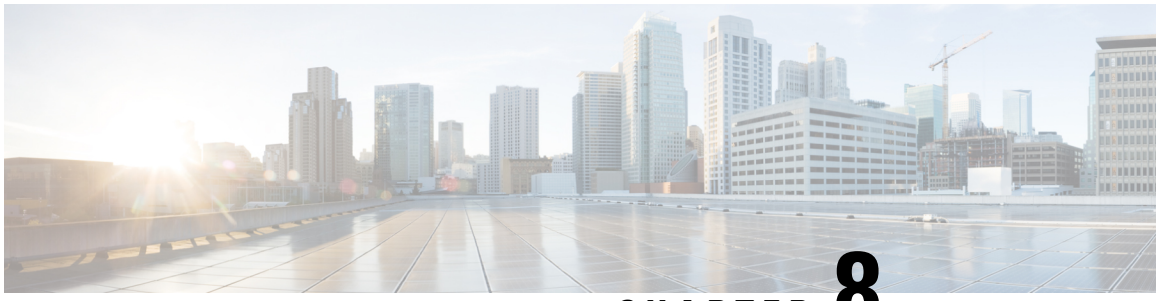
Figure 24: Organizational Unit Validation Errors Dialog Box



This dialog box appears if errors are found during OU validation.

Table 12: Organizational Unit Validation Errors Dialog Box Properties

Property	Description
Validation error for organizational unit:	Displays the OU containing the error found during OU validation.
Error	Displays description of errors found during OU validation.
Location	Displays the location of each error found during OU validation.
Do you want to fix the errors?	Four possible responses: • **Yes** – Fixes the displayed error then attempts to sequentially validate the next OU. If more errors are found, you return to this dialog box. • **Yes to All** – Recursively fixes the displayed error and any errors found during sequential validation attempts for other ICM OUs without returning to this dialog box. • **No** – Does not fix the displayed error but attempts to sequentially validate the next OU. If more errors are found, you return to this dialog box. • **No to All** – Does not fix the displayed error but recursively validates the OUs and logs any additional errors without returning you to this dialog box.



CHAPTER 8

Local Machine Authorizations

Unified CCE supports local authorization that does not involve any Domain security groups for user permissions. All the permissions and privileges are handled by the security groups on the local machines.

- UcceService Group, on page 81
- UcceConfig Group, on page 81
- Local Administrators Group, on page 81

UcceService Group

This security group is created during the installation or upgrade process, in the local machines. The `UcceService` group applies to Fresh Installations as well as all upgrades including Technology Refresh and other supported upgrade paths from an earlier releases.

The `UcceService` group is used to provide permissions and privileges to the service accounts associated with the Logger and Distributor services. For a new installation, the domain service accounts for the Logger and Distributor services must be added to this group. All the permissions required for the service accounts are configured for the `UcceService` group.

UcceConfig Group

The `UcceConfig` group is created during the fresh installation in all local machines. For upgrades, this group already exists in local machines. The `UcceConfig` group is required only for Distributor machines.

The `UcceConfig` group is used to provide local authorization with the necessary permissions and privileges to the Unified CCE configuration users.

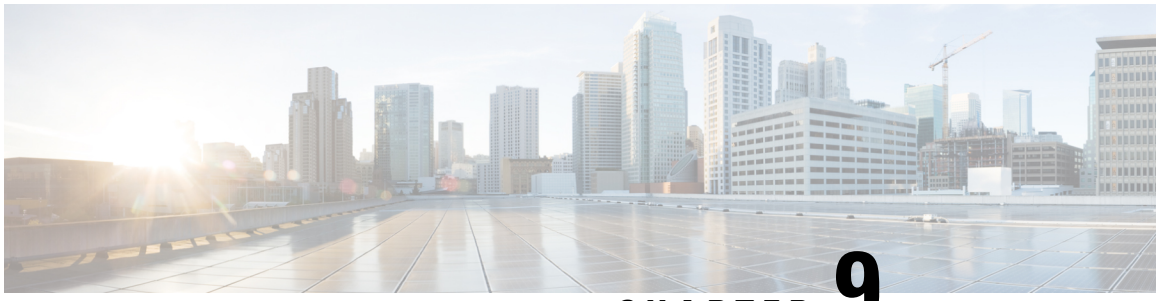
The permissions for registries and local folders must be configured manually. For steps to configure the permissions, see the Configuration Guide for Cisco Unified ICM/Contact Center Enterprise.

Local Administrators Group

Setup users are domain users with local administrator permissions and can run the UCCE installer, Websetup, and Peripheral Gateway Setup tools.

To make a domain user a setup user, you have to manually add the domain user to the Local Administrators Group. This enables the domain user to perform the UCCE setup operations such as, running the Websetup and Peripheral Gateway Setup tools.

Note Domain Administrators can perform UCCE setup operations such as, running the Websetup and Peripheral Gateway Setup tools.



CHAPTER 9

Staging Prerequisites

- System Design Specification, on page 83
- Platform Hardware and Software, on page 84
- Set Staging Environment, on page 85

System Design Specification

Before you begin the Unified ICM staging process, ensure that a Unified ICM/Cisco Unified Contact Center Enterprise System Design Specification is created and approved.

Persons creating and approving this specification must be familiar with the following:

- Windows Operating System
  - AD
  - Security concepts
  - Network configuration and operation
- SQL Server
  - Enterprise Manager
  - Query Analyzer
  - SQL scripting
- Unified ICM/Cisco Unified Contact Center Enterprise
  - Unified ICM/Cisco Unified Contact Center Enterprise Nodes (Router, Logger, Administration & Data Server, PGs)
  - HDS Schema knowledge
  - Deployment models
  - The appropriate release of the*Contact Center Enterprise Compatibility Matrix* and *Solution Design Guide for Cisco Unified Contact Center Enterprise*.

The System Design Specification must contain the following specifications:

- Description of Unified ICM Sites and Nodes
- Data Communications Infrastructure
- Event Notification and Remote Access Points
- Naming Conventions
- IP Addressing Scheme
- AD Plan, including:
  - AD Sites
  - Global Catalog Servers
  - Domain Controllers
  - Trust Relationships
  - Domain Members
  - Standalone Servers
  - Time Source
- DNS Plan (follow Microsoft Guidelines), including:
  - DNS Servers and Clients
  - DNS Forward and Reverse Lookup Zones and Records
- System Diagrams
- Configuration Settings, including:
  - Physical Controller IDs
  - Logical Controller IDs
  - Peripheral Controller IDs
- Third-party Host Forms – A section containing the detailed build information for each server containing the entries and values for fields which are different from defaults presented during third-party software installation and setup. Some examples of this information include: Network Card configuration and binding order, Drive Partitioning Information, System Properties, and passwords.

Platform Hardware and Software

During the System Design phase of the Unified ICM/CCE deployment, you define the hardware specifications, virtualization environment, and third-party software requirements. For supported third-party software, see the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html. For information about Unified ICM/CCE virtualized systems, see the *Virtualization for Unified Contact Center Enterprise* at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.

Set Staging Environment

Procedure

Step 1 Stage all computers in racks or on a work surface.

Step 2 Ensure that all software CDs, driver software, and documentation are in the work area.

Step 3 Ensure that you have all software license numbers available.

Step 4 Ensure that the Unified ICM network is in place and tested. Check that:

- All LAN switches are configured for required subnets per the System Design Specification.
- All IP Routers are configured as required.
- There's IP connectivity between all subnets.
- Required Ethernet connections are in place between Unified ICM software servers and LAN switches.
- Required packet prioritization is configured on IP Routers.

Note Latency is critical for contact center operations, so you must disable the Large Receive Offload (LRO) settings.

Step 5 To disable LRO, log in to the ESXi host or its vCenter with vSphere Client.

Step 6 Select the host and choose **Configuration** > **Advanced Settings**.

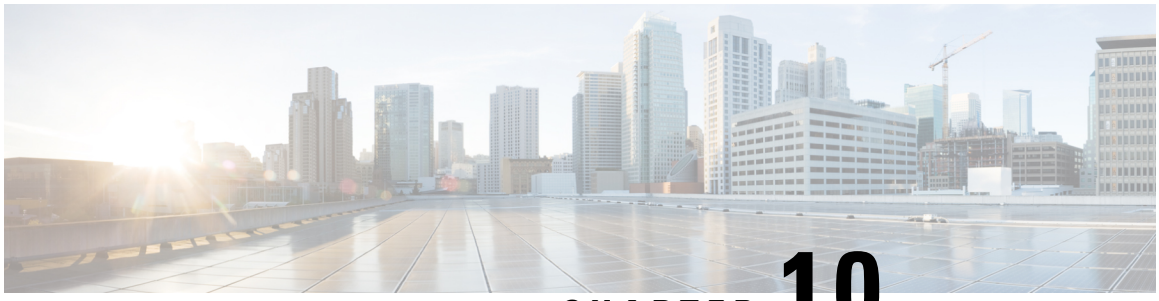
Step 7 Select **Net** and scroll down slightly to set the following parameters from 1to 0:

- Net.VmxnetSwLROSL
- Net.Vmxnet3SwLRO
- Net.Vmxnet3HwLRO
- Net.Vmxnet2SwLRO
- Net.Vmxnet2HwLRO

Step 8 Reboot the ESXi host to activate the changes.

Step 9 Ensure that assigned engineers follow the specifications in these documents:

- *Solution Design Guide for Cisco Unified Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html
- *Virtualization for Unified Contact Center Enterprise* at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html
- *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html



CHAPTER 10

Microsoft Windows Server Staging

- Drive Partition Guidelines, on page 87
- Windows Setup Guidelines, on page 88
- Join Standalone Servers to Domain in Microsoft Windows Server , on page 89
- Set Persistent Static Routes, on page 90
- Collect Existing SNMP Properties, on page 90
- Display Settings, on page 92
- System Properties, on page 92
- Configure Event Viewer, on page 93
- Connectivity Validation, on page 93

Drive Partition Guidelines

Create drive partitions for the servers being built according to settings in the Unified ICM/Cisco Unified Contact Center Enterprise System Design Specification.

Format C drive as NTFS.

Note You might need to use the manufacturer's drive partitioning/RAID array software to set up the partition.

Logger or Administration and Data Server Partition Guidelines

For servers hosting a Logger or Administration & Data Server (Historical Data Server (HDS)), use the following guidelines for partitioning:

- Use the C drive for the operating system, virtual memory paging file size, core Unified ICM, Microsoft SQL Server, and Microsoft SQL Server log and temp files.
- Use the D drive to store the Logger or Historical Data Server database.

Note Keep the Microsoft SQL Server temp and log files on the C drive to maximize database performance.

Partition Guidelines for Other Contact Center Components

For servers hosting a Router, Peripheral Gateway, Administration & Data Server (non-Historical Data Server), CTI Server, and CTI OS Server, use a single partition C drive for the operating system, virtual memory paging file size, core Unified ICM software, the Administration & Data Server database, Microsoft SQL Server, and Microsoft SQL Server log and temp files.

Windows Setup Guidelines

Note For additional information on installing and upgrading Microsoft Windows Server, see the Microsoft Windows Server homepage.

Use the following guidelines when setting up a Microsoft Windows Server for Unified ICM:

- When setting the time zone, ensure that all Central Controller systems are set for the same time zone regardless of their physical location.
- Ensure that the time zone is set the same on PG A and PG B for all peripheral gateway pairs to enable synchronization of Unified ICM Message Delivery Service (MDS) processes.
- For Network Settings, enter the server respective IP and DNS data according to the System Design Specification.
- For the Public Ethernet Card, perform the following tasks:
  - To enter the data for visible IP addresses, subnet mask, default gateway and preferred and alternate DNS servers for the server, click **Start** > **Control Panel** > **Network and Sharing** > **Change Adapter Settings** and then right-click on the Visible network **Properties** > **Internet Protocol version 4 (TCP/IPV4)**, and select **Properties**.
  - In the **Advanced** tab, enter the “high” visible addresses.
  - In the **DNS** tab, for **DNS suffix for this connection**, enter the name of the local DNS zone for the server and check **Register**.
  - If the server requires access to resources in a different trusting or trusted domain or DNS zone, select **append these DNS suffixes (in order)** and enter the local DNS zone for the server first, then add the other secondary zones which represent the trusting or trusted domain.
- If the server has more than one network interface card, for the Private Ethernet Card click **Start** > **Control Panel** > **Network and Sharing** > **Change Adapter Settings**, right-click on the Private network and select **Properties**, and perform the following tasks:
  - Uncheck the **Client for Microsoft Networks** and the **File and Print Sharing** options.
  - For TCP/IP properties, enter the private IP address and subnet mask for the server. Leave the default gateway field blank.
  - In the Advanced tab, enter the “high” private addresses.
  - In the DNS tab, leave the address space empty and uncheck **Register**.

- Because the ICM platform does not directly support IP V6, disable IPV6 on all the Ethernet cards. On the **Adapter Settings** dialog, right-click the card and select **Properties**. Uncheck **Internet Protocol Version 6 (TCP/IPV6)**.

Related Topics

Enable SNMP Management on Microsoft Windows Server, on page 89

Enable SNMP Management on Microsoft Windows Server

Unified ICM/CCE SNMP support automatically installs during setup—you do not need to take extra steps during setup to enable SNMP support. The Microsoft Windows SNMP service is disabled as part of web setup and is replaced by the Cisco Contact Center SNMP Management service to process SNMP requests in its place.

However, you must install Microsoft Windows SNMP optional components on Unified ICM/CCE servers for any SNMP agents to function. The Microsoft SNMP components are required for Cisco SNMP support. You must install these Microsoft SNMP components before you install any Unified ICM/CCE components that require SNMP monitoring.

To install Microsoft SNMP components:

Procedure

Step 1 Choose **Start** > **Control Panel** and then click **Programs and Features**.

Step 2 Click **Turn Windows features on or off**.
The **Server Manager** opens, followed by the **Add Roles and Features Wizard**.

Step 3 Click **Next** to proceed through the wizard until you reach **Select Features**.

Step 4 In the **Features** list, select **SNMP Service** and **SNMP WMI Provider**.

Step 5 Click **Next**, and then click **Install**.

Join Standalone Servers to Domain in Microsoft Windows Server

The following components must be installed on servers that are members of the domain:

- Logger
- CallRouter
- Administration & Data Servers

Procedure

Step 1 Click Start, right-click **Computer** and choose **Properties**.

Step 2 In the section “Computer name, domain, and workgroup settings” click **Change settings**.

Step 3 Click **Change**.

Step 4 In the “Member of” section, select **Domain** then enter the Fully Qualified Domain Name and click **OK**.

Step 5 Enter the Domain Administrator's username and password.

Step 6 Reboot the server and sign in to the domain.

Set Persistent Static Routes

For geographically distributed Central Controller sites, redundant CallRouter, Logger, and Peripheral Gateway components typically have a Private IP WAN connection between Side A and Side B. Windows only allows one default gateway for each VM (which sends the Private Network traffic to the Public Network). So, you add a Static Route to all the VMs running the CallRouter, Logger, and PG applications.

To create a persistent static route with the **route add** command, you need the destination subnet, the subnet mask, the local gateway IP, and the interface number of the local Private Network interface:

```
route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p
```

Procedure

Step 1 On each CallRouter, Logger, or PG VM, run `ipconfig /all`.
Record the `IPv4 Address`, `Subnet Mask`, and `Physical Address` (MAC address) for the Private Network interface.

Step 2 On each of these VMs, run `route print -4`.
Record the `Interface` for the Private Network. You can identify the correct interface by looking for its `Physical Address` (MAC address).

Step 3 On each of these VMs, run `route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p` to add a persistent static route for the remote Private Network.

Collect Existing SNMP Properties

If you already installed and configured SNMP management support for this server, collect the existing configuration parameters so you can use them to configure the components installed by Web Setup. You can find these parameters on the property sheets associated with the Microsoft SNMP Service.

Note For Microsoft Windows Server, to view the SNMP Agent Management snap-in, use the 32-bit Microsoft Management Console Snap-In. To launch the 32-bit Snap-in, run mmc /32. For detailed instructions for Microsoft Windows Server, consult your Microsoft documentation.

To collect existing SNMP properties:

Procedure

Step 1 On the Services MMC console, do one of the following:

- Locate and select the **SNMP Service** in the list, or
- Choose **Start** > **Programs** > **Control Panel** > **Administrative Tools** > **Services**.

Step 2 On the SNMP Service Properties dialog box, select the **Security** tab.

Note the following settings and configuration data:

- The state of the **Send authentication trap** check box.
- The Accepted community names.
- If **Accept SNMP packets from these hosts** is checked, collect the host names or IP addresses configured in the associated list box.

  Note To configure Cisco SNMP agents if you configured host names (versus IP addresses), determine the actual IP address of that host. For security reasons, using static addresses for management stations is preferred.

Step 3 Select the **Traps** tab on the SNMP Service Properties dialog box.

Collect the configured trap destinations and the associated community name.

Note If host names were for trap destinations, determine the actual IP address of that host.

Step 4 On the SNMP Service Properties dialog box, select the **Agent** tab.

Collect the information from the Contact and the Location fields.

What to do next

If the server has not been configured for SNMP manageability, do the following:

1. Determine whether SNMP manageability is required.
2. Acquire the necessary configuration information to enable SNMP access.

The necessary configuration information includes:

- The IP addresses of the management station.
- If using SNMP v1 or SNMP v2c:
  - Community names (if using SNMP v1 or SNMP v2c)
  - Trap destinations and the community name expected by each management station
- If using SNMP v3:
  - Usernames
  - Authentication protocol used (if authentication is required)
  - Privacy protocol used (if privacy is required)

- Trap destinations and the username expected by each management station

The installed Microsoft Management Console Snap-In (Cisco SNMP Agent Management) is used to configure the SNMP properties. See the *SNMP Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html for more details.

Display Settings

Through the Windows Control Panel Display dialog box:

- Ensure that no screen saver is selected.
- Set the Administration & Data Server display for at least 1024 by 768 pixel resolution.
- Set at least 65K colors and at least 60 MHz.

System Properties

For Virtual memory settings:

- Click **Start** > **Control Panel** > **System** > **Advanced System Settings** > **Performance** > **Advanced** > **Virtual Memory**.
- Next, select **Change** and set the initial and maximum page file sizes to appropriate values based on the system memory. See Microsoft documentation for guidance on page file sizes.

Note Microsoft recommends the paging file size to be at least 1.5 times the VM memory.

For Startup and Recovery settings:

- Click **Start** > **Control Panel** > **Advanced System Settings** > **Startup and Recovery** > **Settings**.
- Next, set the value of the **Time to display list of operating systems** to **3** seconds.

Note Click **Start** > **Control Panel** > **System** > **Advanced System Settings** > **Performance** > **Advanced**. Confirm that the **Adjust for best performance** option is set to either **Programs** or **Background Services**.

Configure Event Viewer

Procedure

Step 1 For each type of event, set the **Maximum log size** to **8192 KB**.

Step 2 Select **Overwrite events as needed**.

Note See the Security Guide for Cisco Unified ICM/Contact Center Enterprise available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-technical-reference-list.html for additional information.

Connectivity Validation

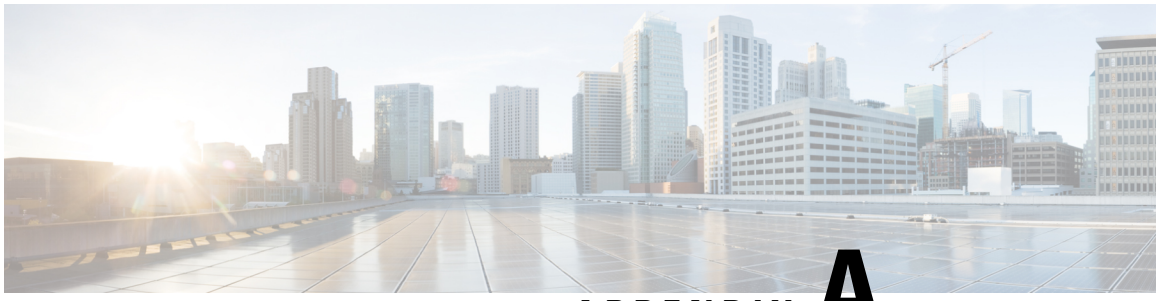
Before you begin the Unified ICM installation process, validate network connectivity for all servers that are part of the Unified ICM system.

On each server:

- Validate the TCP/IP properties for each network card, including the DNS settings.
- Validate that you can ping each machine on the visible network.
- If applicable, validate that you can ping each private network connection.
- Test remote access.

Related Topics

System Design Specification, on page 83



APPENDIX A

Domain Controller Installation on MS Windows Server

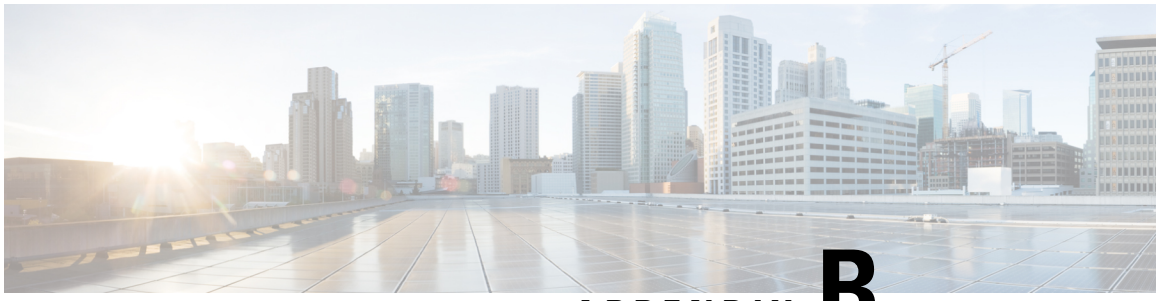
• Install Domain Controller on Microsoft Windows Server, on page 95

Install Domain Controller on Microsoft Windows Server

Before you install the Domain Controller, ensure that the host has a static IP address and then configure the Preferred DNS Server at that static IP address.

See Microsoft documentation for instructions on installing Domain Controller on Microsoft Windows Server.

Domain Controller Installation on MS Windows Server



APPENDIX B

Moving the Cisco Root OU

- Introduction, on page 97

Introduction

This section describes the instructions to move the Cisco Root OU safely from one OU to another within the same domain. The procedure involves moving the OU in which ICM is installed to another (created or existing) OU, and then moving the Unified ICM into the destination OU.

Warning Moving the Cisco Root OU is only supported if the OU is moved within the same domain. Transferring an OU from one domain to another is not supported.

Definitions

This section defines the terms used in the movement of Cisco Root OU:

Cisco Root OU

The OU contains all Unified ICM created domain resources. The OU defines the permissions for all Unified ICM instances. When you use this tool, you determine which uses a Cisco Root OU named “Cisco_ICM”. Only one Cisco Root OU exists in each domain.

Domain Manager

A tool for creating all Cisco OUs along with their associated groups and permissions. This tool helps you to determine which users in your corporate domain have access rights to perform Unified ICM-related tasks.

Requirements and Prerequisites

The instructions in this document are subject to the following requirements and prerequisites:

- The OU might only be transferred to a new location within the same domain.
- Stop all Unified ICM Services and applications before following these instructions. For duplexed systems, stop both the primary and secondary systems.

- Obtain and record the Instance Number of each Unified ICM instance on the system.

Preparatory Steps

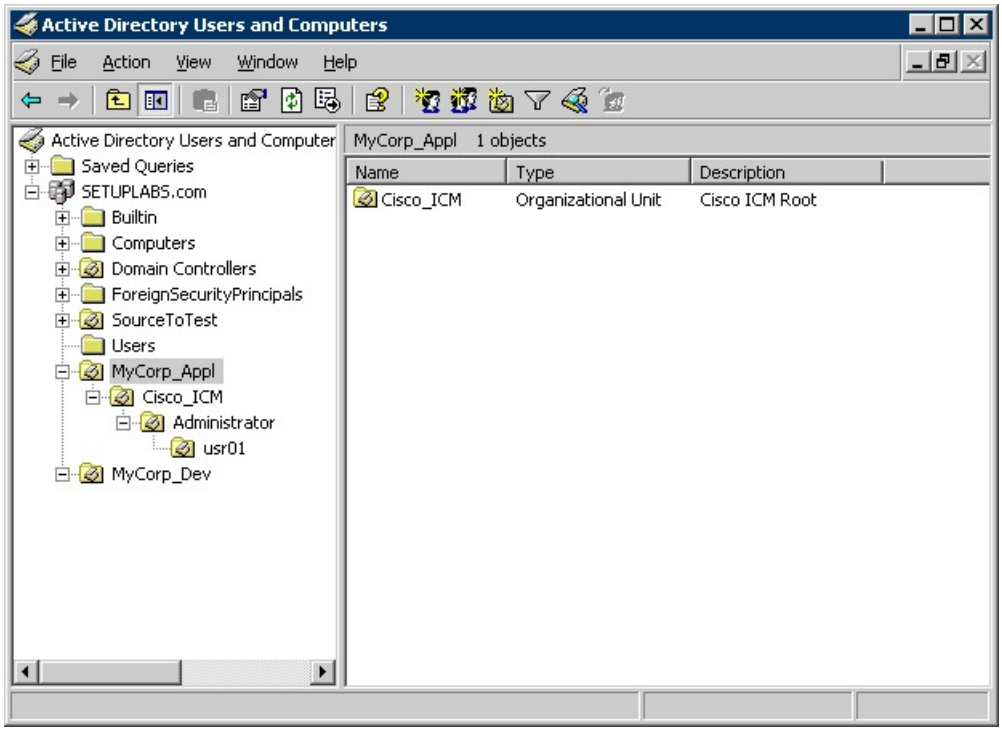
Before moving the OU:

1. Stop all Unified ICM Services before removing the OU.
2. Reset the permissions for the users using the User List Tool.
   - Run Web Setup to edit each component of each instance to reset the service account to the new OU.
   - Start all Unified ICM Services.
   - Run the **Configuration Manager** tool.
   - Run the **User List** tool and re-establish the permissions for individual users to ensure all the users in the User List Tools have the correct permissions.

Transfer Cisco Root OU to Another OU

As an example, see the following diagram which illustrates the domain SETUPLABS. Assume that the original Cisco Root OU was created under the OU MyCorp_Appl. The task is to move Cisco_Root OU from MyCorp_Appl into a new OU called MyCorp_Dev.

Figure 25: SETUPLABS Domain



Procedure

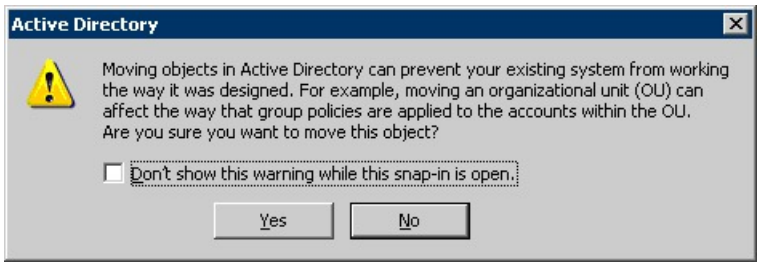
Step 1 On the Domain, find the OU in which the Cisco Root OU is contained.

Step 2 Stop all Unified ICM services and applications on the Unified ICM system.

Step 3 On the domain **SETUPLABS.com**, drag and drop **Cisco_ICM** from **MyCorp_Appl** to **MyCorp_Dev**.

The following message is displayed.

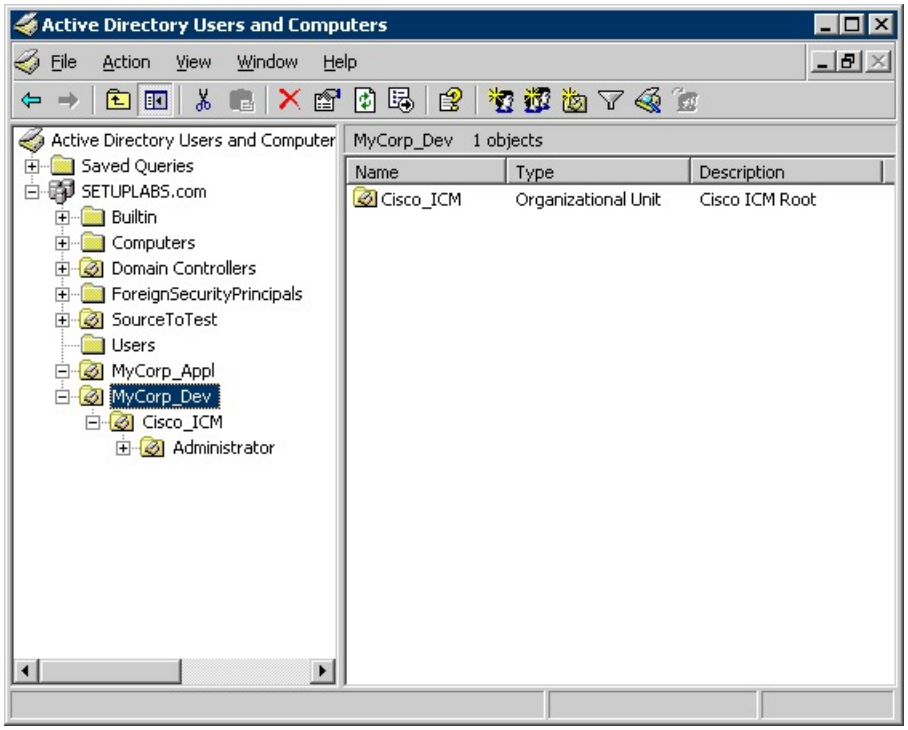
Figure 26: AD Moving Objects Error Message



Step 4 Click **Yes** to continue.

The following diagram illustrates the current location of the Cisco Root OU.

Figure 27: Cisco Root OU Location



Step 5 On all the CCE machines, run Web Setup. Open the Instance Management page.

Moving the Cisco Root OU

Figure 28: ICM Setup Dialog Box

Step 6 Select the existing instance being used.

Step 7 Click **Edit**.

Step 8 Edit the **Facility** or the **Instance Number** fields.

You cannot edit the **Domain** field.

Step 9 After making any desired changes, click **Save**. You return to the Instance List page.

Step 10 Start all Unified ICM/CCE services.

Step 11 Run the **Configuration Manager** tool.

Step 12 As the permissions for the users in the User List were lost, run the **User List** tool and re-establish the permissions for individual users. When you re-establish the permissions, ensure that all the users in the User List Tools have the correct permissions.