Staging Guide
for Cisco Unified ICM/Contact Center Enterprise & Hosted

Release 8.x(y)

June 2012

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: 408 527-0833

Table of Contents

List of Figures

Preface

Purpose

This document contains system diagrams, staging steps and sample test cases for supported models of Unified Contact Center Enterprise/Hosted. The supported models are:

- Dedicated Forest/Domain Model
- Child Domain Model
- Hosted Network Applications Manager (NAM)/ Customer ICM (CICM) Model

Note: This document is intended for the individuals responsible for staging deployments of Cisco Unified Intelligent Contact Management Enterprise/Hosted (Unified ICM/ICMH). Individuals must be trained on the use and functions of Unified ICM as well as Windows Server 2003 SP2, Windows Server 2008, Windows Server 2008 R2 SP1, Active Directory (AD), and DNS. This document does not provide detailed Cisco Unified Intelligent Contact Management Enterprise (Unified ICM), Hosted NAM/CICM, or Windows Server 2003 SP2 specific information. This information can be found elsewhere in specific documentation from Cisco and/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:

- Hosted NAM/CICM Model
- Cisco Unified ICM Scripting and Configuration Tools

- Cisco Unified ICM WebView and third party software (if installed)

  Note: Webview is not supported in Release 8.5(x) or later and is not supported on Windows Server 2008 R2.

- Windows Server 2003 SP2, Windows Server 2008 R2, and Windows Active Directory administration

- Microsoft SQL Server administration

Note: The information in this guide does not pertain to specifics of Cisco Unified System Contact Center Enterprise (Unified SCCE) deployments. The Cisco IPCC Enterprise Web Administration Tool is used for administering Unified SCCE. (Unified SCCE Release 7.5 is supported in the 8.0(1) solution.) For information on Unified SCCE staging deployments, see the documentation for Unified SCCE Release 7.5(1).

Organization

Chapter	Description
Chapter 1: About Active Directory for Unified ICM (page 9)	Provides an overview of AD, the benefits of using it, and the versions supported by Unified ICM.
Chapter 2: Domain Requirements and Supported Topologies (page 13)	Provides the domain and AD requirements for Unified ICM. Discusses Unified ICM requirements for Group Policy in AD, DNS requirements, and the supported domain topographies. Provides the steps necessary to configure AD sites, assign the Global Catalog and FSMO roles, configure the time source, change domain controllers to Native mode, and configure the DNS server on the forest root domain controller.
Chapter 3: About Organizational Units (page 39)	Covers Organizational Units (OU), the OU hierarchy, the Cisco Root OU, Facility and Instance OUs, and how they relate to Unified ICM.
Chapter 4: User Migration Tool (page 51)	Provides information on and how to use the User Migration Tool.
Chapter 5: Service Account Manager (page 67)	Provides information on and how to use the Service Account Manager (SAM).
Chapter 6: About Web Setup and Active Directory (page 83)	Covers how to prepare to work with AD; how the Web Setup, the Domain Manager, and the OU hierarchy relate, and a listing of the functions of the Domain Manager.
Chapter 7: About the Domain Manager (page 85)	Discusses the theory of operation and use of the Domain Manager.
Chapter 8: Handling the User List Tool and Agent Explorer in Multi-Instance Situations (page 101)	Discusses the LimitUserAssociationBy Instance registry key and its ability to restrict associating or adding a duplicate user to multiple instances.
Chapter 9: About Staging Prerequisites (page 105)	Discusses system design specification, the hardware and software platform requirements, and how to set the staging environment.
Chapter 10: About Windows Server 200/2008 R2 Staging (page 109)	Provides the information necessary to stage a Windows Server 2003 or Windows Server 2008 R2 system in preparation prior to installing Unified CCE.

Chapter	Description
Chapter 11: About Microsoft SQL Server Staging (page 123)	Provides the information necessary to properly stage a system in preparation for installing SQL Server 2003.
Appendix A: How to Install the Domain Controller on Windows Server 2003 SP2 (page 129)	Discusses the steps required to install the Domain Controller on Windows Server 2003 SP2.
Appendix B: Moving the Cisco Root OU (page 131)	Provides the necessary information and steps required to move the Cisco Root OU from one OU to another within the same domain.

Related Documentation

Documentation for Cisco Unified ICM/Unified Contact Center Enterprise & Hosted, as well as related documentation, is accessible from Cisco.com at **http://www.cisco.com/cisco/web/psa/default.html?mode=prod**.

- Related documentation includes the documentation sets for Cisco CTI Object Server (CTI OS), Cisco Agent Desktop (CAD), Cisco Agent Desktop - Browser Edition (CAD-BE), Cisco Unified Contact Center Management Portal, Cisco Unified Customer Voice Portal (Unified CVP), Cisco IP IVR, Cisco Support Tools.

  For documentation for the above Cisco Unified Contact Center Products, go to **http://www.cisco.com/web/psa/products/index.html** (http://www.cisco.com/web/psa/products/index) and choose **Products > Voice and Unified Communications > Customer Contact > Cisco Unified Customer Contact Center Products**. Click the product/option you are interested in.

- The documentation for Cisco Unified Communications Manager (Unified CM) is available at **http://www.cisco.com/cisco/web/psa/default.html?mode=prodl** (http://www.cisco.com/cisco/web/psa/default.html?mode=prod).

- Technical Support documentation and tools can be accessed from **http://www.cisco.com/en/US/support/index.html**.

- The Product Alert tool can be accessed through (login required) **http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice**.

Important: You must also read and follow the guidelines set forth in the document *Security Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.0(1)* available on **www.cisco.com** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html), before staging your Windows Server 2003 SP2 environment. The Security Best Practices document contains important guidelines for creating a secure Windows Server environment.

Related Documentation

Documentation for Cisco Unified ICM/Contact Center Enterprise & Hosted, as well as related documentation, is accessible from Cisco.com at: **http://www.cisco.com/cisco/web/psa/default.html**.

Related documentation includes the documentation sets for Cisco CTI Object Server (CTI OS), Cisco Agent Desktop (CAD), Cisco Agent Desktop Browser Edition (CAD-BE), Cisco Unified Contact Center Management Portal, Cisco Unified Customer Voice Portal (CVP), Cisco Unified IP IVR, Cisco Unified Intelligence Center. The following list provides more information.

- For documentation for the Cisco Unified Contact Center products mentioned above, go to **http://www.cisco.com/cisco/web/psa/default.html**, click **Voice and Unified Communications**, then click **Customer Collaboration**, and then click **Cisco Unified Contact Center Products** or **Cisco Unified Voice Self-Service Products**, then click the product or option you are interested in.
- For troubleshooting tips for the Cisco Unified Contact Center Products mentioned above, go to **http://docwiki.cisco.com/wiki/Category:Troubleshooting**, and then click the product or option you are interested in.
- Documentation for Cisco Unified Communications Manager is accessible from: **http://www.cisco.com/cisco/web/psa/default.html**.
- Technical Support documentation and tools are accessible from: **http://www.cisco.com/en/US/support/index.html**.
- The Product Alert tool is accessible from (login required): **http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice**.
- For information about the Cisco software support methodology, see *Software Release and Support Methodology: ICM/IPCC* available at (login required): **http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1844/prod_bulletins_list.html**.
- For a detailed list of language localizations, see the *Cisco Unified ICM/Contact Center Product and System Localization Matrix* available at the bottom of the following page: **http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html**.

Product Naming Conventions

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

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

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

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder 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; for example: A *skill group* is a collection of agents who share similar skills • For emphasis; for example: *Do not* use the numerical naming convention • A syntax value that the user must replace; for example: IF (*condition*, *true-value*, *false-value*) • A book title; for example: Refer to the *Cisco CRS Installation Guide*
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays; for example: **`<html><title>Cisco Systems,Inc. </title></html>`** • Navigational text when selecting menu options; for example: **`ICM Configuration Manager > Tools> Explorer Tools > Agent Explorer`**

Convention	Description
< >	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

Obtaining Documentation and Submitting a Service Request

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

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

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

Documentation Feedback

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

ccbu_docfeedback@cisco.com (mailto:ccbu_docfeedback@cisco.com)

We appreciate your comments.

Part 1: Active Directory and Unified ICM

Chapter 1

About Active Directory for Unified ICM

What is Active Directory for Unified ICM?

Microsoft Windows Active Directory (AD) is a Windows Directory Service that provides a central repository to manage network resources. Unified ICM uses AD to control users' 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 more general information on AD. Therefore, the Unified ICM Administrators must be familiar with Microsoft's AD documentation.

See Also

Microsoft Windows Server 2003 Active Directory Web Site (http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx)

or **Microsoft Windows Server 2008 Active Directory Web Site** (http://www.microsoft.com/windowsserver2008/en/us/ad-main.aspx)

What Versions of AD are Supported by Unified ICM?

Unified ICM supports AD for **Windows Server 2003** and **Windows Server 2008**, and **Windows Server 2008 R2 (64-bit)**.

Upgrading Windows Server 2003 to Windows Server 2008 R2 does not require the use of User Migration Tool if the new Windows 2008 R2 servers are connected to the same domain. For information on upgrading domain controllers, see the Microsoft website **Determine Domain**

Controller Upgrade Order at **http://technet.microsoft.com/en-us/library/cc732085(WS.10).aspx**.

See Also

For detailed information on supported platforms for Unified ICM, see the *Hardware & System Software Specification (Bill of Materials) for Cisco Unified ICM/Contact Center Enterprise & Hosted* available on **www.cisco.com** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

What are the Benefits of Using AD?

The benefits of using AD are:

- Support for Corporate Domain Installations (page 10)
- No Domain Administrator Requirement (page 10)
- Flexible and Consistent Permissions (page 10)
- Streamlined Administration (page 11)
- Standard Windows Naming Conventions (page 11)

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. in an existing Windows domain, including the corporate domain, and utilize the AD functionality your network already supports to control access to functions. Decide where to place the collocate resources in your Organizational-Unit (OU) (page 39) hierarchy.

No Domain Administrator Requirement

You need only be a local machine administrator to belong to the setup group for any instance 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 (page 85).

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. Administrators do not need to enter redundant user information. Unified ICM relies on AD for setup, configuration, and reporting permissions; the use of the User List tool is reduced.

Standard Windows Naming Conventions

AD supports standard Windows naming conventions. There are no specific naming requirements for the Unified ICM usernames or the domain name.

Active Directory and Windows Server 2008/ 2008 R2 SP1

Release 8.x(y) supports Active Directory on Windows Server 2008/2008 R2 domain controllers with the domain functional level of Windows Server 2008/2008 R2 SP1.

The improvements in Active Directory 2008/2008 R2 increase the support and security of an Active Directory based network. Windows 2008/2008 R2 supports Read Write Domain Controller (RWDC) and Read Only Domain Controller (RODC) as part of the security enhancements.

Note: None of the RODC deployments of Windows 2008/2008 R2 Server are currently supported by Release 7.5(10). Hence, Client machines must be connected to the Windows 2008/2008 R2 RWDC.

Active Directory support has been enhanced and extended to include:

- Active Directory Domain Services
- Active Directory Lightweight Directory Services
- Active Directory Certificate Services
- Active Directory Federation Services
- Active Directory Rights Management Services

The following sections explain the details of this enhancement under AD 2008/2008 R2 and its impact on Release 8.x(y). Note that Release 8.x(y) does not make use of any other feature enhancements under AD 2008/2008 R2 and remains unaffected by them.

Active Directory Domain Services

Active Directory Domain Services form the core area for authentication of user configuration information and also hold information about objects stored in the domain. The Active Directory Domain Services was known as Active Directory Services in Windows 2003.

RWDC Authentication

The Unified CCE application user must get authenticated if the client machines are connected to RWDC and not to RODC.

RWDC LDAP Read

Unified CCE must be able to perform the LDAP read operation successfully when the client is connected to RWDC and not RODC. LDAP Read operations happen when Unified CCE Configuration applications read the data from the Active Directory. Unified CCE issues LDAP ADSI calls to perform this.

RWDC LDAP Write

Unified CCE must be able to perform the LDAP Write operation successfully when the client is connected to a RWDC and not RODC. LDAP Write operations happen when Unified CCE Configuration applications write the data to the Active Directory. Unified CCE issues LDAP ADSI calls to perform this.

RWDC Password Change

Unified CCE must be able to change the password for the Unified CCE users through the Configuration application if the clients are connected to RWDC.

Read-Only Domain Controller

Since Unified CCE does not use Windows 2008/2008 R2 LDAP library, the calls by default reach only the RWDC and not the RODC, even if the Unified CCE components are connected to RODC. In addition, since all the writable requests are routed to RWDC through referrals from the RODC, there could be a considerable amount of efficiency impact. This causes Unified CCE operations to slow when connected to RODC. Therefore, considering this impact, Unified CCE does not support RODC in its deployments.

Restartable Active Directory Domain Services

Previously, there was no provision to restart Active Directory separately. As a part of this new enhancement, the Active Directory Domain Services can be stopped and restarted without restarting the domain controller.

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

Since Unified CCE does not use the Windows 2008/2008 R2 LDAP library, no error displays when Active Directory Domain Services is restarted.

Chapter 2

Domain Requirements and Supported Topologies

This chapter contains the following topics:

Ensuring a Healthy AD Environment for Unified ICM 8.0(1)

When preparing to install Unified ICM in a new or existing AD environment, it is important that the environment be stable. As a general rule, for all domain controllers in a forest, you must monitor replication, server, and AD health on a daily basis using Microsoft Operations Manager (MOM) or an equivalent monitoring application. For information about using MOM to monitor AD, see *Active Directory Management Pack Technical Reference for MOM 2005* 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 these tools are listed in the following table.

Table 1: Microsoft AD Tools

Tool Name	Location	Purpose	Command Line
dcdiag.exe	Windows CD in the Tools subfolder	• 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:** You must run this tool on the enterprise domain.
netdiag.exe	Windows CD in the Tools subfolder	• Generates a diagnostics report on LAN/WAN communications. • Verifies DNS functionality, network connectivity, name resolution, and IP configuration.	netdiag /fix /v /l
repadmin.exe	Windows CD in the Tools subfolder	• 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:

- The reports generated by these tools need to be evaluated by your network administrator, or a qualified AD expert (for example, Microsoft Support Services).
- If the Windows Server 2003 Support Tools are not already installed, install them now. If you do not have a Windows installation disk available, download the **Windows Server 2003 Support Tools** (http://www.microsoft.com/downloads/details.aspx?familyid=6EC50B78-8BE1-4E81-B3BE-4E7AC4F0912D&displaylang=en) .
- After installing the Windows Server 2003 Support Tools, you must either sign out and sign in again or reboot your system in order to set the path.

On Windows Server 2008/2008 R2, support tools are located in the "support\tools" directory on the Windows Server 2008/2008 R2 CD.

After the tools are installed, run the following setups:

- dcdiag.exe
- netdiag.exe
- repadmin.exe

How to run dcdiag.exe

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

This creates the text file dcdiag.txt in the folder containing dcdiag.exe.

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

Step 6 Correct all the issues, then re-run dcdiag.exe to ensure there are no remaining issues.

How to run netdiag.exe

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

Step 2 Type **cmd**.

Step 3 Press **Enter**.

A command console opens.

Step 4 At the prompt, enter **netdiag.exe /fix /v /l** .

This creates a text file (netdiag.txt) in the folder containing netdiag.exe.

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

Step 6 Correct all the issues, then re-run netdiag.exe to ensure there are no remaining issues.

How to run repadmin.exe

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**.

Note: MS Excel is required to read the CSV (comma separated values) file created when running repadmin.

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

Note: These instructions assume you are using Microsoft Excel 2007.

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

Step 9 In the MS 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:

1. Under Source DC, click **does not contain**.
2. 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:

1. Under Last Failure, click **does not equal**.
2. 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:

- 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:

- working domain controllers only
- failing domain controllers only
- domain controllers that are the least, or most recent

You can observe the replication partners that are replicating successfully.

Step 16 Locate and resolve all errors.

Step 17 Re-run repadmin.exe to ensure 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.

The following are domain requirements:

- Choose the following supported domain model in this guide.
- AD on:
  - Windows Server 2003 functional level (on Windows 2003 Server)
  - Windows Server 2008 functional level (on Windows 2008 Server)
  - Windows Server 2008 R2 functional level (on Windows 2008 R2 Server)
- Location of Time Source (DNS name).

Unified ICM Requirements for AD

- Authenticated users require credentials of an domain account with write privileges to the ICM OU.
- Microsoft AD tools or Domain Manager are the only supported tools for provisioning AD.

  Note: Permissions are needed during setup for creation of Service Logon accounts.
- Unified ICM servers can not be created in the Unified ICM OU hierarchy.

- Only the Unified ICM group policy template can be applied to OUs containing the Unified ICM servers.
- Single-label DNS domain names (such as "ICM") are not supported when used with Unified ICM/Unified 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** (http://support.microsoft.com/kb/300684/en-us).
- No AD schema changes are required. Authenticated users require read access to the contents of AD.

Note:

- The Unified CCE application requires read rights on the User OU on the corporate domain.
- Unified Contact Center Enterprise on Windows Server 2008 R2 is supported with Domain Controllers on Windows Server 2008/2008 R2 Domain Functional Level and also with domain controllers on Windows Server 2003/2003 R2.

Unified ICM Requirements for Group Policy in AD

Group Policy plays a pivotal role in AD management and 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 users' 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. As such, it is necessary to control the OU structure for Unified ICM components and ensure adherence to a standard.

Defining Group Policy

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 additional

information see **Group Policy management and the Group Policy Management Console** (http://www.microsoft.com/windowsserver2003/gpmc/default.mspx#EOC).

Unified ICM Requirements

Unified ICM has optional predefined policies that you can choose to apply to its OU structure to ensure security. These policies do not disrupt Unified ICM functionality.

Unified ICM Server Requirements

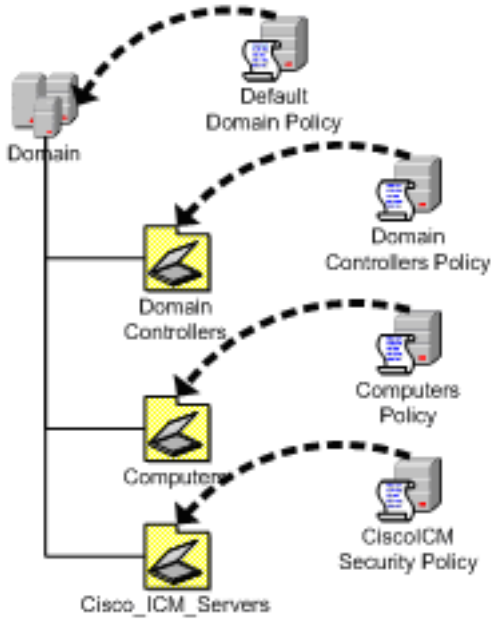
All Unified ICM servers can be moved into a separate OU to ensure proper functioning of the Unified ICM application and to improve security. The OU must be clearly identified as Cisco_ICM_Servers (or a similar clearly identifiable name) and documented in accordance with your corporate policy.

Note: You must create this OU at the same level as the computer OU or at the same level as the Cisco_ICM Root OU. Do not create the OU under the Cisco_ICM Root OU.

You have the option of installing a Cisco customized security template file to the local machine while running the Unified ICM/Unified CCE setup or the Cisco Unified ICM/CCE/CCH Installer applications. This .inf file is located in the Security Templates folder on the Unified ICM, and is documented in the *Security Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 9.x(y)* available on **www.cisco.com** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html). Add the security template using an existing Group Policy infrastructure as shown in the following figure.

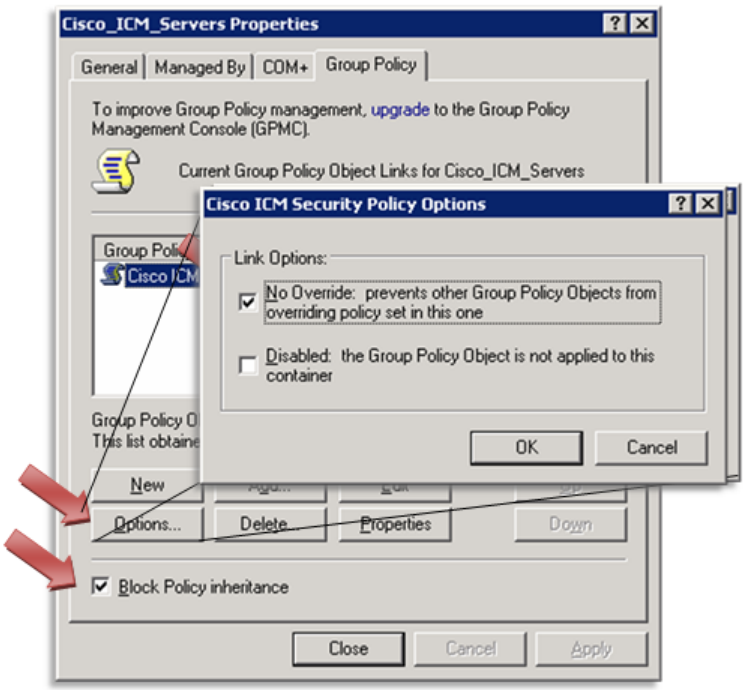
Note: If you are unfamiliar with AD, engage your Domain Administrator to assist you with Group Policy deployments.

Figure 1: Group Policy Deployments



After applying the policy to the OU, you must prevent propagation of default or custom Group Policies to this OU. This is accomplished by going to the OU property page and checking the **Block Policy inheritance** check box. You must also prevent improper policies from being used on the machines directly. This can be accomplished by clicking **Options** and checking the **No Override** check box.

Figure 2: Preventing Propagation of Improper, Default or Custom Group Policies



Note: If Block Inheritance is grayed out, a Parent object has **No Override** enabled. Uncheck **No Override** on all parent OUs.

Administration & Data Server Requirements

If you are setting up an Administration & Data Server in a domain other than the Central Controller domain, perform the following tasks to update the NAM Unified ICM AD OU environment so that the Administration & Data Server points to the CICM Central Controller.

Note: The following steps are only required when the Administration & Data Server is in a different domain than the Central Controller.

To ensure that the permissions are set up correctly:

1. Get the name of the Facility and instance from the CICM ICM AD Environment.

   Note: This can be done by running Domain Manager on a Unified ICM Server in the CICM domain.

2. Run the Domain Manager on a Unified ICM Server in the NAM domain.

3. In the Domain Manager, select the **Cisco_ICM root**.

4. Add a Facility with the same name used in the CICM Domain.
5. Select this Facility and add the instance with the same name that was used in the CICM Domain.
6. Once the CICM Facility and instance have been recreated on the NAM domain, run the Service Account Manager tool to generate the Service Account and password.

   The Service Account Manager tool sets the new service account in the Unified ICM Service Security group of the instance in the NAM domain and in the CICM domain. The service group is created in the NAM domain.

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/Unified CCH Child Domain model or the Unified ICMH/ Unified CCH Domain model.
- All additional addresses added manually (high, privates, private highs, etc.) 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

The Global Catalog is a central repository of domain information in an AD forest. In a multi-domain forest, Cisco requires you to have a Global Catalog at each AD site. Without a Global Catalog server, every AD query needs to search every domain in the forest; and multi-site deployments need to query across WAN links. Without the local Global Catalog, AD queries cause significant performance degradations/failure.

Supported Topologies

The following AD topologies are supported for Unified ICME/Unified CCH systems:

- Single Domain
  - Unified ICM/Unified CCH in the Corporate domain
  - Unified ICM/Unified CCH in a child domain of the Corporate domain

  - Unified ICM/Unified CCH as a standalone domain
  - Unified ICM/ Unified CCH as a tree root

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

The following AD topologies are supported for Unified ICMH/Unified CCH systems:

- Single Domain
  - NAM/CICM/Customer HDSs in a single domain
- Single Forest, Single Tree
  - NAM as a parent domain
    - CICM as the NAM child, Customer HDSs as the CICM child
    - CICM and Customer HDSs in a single domain as the NAM child
- Single Forest, Multiple Tree

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

Note: The OU hierarchies are discussed in About OUs (page 39).

This information is intended for the individuals responsible for:

- Configuring the AD Domain and Forest Topologies
- Staging new deployments of Unified ICMH/Unified CCH or Hosted NAM/CICM on Windows Server 2003 SP2

The administrators of your Unified ICMH/Unified CCH system must be trained on the use and functions of:

- Unified ICMH/Unified CCH
- Windows Server 2003 SP2 Servers
- AD
- DNS

This section does not provide detailed Unified ICME, Hosted NAM/CICM, or Windows Server 2003 SP2 specific information. This information can be found elsewhere in specific

documentation from Cisco and Microsoft. 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 Release 8.0(1). The impact that the unique environments in these existing infrastructures has on Unified ICM can be mitigated with minor adjustments to the support schema.

Previous releases did not clearly specify the supported topology models. This led to a variety of deployment structure interpretations, which, in turn, increased the support requirement and subsequently reduced customer satisfaction. In order to mitigate the misinterpretations and streamline the deployment strategy, the environments supported by Unified ICME are specified in detail.

Multiple Forests Are No Longer Supported

Multiple forests means two or more forests in a given environment that share resources through manually created trust relationships. After careful review, Cisco Systems, Inc. has determined that is that it is necessary to constrain the deployment scenarios and ensure customers use only single forest topologies. Multiple forest topologies (in regards to Unified ICM) are not supported. All Unified ICM components must be in the same domain or forest. This allows the automatic transitive trust relationships in the forest to replace the manual external trusts. The appropriate solution will simplify, or limit, the exposure to topology based deployment problems.

For additional information, see *Security Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.0(1)* .

Cisco Systems, Inc. *strongly* recommends the procurement of Microsoft Support Services to mitigate any Microsoft specific issues that might arise, as domain topologies vary.

Single Forest, Single Tree, 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
  - Hosted Environment Deployment

Single Domain Model

This type of domain structure comes with 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. The establishment of trust relationships between other domains is not necessary and execution of Group Policies is made easier by this simple structure.

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. It has been simplified and the capacity to span multiple domains in a single forest has been improved.

Choosing the Single Domain Model

The single domain model is ideal for many Unified ICM deployments. A single domain structure possesses multiple advantages, the first and foremost being simplicity. Adding unnecessary complexity to a system architecture introduces potential risk and makes troubleshooting more difficult. Consolidating complex domain structures (such as those found in NT 4.0) into a simpler, single AD domain structure reduces the administration costs and minimizes setbacks in the process.

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. Since NT domains were lacking in their capability 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.

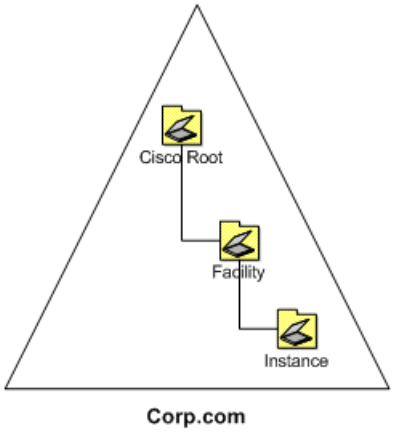
Unified ICM benefits from this design because AD traversal queries are limited to the single domain. As a result, request processing time is significantly reduced. AD controls access and provides security. This dramatically improves the overall performance of Unified ICM.

Designing a Single Domain Topology

Design is the most important aspect of any AD deployment. Follow the Microsoft Planning guide to ensure a smooth transition.

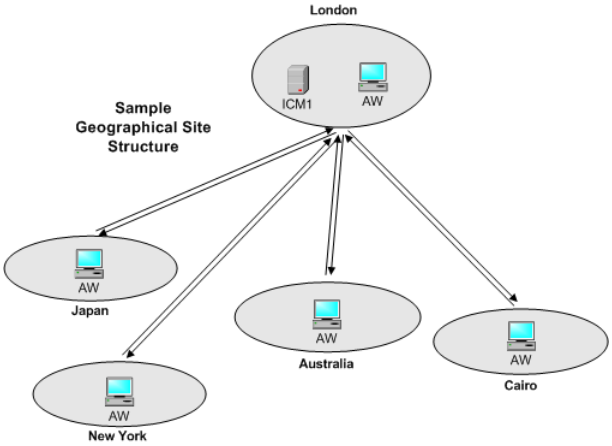
Delegation of password-change control and other local administrative functions can be granted to individuals in each specific geographical OU. The delegation of administrative functions provide administrators with permissions specific to the resources within their own group while maintaining central administrative control in the root OU. A detailed discussion of OU design is covered in About OUs (page 39).

Figure 3: Sample Single Domain Layout



Several AD sites can be created to control the frequency of replication. A site must be positioned to correspond with a separate geographical area, creating a site structure similar to the one shown in the following figure.

Figure 4: Site Organization by Geographical Location

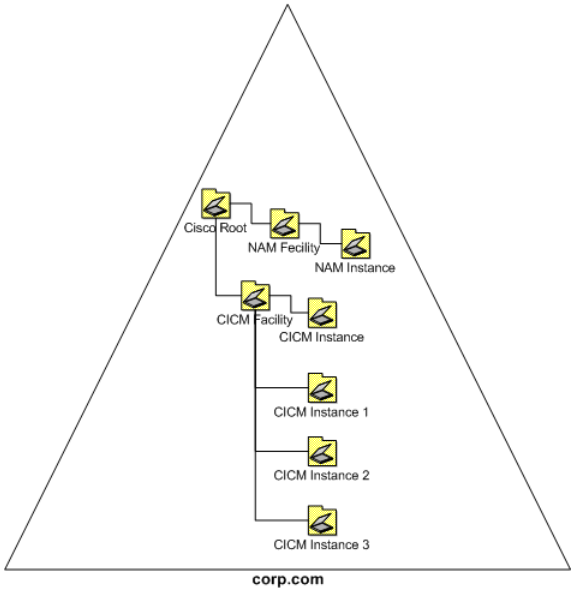


Creating separate sites helps throttle replication traffic and reduces the load placed on the WAN links between the sites. For more details about site links and replication, see **How Active Director Replication Topology Works** (http://technet2.microsoft.com/WindowsServer/f/?en/library/1f3bb1c1-ba8a-4b4e-9f23-f240566e3d661033.mspx).

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

There are hosted scenarios where you have many instances deployed in a variety of ways (such as geographically, based on client size, or however this model fulfills your needs). An example domain layout is shown in the following figure.

Figure 5: 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 and increased return on investment for the entire organization.

Single Tree Multiple Child Domains

For Unified ICMH/Unified CCH systems, it might be necessary to install Unified ICM in more than one domain. When this occurs, the addition of one or more child domains into the forest might be necessary (Unified ICM/Unified CCH systems must be in a single domain). When adding a domain, proper consideration must be given to the particular characteristics of multiple domain models.

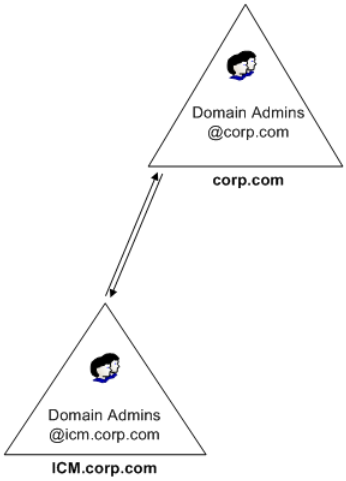
By default, two-way transitive trusts exist between the child domain and the parent domain in AD. However, this does not mean that resource access is automatically granted to members of other domains. For example, a user in the child domain is not automatically granted any rights in the parent domain. All rights need to be explicitly defined through the use of 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 absolutely necessary. Adding child domains to your existing domain structure might become necessary if the need for decentralized administration exists within your infrastructure. If your organization requires Unified ICM to be managed by its own IT structure and there are no future plans to consolidate them into a centralized model, multiple interconnected domains might be useful. A domain acts as a security boundary for most types of activities and is set up to block administration from escaping the boundaries of the domain. This approach operates in much the same way as NT domains, inheriting many of their associated limitations. It is better to try to centralize administration before deploying AD because you gain more AD advantages (for example: centralized management, a simpler deployment model, simplified user and group management,

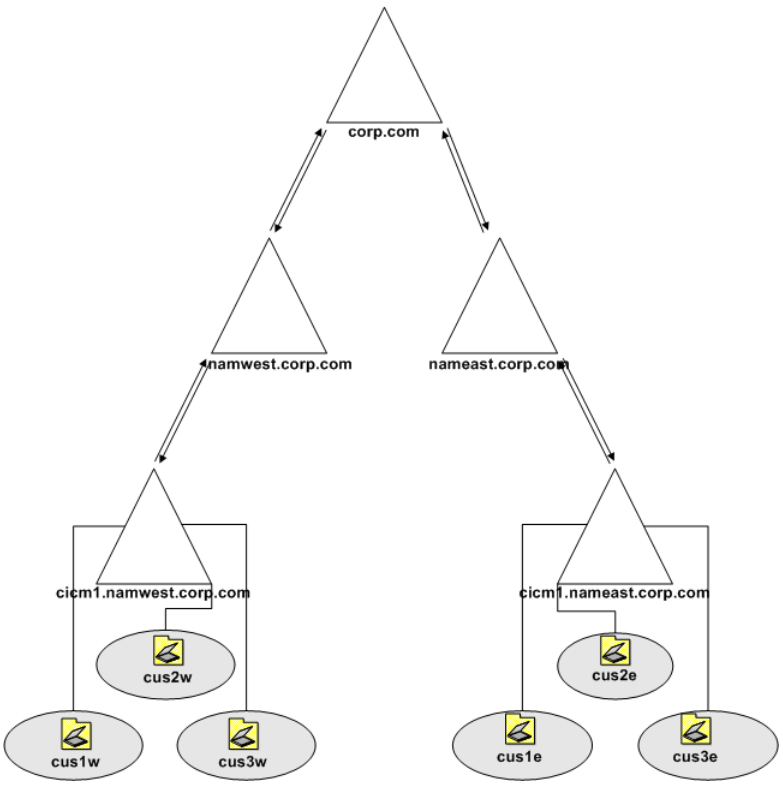
and enhanced operability). The following figure demonstrates the boundary as it exists by default in this topology. In order to give the user access to resources in the parent domain, the rights must be assigned.

Figure 6: Active Directory Boundaries



If there are geographic limitations (such as extremely slow or unreliable links), segment the user population into separate groups. This helps to limit replication activity between domains and makes it easier to provide support during working hours in distant time zones. Note that slow links by themselves do not necessitate the creation of multiple domains as AD sites throttle replication across slow links. Administrative flexibility is the main reason to create a domain for geographical reasons. For example, if there is a problem with the network in Asia, a local administrator has the power and resources to administer the Asia domain and has no need to contact a North American administrator.

Figure 7: Regional Domains

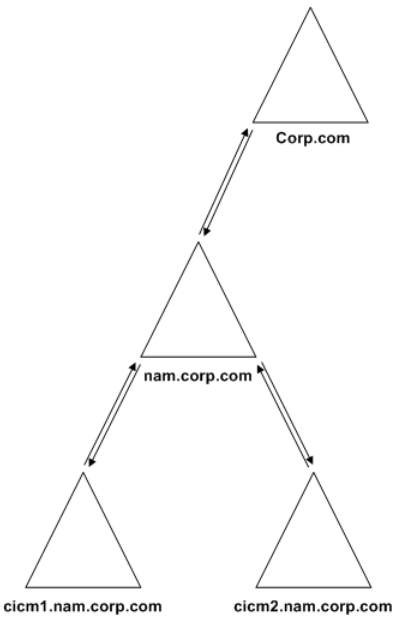


The single tree multiple child domain model allows each region to perform its own administration, creating an easily distributed and extremely flexible topology. This allows for a wide support base with immediate incident response. It also keeps the deployment clean and logical.

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 is appealing to some service providers because the logical boundary of the domains can provide a clear delineation in the NAM/CICM relationship while still maintaining AD functionality.

The single tree multiple child domain topology provides a contiguous namespace where the DNS domain names are related by the naming convention. For additional information, see Domain Name System (DNS) (page 33).

Figure 8: Contiguous Namespace



The flexibility in this model is apparent, however it is important to be familiar with your organization's requirements for a distributed, collaborative application such as Unified ICM. Use the simplest possible topology that meets your requirements.

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

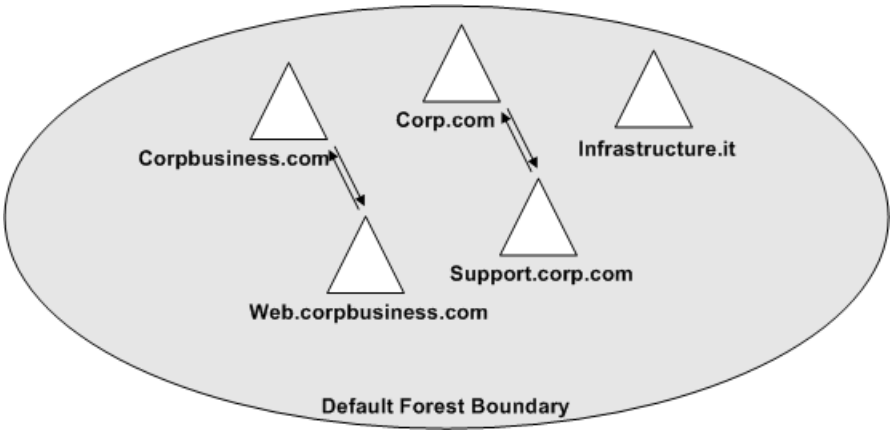
Any domain added to the forest that maintains a unique namespace form a new tree in the forest. An AD forest can consist of one or many trees in a single forest. In some instances, multiple trees are required so that a company can meet its business requirements.

Multiple Trees in a Single Forest Model

If your organization has decided to move to an AD environment and wants to use an external namespace for its design, then the external namespace can be integrated 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. Multiple DNS namespaces can be integrated into a single AD forest as separate trees in the forest as indicated by the following figure.

Figure 9: Simple Multiple Tree Topology



Only one domain in this design is the forest root (Corp.com in the figure above), and only this domain controls access to the forest schema. All the other domains shown (including the subdomains of Corpbusiness.com, as well as 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 need to maintain their distinct public identities as well as separate (noncontiguous) DNS names, multiple trees might have to be created in a single forest.

When to Choose a Multiple Tree Domain Model

If your organization currently operates multiple units under separate DNS namespaces, one option is to consider a multiple tree design such as this. It is important to understand, however, that simply using multiple DNS namespaces does not automatically qualify you as a candidate for this domain design. For example, you own five separate DNS namespaces and decide to create an AD structure based on a new namespace that is contiguous throughout your organization. Consolidating your AD under this single domain simplifies the logical structure of your environment while keeping your DNS namespaces separate from AD.

If your organization makes extensive use of its separate namespaces, consider a design like this: Each domain tree in the forest can then maintain a certain degree of autonomy, both perceived and real. Often, this type of design seeks to satisfy the needs of branch office administrators.

This type of domain design is logically more convoluted, but technically carries the same functionality as any other single forest design model. All the domains are set up with two-way transitive trusts to the root domain and share a common schema and global catalog. The difference lies in the fact that they all utilize separate DNS namespaces, a fact that must also be reflected in the zones that exist on your DNS server.

Choosing the Right Topology

The preceding sections provided a general overview of the considerations necessary when choosing a topology for Unified ICM in a corporate environment. As other considerations might arise, depending on corporation's internal directives, it is important to keep in mind the information in the following topics.

Single Domain

In general, a Windows 200x domain structure must be as simple as possible. The simplest approach is to create just one domain.

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—a domain administrator is not required 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 benefit:

- The domain administrator of the root domain has complete power over the AD tree

Single tree, multiple domain approach drawbacks:

- 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 too many child domains are created

Single Forest, Multiple Trees

All domains in a forest can belong to a single domain tree if their DNS names are contiguous. If their DNS names are not contiguous, separate domain trees must be created. Accordingly, if one domain tree is sufficient, there is no inherent need to create multiple trees.

Single forest, multiple tree approach 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

In some organizations there exists a need to have a separation between business units. This is perceived as providing 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 can be setup 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 affect AD has on the domain structure. If you turn all of the Domain Controllers off simultaneously, anything that relies on AD will break. To avoid this problem, stagger the Domain Controller reboots so at least one domain controller per domain remains online at any given time.

This is just one example. There are many variations and unique policies that could possibly have an impact on 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, this allows you to correct them prior to deployment.

Domain Name System (DNS)

AD is integrated with the Domain Name System (DNS) in the following ways:

- AD and DNS have the same hierarchical structure.

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

- DNS zones can be stored in AD.

  If using the Windows Server 2003 DNS Server service, primary zone files can be stored in AD for replication to other AD domain 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 (page 15) and netdiag.exe (page 15) to troubleshoot client computers that cannot locate a domain controller. These tools 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). In order to locate a domain controller, an AD client queries DNS. AD requires DNS to function.

Follow the Microsoft best practices for AD to create lookup zones and configuring DNS servers.

- Select **AD Integrated Zone** for both forward and reverse lookup zones.

- Listen only on a single Visible IP address (DNS – Properties – interfaces tab).

- Select the **Allow Dynamic updates** and **Only Secure updates** options.
- Limit zone transfers to limited and trusted servers only.
- Add all additional addresses manually (high, privates, private highs) in DNS as a Host record.
- If using Corporate DNS servers as opposed to the Domain Controllers for name resolution, ensure that the Corporate DNS servers have forwarding enabled to the AD servers.
- Unified ICM Servers must have a primary DNS server in the same AD site where they reside.

How to Install and Configure DNS on an Additional Domain Controller

Step 1 Choose **Start** > **Control Panel** > **Add/Remove Programs**.

Step 2 On the Add\Remove Windows Components, check **Networking Services** and click **Details**.

Step 3 Check only **DNS**, click **OK**, then select **Next**.

Step 4 Browse to the Windows Server 2003 SP2 CD. DNS installs.

Step 5 Validate that all DNS Zones were replicated from the first DNS Server in the AD Domain to this DNS Server.

a. Select the machine name, right-click and select **Properties**.

b. On the Interfaces tab, select **Listen on Only the following IP addresses**, remove all but the visible machine address.

For a Unified ICME Child Domain model, perform the following additional steps:

1. Manually add the **Enterprise level Standard Secondary Zone**.
2. Change DNS Settings on the First Domain Controller in the Child Domain to point to this additional Child Domain level DNS Server.

For a Hosted NAM/CICM model, perform the following additional steps:

1. Manually add the **Enterprise level Standard Secondary Zone**.
2. Change DNS settings on the First Domain Controller in the CICM/Child Domain to point to this additional CICM/Child Domain server.

How to Configure AD Sites

On Unified ICM Root Domain Controller:

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 have been added as entries in the Sites in this Site Link window.

c. Change the Replicate Every value to **15 minutes**.

How to Assign Global Catalog and Configure the Time Source

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

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/Unified 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 has been moved to another Domain Controller, the Time Source must be redefined as either that server or an external Time Source might be

utilized. Since the PDC Emulator was moved to another Domain Controller, you need to redefine the Time Source as either that server, or using 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).

How to Configure DNS Server on Forest Root Domain Controller

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **DNS**.

Step 2 Expand Hostname Tree.

Step 3 Expand Forward Lookup Zones.

Step 4 Right-click the Root folder (the folder named ".") and select delete.

You will see a warning about the zone.

Step 5 Click **Yes**.

Step 6 Select the machine name, then right-click and select **Properties**.

Step 7 On the Interfaces tab, select **Listen on Only the following IP addresses** and remove all but the visible machine address.

Step 8 Complete the configuration of AD Integrated Forward and Reverse Lookup Zones.

- Select the Unified ICM Domain zone name under Forward Lookup Zones, right-click and select **Properties**.
- On the General tab, for Allow Dynamic Updates, select **Only Secure Updates** from the menu.
- Only use the Zone Transfers tab when there is a Trust between this domain and another domain. You need to Transfer Zone updates from this AD Integrated Zone to a Standard Secondary Zone on the DNS Servers in the other domain. **Allow Zone Transfers**, then select **only to the following servers** and enter the IP Addresses of the DNS Servers in the other domain.
- To configure the required Reverse Lookup Zones, repeat the Step 13 below for each Unified ICM domain level network within the Forward Lookup Zone.

  Note: Networks within a Forward Lookup Zone include all visible and private networks utilized within a DNS Zone. These networks define Reverse Lookup Zones relative to the Forward Lookup Zone.

Step 9 Under the Server Name, right-click on **Reverse Lookup Zones** and select **New Zone**.

Step 10 Within the New Zone wizard, select **Active Directory Integrated**.

Step 11 In the Reverse Lookup Zone window, select **Network ID** and enter the required number of octets for the Reverse Lookup Zone. The Reverse Lookup Zone Name is automatically entered.

Step 12 Repeat the Steps below for each Unified ICM domain Reverse Lookup Zone.

a. Select the Zone name under Reverse Lookup Zones, then right–click and select **Properties**.

b. On the General tab, for Allow Dynamic Updates, select **Only Secure Updates** from the menu.

Step 13 Manually complete the DNS Host and PTR records.

a. Manually enter the hostnames for the machines that house ICM nodes, as well as all NICs and Peripherals for which Web Setup requires hostname resolution into the appropriate DNS Forward Lookup Zone.

b. On the DNS Server, right-click on the **Forward lookup Zone Name** and select **New Host**. (The hostname of this Root Domain Controller is already in the file.)

c. Add all Unified ICM hostnames (visible, visible high, private, private high, SAN) and their associated IP Addresses. Check the box to create an associated PTR Record (reverse lookup zone record).

d. Manually enter any Peripherals (ACDs/VRUs) and NICs accessed by the Unified ICM using hostname resolution in the Forward Lookup Zone.

Chapter 3

About OUs

What is an OU?

An OU is a container in the AD domain that can contain other OUs, as well as users, computers, groups, etc. 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 (page 42).

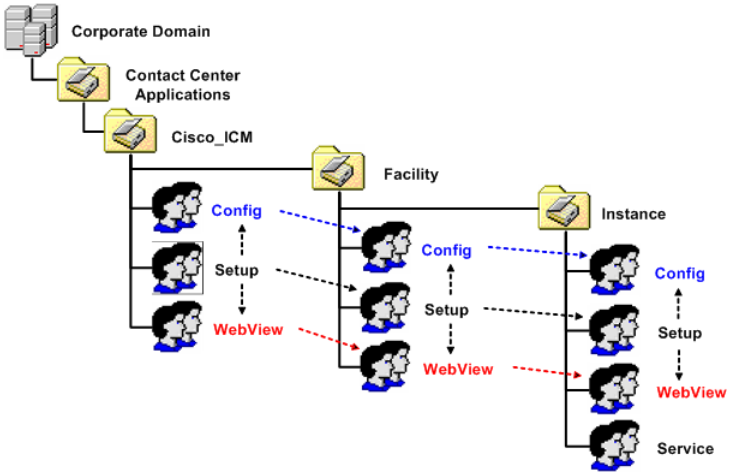
Permission to create an OU is controlled by AD. Typically, the Domain Administrator has rights to create OUs at the Root of the domain, then delegates control of those OUs to other users. Once a user has had control of an OU delegated to them, they have permission to create the Cisco Root OU.

OU Hierarchies

Unified ICM uses the following hierarchy of OUs:

- The Cisco Root OU (page 40) (Cisco_Root)
- One or more Facility OUs (page 41)
- One or more Instance OUs (page 41)

Figure 10: Organizational Unit (OU) Hierarchy



All objects that Unified ICM requires are created in OUs on the domain. The OU hierarchy created by the Unified ICM can be placed at the Root of the domain, or in another OU. Servers are not placed in this OU hierarchy. They can be placed in other OUs on the domain.

Note:

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

What is the 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 (page 41).

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

Note:

- For information on how to move the Cisco Root OU, see Appendix B (page 131).

- See How to Create (Add) the Cisco Root OU (page 92).

What are Facility OUs?

A Facility OU is a group of Instance OUs (page 41) that are organizationally related or have similar management needs. Permissions defined for a Facility OU are propagated 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; or in a Unified ICMH deployment, you might have separate Facility OUs for NAM and CICM instances.

An Facility OU inherits the permissions set for the containing Cisco Root OU (page 40); you can then specify different user permissions specific to that Facility.

Note: Facility OU names must be 32 characters or less.

What are Instance OUs?

An Instance OU inherits the permissions set for the containing Facility OU (page 41); you can then specify different user permissions specific to that instance.

What are Unified ICM instance OUs?

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.
- Define permissions for that instance as part of that Instance OU.

  An Instance OU inherits the permissions set for the containing Facility OU (page 41); you can then specify different user permissions specific to that Instance.
- Name is specified 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)

About Security Groups

This sections contains the following topics:

Security Groups and OUs

Each OU in the OU hierarchy (page 39) 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 (page 41) have the privileges of that security group for all Instance OUs (page 41) contained in that Facility OU.

Each OU has the following security groups:

- Config Security Group
- Setup Security Group
- WebView Security Group

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

Warning: At the Cisco_ICM OU level, the Domain Admin Group is a member of each security group. Due to current Microsoft limitations (70 – 80 security groups, see MS02808300), the cascading number of groups in the OU hierarchy makes it possible for the cascading number of groups to exceed the number of groups a Domain Admin can be a member of. See the Microsoft website, if you need to use more than 20 OUs (3 security groups, including all the facility and instance OUs, plus 1 ICM root for a total of 20 security groups per created OU).

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

What is a Security Group?

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

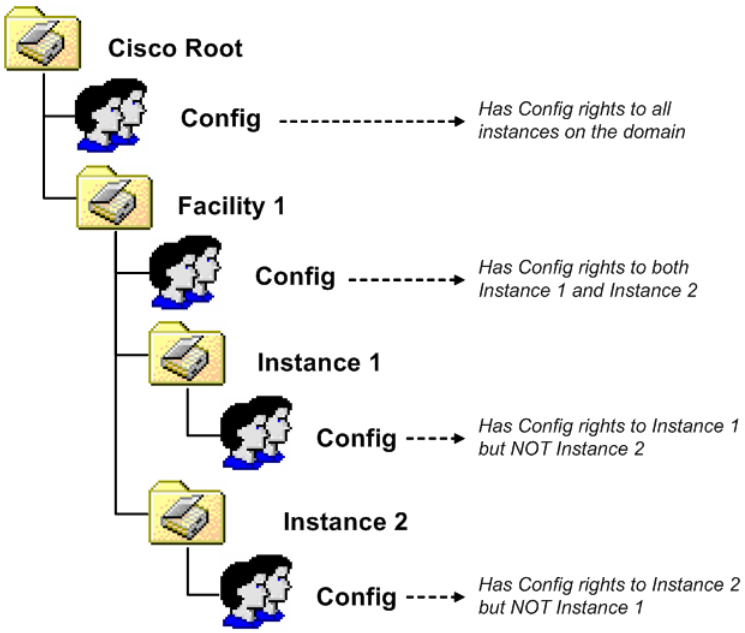
For each security group, you add domain users (page 97), who are granted privileges to the functions controlled by that security group. Users are given membership in the security groups to enable permission to the application. These users can be created in other OUs in this domain, or in any trusted 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 11: Security Group Nesting



- Use AD Domain Local Security Groups.

Security Group Names and Members

The function names of the security groups are Setup, Config, WebView, 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::

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

NetBIOS names truncated if needed and random digits are appended.

Security Group Members:

- Any user from a trusted domain can be added to a group.
- Group nesting allows for groups outside the OU hierarchy.

What is the Config Security Group?

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

Domain users whom you add 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.

What is the WebView Security Group?

Note: Webview is not supported in Release 8.5(x) or later and is not supported on Windows Server 2008 R2.

The WebView Security Group controls access to the WebView reporting application.

The WebView Security Group members have no database access, the WebView reporting application has the required database access because it has been granted to the Jaguar service account.

What is the Setup Security Group?

The Setup Security Group controls rights to run:

- ICM Installation and Setup Tools
- Configuration Manager
- WebView

Users who are members of the Setup Security Group can:

- Install Unified ICM instances and software components.
- Add users to security groups
- Create service accounts.

  Note: See the Service Account Manager (page 67) chapter for additional information.

- Manage OUs, groups, users, and permissions.

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

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

Figure 12: Setup Security Group Permissions

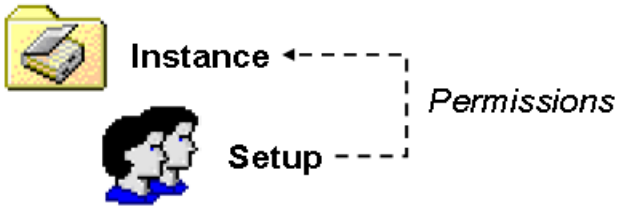


Table 2: Setup Security Group AD Permissions

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

How Do OU Hierarchies and Security Relate?

OUs are nested as described above, with the Root OU containing Facility OUs (page 41), which contain Instance OUs (page 41). In the case of Unified ICM, the Cisco Root OU is the "Cisco_ICM" OU. As OUs have associated security groups, the nesting of OUs allows 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

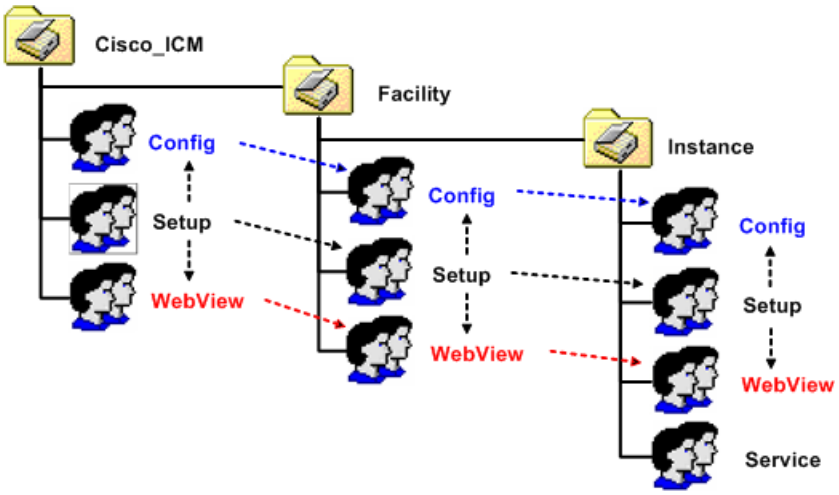
- Permissions/access rights in the Root WebView security group.

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

– Facility WebView group

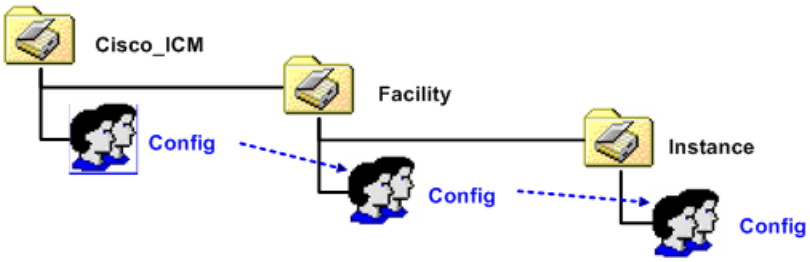
– Instance WebView group

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



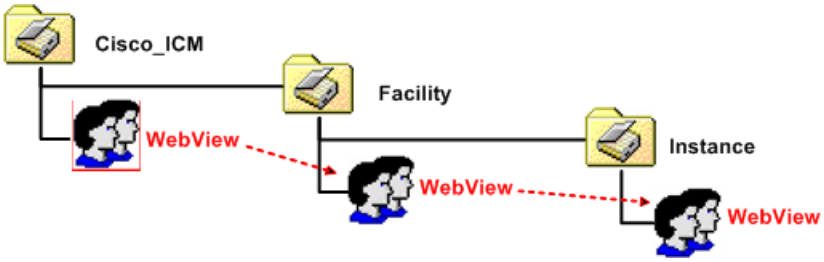
Making a user a member of the Root Config security group grants permissions/access rights in that security group as well as the Facility and the Instance Config security groups.

Figure 14: Root Config Security Group Member Permissions/Access Rights



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

Figure 15: Root WebView Security Group Member Permissions/Access Rights

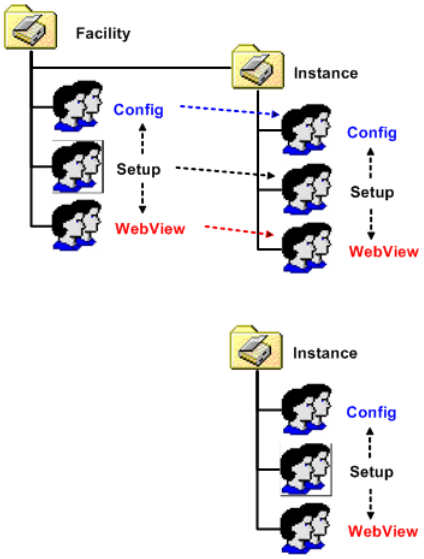


Members of a Facility security group have all the permissions/access rights granted to Instance OUs nested within that Facility. However, members of those Instance OU's security groups do not necessarily have the permissions/access rights granted to their containing Facility OU.

In the following illustrations, a member the Facility Setup security group has permissions/access rights to all the Facility security groups (remember, the Setup security group member is granted permissions/access rights to both the Config and WebView security groups at the same level as well), and the Instance Setup security group. The permissions/access rights granted from the Facility Config and WebView also grant permission/access rights to the Instance Config and Instance WebView security groups respectively.

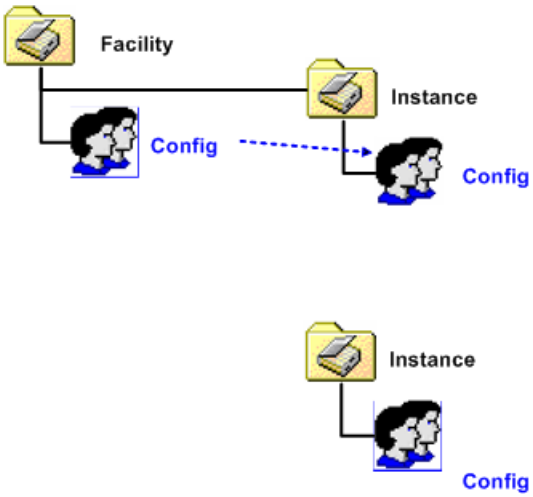
A member of the Instance Setup security group is granted permissions/access rights only to the Instance level security groups (Setup, Config, and WebView).

Figure 16: Faciliy/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.

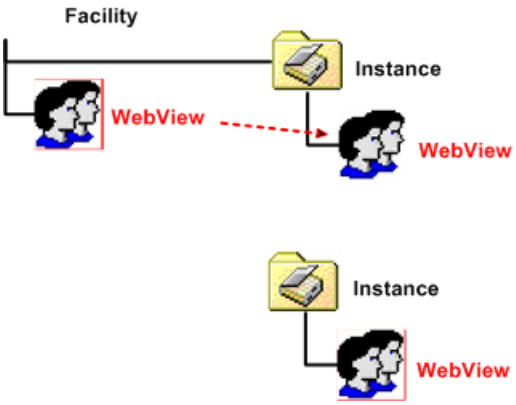
Figure 17: Faciliy/Instance Config Security Group Member Permissions/Access Rights



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

However, a member of the Instance WebView security group only has permissions/access rights to that security group.

Figure 18: Faciliy/Instance WebView 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: An Instance cannot be moved from one Facility to another.

What is the Service Security Group?

The Service Security Group is a security group generated automatically for Instance OUs (page 41). 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
- WebView DB

  Note: Webview is not supported in Release 8.5(x) or later and is not supported on Windows Server 2008 R2.

- Outbound Option DB

The Service Account Manager creates Service Logon Accounts in the Instance OU for the following services:

- Logger
- Distributor
- WebView (Jaguar)
- Tomcat

Service Logon Accounts

- Passwords do not have to be randomly generated, they can be provided and saved in AD, saved on the local machine, or saved 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
  - Jaguar
- 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 its uniqueness; there is no guarantee however. The list of possible components is the same as those for the DNS names except as indicated above.

Chapter 4

User Migration Tool

The User Migration Tool (UMT):

- Is a stand-alone Windows command-line application that performs migration in the granularity of a Unified ICM instance.

  It migrates only Unified ICM AD user accounts (config/setup/WebView users and supervisors) and can be used during Technology Refresh (TR) upgrade to a new domain, or if the Unified ICM machines are moved to a new domain.

- Finds the users in the Logger database and in all the security groups (Root, Facility, and Instance) each user belongs to; finds any additional users (not in the database) that are members of the Instance security groups; then generates a flat file (containing all users found) on the Logger system of the source domain.

  When the generated file is used on the Logger system in the target domain, the users are created in the new domain and added as members of the appropriate security groups. In addition, the database is updated with the migrated user information.

- Must be executed on a Logger system.

  The Logger database must reside on Logger system in the source domain, as well as in the target domain.

  Note: Microsoft .NET Framework 3.5 must be installed on the Logger system in both the source domain and the target domain. The Release 8.0(1) main ICM installer installs Microsoft .NET Framework.

- Performs migration of Unified ICM users from:

  – One domain to another.

  – One Unified ICM facility to another in the same domain.

  – One Unified ICM facility in one domain to another facility in another domain.

- Serves the following purposes:
  - All users retrieved from the Logger database are migrated from the source to the target AD domain.
  - All AD user accounts that are directly a member of Unified ICM instance security groups are migrated from the source to the target domain.
  - The user information table in the Logger database in the target server is updated to point to the user accounts created in the target AD domain.
  - In the target domain, Unified ICM security group membership is updated for the users belonging to an external domain.

This chapter contains the following topics:

User Migration Tool Prerequisites

The following prerequisites must be met prior to running the User Migration Tool:

- In the target domain, the Unified ICM OU hierarchy must have been laid out and the Unified ICM security groups created for each Unified ICM instance, prior to running the User Migration Tool. This must be done by running the Domain Manager.
- Import the exported Unified ICM registry from the source Logger system to the target Logger system.
- The Logger database must be backed up from the source Logger system and be restored on the target Logger system prior to running the User Migration Tool in the target domain
- If there are users from an external domain that are a member of the Unified ICM security groups at the source domain, then the trust relationship need to be established between the target domain and the external domain corresponding to the trust relationship that existed between the source domain and the external domain. This can be done using "Active Directory Domains and Trusts" tool.

- If the Unified ICM server is moved to a new domain, it is the user's responsibility to make sure that the SQL Server is migrated to the new domain before running the User Migration Tool.
- 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,
- For migration of the membership of Unified ICM users who belong to an external domain, credentials of an external domain user account with read privileges is required to access the external domain.

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.

Migration Scenarios

The User Migration Tool is intended to be used 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, you can store the usernames in non-Western European characters (but not in Unicode) in the Unified ICM database, but the domain names are always in Western European character set. The User Migration Tool is able to perform user migration for localized systems.

Performance Considerations

The larger the number of users being exported or imported, the longer the operation takes.

During migration, there is an average memory growth of 10 MB for 1000 users due to Microsoft API memory leaks.

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,

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

Localization Considerations

Note: Webview is not supported in Release 8.5(x) or later and is not supported on Windows Server 2008 R2.

1. For Japanese, Chinese, Korean, and Russian customers:

   – Install Logger, Administration & Data Server, and WebView servers on your native Windows Server 2003 SP2 server or MUI (Multilingual User Interface) version of Windows Server 2003 SP2 server to display agent names in your native characters.

     For example: Japanese customers must install Unified ICM Servers on a Japanese Windows Server 2003 SP2 server, or English 2003 Server with a full set of Japanese language pack applied.

   – English Windows Server 2003 SP2 with a language support is different from the MUI version of Windows Server 2003 SP2 server.

     For example: The type of deployment is not supported by ICM 7.x, where a Japanese customer checks the Install files For East Asian Languages check box from the **Control Panel** > **Regional and Language Options** > **Languages** tab of an English Windows Server 2003 SP2, and then installs ICM 7.x on it.

2. Date time format

   The date range on a WebView report and WebView server must be in the same format.

   For example: if the WebView server has a US English locale with MM/DD/YYYY date format and WebView client has a French locale with DD/MM/YYYY date format, the report generated from the WebView client machine will have a mixed date format. The Date range will be in MM/DD/YYYY format and Run Date will be in the DD/MM/YYYY format

3. Client/Server language compatibility

   – Any WebView client, regardless of the language it has, can connect to an English WebView server.

     For example, a Russian WebView client can connect to an English WebView server. However, the client might experience the following issues in such a deployment:

     - All agent names are in English.

     - Date range on WebView report is shown in U.S. date format.

– For customers using Latin1 languages, WebView server and clients can be in different language.

  For example, an Italian WebView client can connect to a German WebView server because both Italian and German languages are included in the Latin1 character set.

– For Japanese, Chinese, Korean and Russian customers, WebView client must be in the same language as the WebView server to display agent names and report descriptions in their native characters.

User Migration Steps

Note: Webview is not supported in Release 8.5(x) or later and is not supported on Windows Server 2008 R2.

The User Migration Tool is first run 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's group memberships (the Setup, Config, and WebView 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. It looks for the users in the external domain and, if they are found, 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, Config, and WebView) to find any user accounts. If it finds any, that user information is added to the flat file as well.

The User Migration Tool is then run 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.

Source Server in the Source Domain

Perform the following steps:

Step 1 Backup the Logger database for each Unified ICM instance using Microsoft SQL Server Tools.

Step 2 On the Logger system, for each installed Logger instance, execute 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 executed.

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 the User Migration Tool will be run on the target system).

b. Backup and export the registry.

c. Verify the log file for any errors.

Target Server in the Target Domain

Perform the following steps:

Step 1 Shut down the Unified ICM services if they are running.

Step 2 If the domain name needs changing when in a Common Ground upgrade scenario, see the section Changing the Domain Name Using the Web Setup (page 57).

Step 3 In a Technology Refresh upgrade scenario:

a. Make sure 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 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 Optionally, run the User Migration Tool in verify mode to validate the migration.

Step 6 For duplex Logger systems, run icmdba to synchronize side A and B.

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

Changing the Domain Name Using the Web Setup Tool

To change the Domain for a system you must run Web Setup. You must have the necessary permissions before you can change the domain. To change the domain for all instances on the machine, complete the following steps:

Step 1 Run Web Setup.

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

Step 3 Delete any instances and facilities that you do not want to use in the new domain.

Step 4 Run Domain Manager and ensure that the instances and facilities defined in Domain Manager match what is actually on the machine. Failure to do this will cause the Web Setup Change Domain operation to fail .

Step 5 Select the Instance to be modified, then click **Change Domain**.

The Change Domain page opens displaying the currently configured Domain and the machine's new domain name.

Step 6 Click **Save**. A query is sent to confirm that you want to change the domain.

Step 7 Click **Yes**. If successful, you are returned to the Instance List page.

Note:

- If the Instance does not exist, it must be created running the Domain Manager. Create the Instance under the selected Facility in the new Domain.
- If you encounter a problem, Web Setup might direct you to use the Domain Manager or AD tools to resolve the problem.

User Migration Tool Modes

The User Migration Tool can be run multiple times without affecting anything.

For example, in the source domain, if the tool is run in Export mode multiple times, the exported file is completely overwritten every time. Similarly, in the target domain, if the tool is run in Import mode multiple times using the same input file, the security group membership is not affected.

The User Migration Tool 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.

    The name of the exported file is a combination of 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. This eliminates the need to specify these parameters during the Import mode.

- **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, you must wait 15 minutes after an Import is completed before running the User Migration Tool in Verify mode.

- **Verify**
  - Runs on the Logger system in the target domain after an Import has been performed.
  - Validates the import.

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

See the following sections for additional information concerning the Export (page 60), Import (page 61), and Verify (page 62) modes.

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: name of the user accounts that are migrated, and their security group membership details.

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 is run, 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 the User Migration Tool execution results in three categories:

- Info
- Warning
- Error

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

Mode Considerations

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

After a user migration import, if you use a newly created AD account to login using the WebView login interface, the log on fails. This is because the AD accounts are created using the **Change password during the next logon** option and WebView does not have the ability to solicit the new password from the end user.

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 WebView interface to login.

Export Mode

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

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

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

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

Table 3: 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.
- For additional information on the Content Parameters, see Content Parameter Descriptions (page 63).
- 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.

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 so that the user is forced 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 is then updated with the user account's AD Globally Unique Identifier (GUID) and the target domain name.

The following information is imported from the exported file:

- the Logger database name
- the Unified ICM facility
- the Instance name

In the Import mode, the User Migration Tool can be run 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:

- the user accounts do not need to be created and the Logger database does not need to be updated
- only the Unified ICM security group membership of the user account is updated

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

Table 4: 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 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 so that the user is forced to change the password during the next logon.

Note:

- For additional information on the Content Parameters, see Content Parameter Descriptions (page 63).
- 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.

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 5: 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:

- For additional information on the Content Parameters, see Content Parameter Descriptions (page 63).
- 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.

Content Parameter Descriptions

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

Table 6: User Migration Tool Parameters

Parameter	Description
/DBName	The Logger database name.
/Facility	The Unified ICM instance facility name. When it is optionally specified 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 logging in for the first time.

Users from Trusted Domains

It is possible that there are user accounts from trusted AD domains with authorization in the current domain. This is 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 if, and 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.

  The security group FOO is a member of the Cisco_ICM_WebView security group.

  This makes *ExtUser1* an **indirect** member of the Cisco_ICM_WebView security group.
- 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. The Cisco_ICM_WebView security group is not selected.

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

In order 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 whether or not there are any users from that domain that 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 the error messages and solution for the User Migration Tool error messages.

Table 7: User Migration Tool Error Messages

Error Message	Solution
Cannot connect or authenticate to the Logger database.	Verify that the Logger database exists and can be authenticated 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.
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.

Error Message	Solution
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.	Same version of the User Migration Tool must be used for both modes of the migration.
The User Migration Tool is being run on ICM/IPCC version earlier than 7.5(1).	The User Migration Tool must be run on Unified ICM/ Unified CCE 8.0(1) or later systems only.
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.	The User Migration Tool cannot be run in Import mode under the same Unified ICM facility and domain that it was exported from. It must be run 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

Unified ICM and Unified Contact Center Enterprise services, such as Logger or Distributor, execute under the context of a domain user account commonly known as a service account. The Service Account Manager (SAM) tool handles creation and maintenance of service accounts. With Service Account Manager, you can do the following:

- either create a new service account or choose an existing service account.
- enter your own password or fix service account group membership issues let the Unified ICM application generate one for you.

  Note: If passwords are changed using an application other than SAM, SAM cannot detect the changes.
- choose whether (when applicable) or not to update the account in AD and use existing AD accounts as Unified ICM service accounts.
- fix service account group membership issues (such as modifying Unified ICM service account passwords) without recreating accounts or without re-running ICM installation or setup tools.

You have the option to re-run the Service Account Manager post-installion to modify the Unified ICM service account, or its password, or to verify the account health. The Service Account Manager must be executed on each server locally to configure the service accounts for services listed below.

The Service Account Manager is limited to function only with the following services:

- Administration & Data Servers
- LoggerA
- LoggerB
- Jaguar

This chapter contains the following topics:

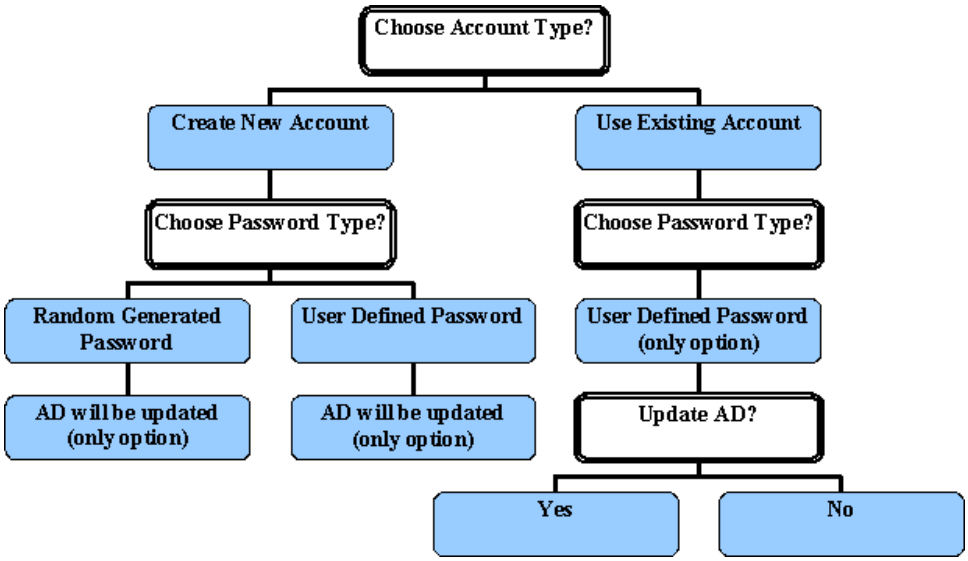
Managing Service Accounts

The Service Account Manager serves three purposes. It allows you to:

1. Create new accounts with random passwords
2. Use existing AD accounts as Unified ICM service accounts.
3. Provide an interface to modify Unified ICM service account passwords.

The following diagram illustrates the basic workflow of the Service Account Manager.

Figure 19: Service Account Manager Application Workflow



Other Considerations

Permissions

You must have the correct privileges to create or modify accounts in the domain. Typically, this action is performed by a domain administrator. However, the Service Account Manager

does not enforce domain administrator privileges. You are expected to have the right permissions before invoking the Service Account Manager.

Domain Restriction

The service account must be in the same domain as the Unified ICM server. When choosing an existing account, the Service Account Manager restricts the account to be selected from the same domain as the server.

Special Case: When the distributor is in a different domain than the logger, the distributor service account must be placed in the instance service security groups of both its own domain and the logger domain.

AD Update Failures

If the Service Account Manager finds that a service is running, it first requests your permission; if you approve, it stops the service. If you choose not to stop the service, the Service Account Manager does not modify the service account information. The Service Account Manager automatically starts the service if it had explicitly stopped the service prior to editing the account information. If the Service Account Manager fails to update the account in AD, due to either a noncompliant password policy or any connectivity error, the Service Account Manager warns you and logs the error. At that point, you can choose to fix the problem and retry, or cancel.

Logging

The application maintains its own log file, when invoked as a standalone application. If called through the Web Setup tool, logs are written to the Websetup log files only.

Set Service Account Memberships for CICR Replication

When upgrading the Unified ICMH to Unified ICM 8.0 (or later), the CICR replication process (CRPL) does not have proper permission to make configuration updates to customer instances (CICM) and slave NAM instance without manually configuring the Active Directory.

This configuration entails adding the Provisioning NAM's logger service accounts to the service groups of the CICMs and the slave NAM. Thus the Provisioning NAM's service account has the permissions necessary to update the databases of the CICM and the slave NAM.

One function the Service Account Manager provides is to automate the manual configuration steps (as described on **www.cisco.com** (http://www.cisco.com/en/US/products/sw/custcosw/ps5053/products_tech_note09186a00806c6609.shtml)). This functionality is exposed through the Service Account Manager command-line interface as described in the *Set Service Account Memberships for CICR Replication* section.

Typically this functionality is utilized through two batch files (one for the A side and the other for the B side) where there is an entry for each CICM or slave NAM as a destination (/Dest). Each time the Web Setup is executed, running the batch file enables you to configure the Active Directory permissions properly.

Service Account Manager End User Interfaces

The Service Account Manager has two user interfaces:

- The Graphical User Interface (page 70) consisting of the following dialogs boxes:
  - Main (page 71)
  - Edit Service Account (page 76)
- The Command Line Interface (page 77)

Service Account Manager Graphical User Interface Dialog boxes

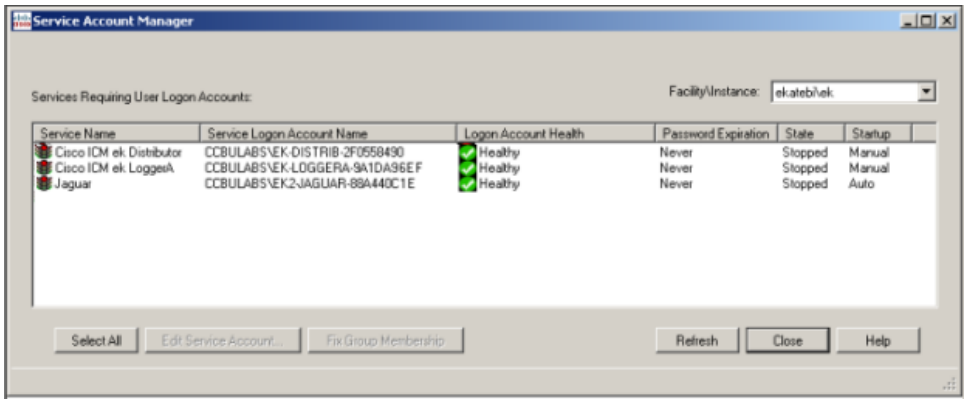
A shortcut to the application can be found in Windows **Start** > **Programs** > **Cisco Unified ICM-CCE-CCH Tools** folder.

The Service Account Manager has two dialog boxes:

- Main

  Lists all services with their account information.

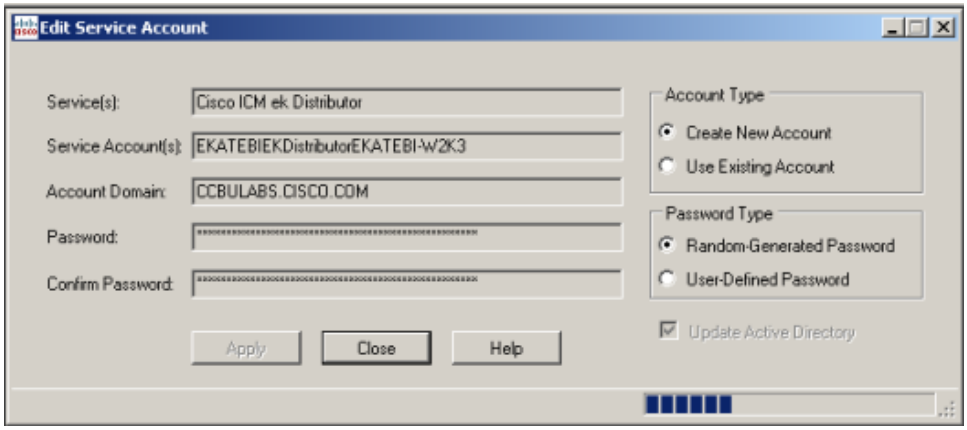
  Figure 20: Main Service Account Manager Dialog



  Note: For additional information on all fields and buttons in the dialog box, see Service Account Manager - Main Dialog Box (page 71).

- The Edit Service Account dialog box opens. Use this dialog box to edit the service account information.

Figure 21: Service Account Manager - Edit Service Account Dialog



Note: See Service Account Manager - Edit Service Account Dialog Box (page 76) for additional information on all fields and buttons in this dialog box.

Service Account Manager - Main Dialog Box

The Service Account Manager can be used as a standalone application as well as being invoked from Web Setup for Cisco Unified ICM/Contact Center Enterprise & Hosted and the Cisco Unified ICM/CCE/CCH 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, TomCat, Jaguar, 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.
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 normal.

Field/Button/ Drop-down	Description
	• 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 domain or local security groups. – *Account not associated with service*: service account created but not replicated, hence not associated yet. 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 Unified ICM/CCE/CCH security 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 create a service account for each service. • Account not in Instance Domain – The Service Account Manager is capable of detecting whether or not a service account exists in the domain. • Account Disabled

Field/Button/ Drop-down	Description
	– In AD an account can be enabled or disabled. This message indicates the account is disabled in the domain. • Password Expired • Account not a member of the Instance Service Group • Service Group not a member of local Administrators group • 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 will be 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 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 will be 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

Field/Button/ Drop-down	Description
	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. • EAServer configuration for WebView failed (Jaguar only) – After an account is associated with the Jaguar service and validated SAM attempts to run a script to configure WebView. If that script fails, this message appears. • 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. A service has an *Invalid Account* health state immediately after creation since 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 reattempts placing the account in the relevant local and domain security groups.

Field/Button/ Drop-down	Description
	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	Service account passwords created by the Service Account Manager are set not to expire. However, you do have the option of setting the service account passwords to expire. **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 stateof 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, TomCat, Jaguar, 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. Once in the dialog box, the Service Account Manager prompts you to try to use the account recently created, as it keeps track of it. If you agree to use the recently created account, the application tries to reuse the previously created account, thereby escaping from the recursive cycle of trying to create and use an account. If you chose random password, the application creates a new one, or prompts you to enter one. The application never stores the password.

Field/Button/ Drop-down	Description
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 create a new or use an existing account, and to choose a random or a user defined 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's domain. (Read Only)
Password	If the Password Type selected is **Random-Generated Password**, this field is populated with the generated password. If the Password Type selected is **User-Defined Password**, enter the password to be used for this account.
Confirm Password	If the Password Type selected is **Random-Generated Password**, this field is populated with the same generated password as the Password field. If the Password Type selected is **User-Defined Password**, re-enter the password to be used for this account.
Account Type	Allows you to either create a new account or use an existing account by selecting the appropriate radio button. **Create New Account** is the default if no domain account assigned yet. **Use Existing Account** is the default if a domain account is already assigned.
Password Type	Allows you to choose a random-generated or a user-defined password by selecting the appropriate radio button.

Field/Button/check box	Description
	Random Generated Password is the default if you are creating a new account. **User Defined Password** is the default, and only, option when using an existing account.
Update Active Directory	**Checked** is the default, and only, option if you are creating a new account. **Note:** By checking this check box, you are actually making changes to the Active Directory domain and any changes to passwords will affect the password of the existing user. **Unchecked** is the default if using an existing account.
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 Service Account Manager finds that the you did not successfully associate a valid domain account with a service, it warns you that the service will fail 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.

Service Account Manager - Command Line Interface

Note: The Service Account Manager command line option is only supported for NAM/CICM replication.

Creating Default Service Accounts Silently

The command line interface is used by Web Setup to silently create 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 be used are:

  – Distributor

  – LoggerA -- For use when on Side A of the logger or for All-In-1 ICM/CCE

  – LoggerB -- For use when on Side B of the logger only

  – Jaguar

/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/CCH 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.

Setting Service Account Memberships for NAM/CICM Replication

When the application is invoked from the provisioning NAM's Logger servers (sides A and B), the command line is as follows:

- ServiceAccountManager
- /SrcInstance<InstanceName>
- /DestDomain<DomainName>
- /DestFacility<FacilityName>
- /DestInstance<InstanceName>

Service Account Manager - How to ...

How to create a new account for a single service

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 Select **Create New Account**.

If no domain account is associated with the service then **Create New Account** is selected by default.

Step 4 Enter a password or have one generated randomly.

Random-Generated Password is selected by default.

Step 5 Click **Apply**.

The Service Account Manager creates a new account in AD with a password.

If the account name already exists, the Service Account Manager asks you to either recreate it, or just update the password.

The application associates the account with the service on the server. It places the account in the required domain security group and local security group, and sets the required permissions. Service account gets recreated, or just the password changes, based on your selection prior to clicking **Apply**.

Note: If the Service Account Manager fails to put the account in domain security group, it asks you to rerun the application 20 minutes later to give AD time to replicate the account.

How to update an existing account for a single service

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 Select **Use Existing Account**.

If a domain account is associated with the service, **Use Existing Account** is selected by default.

Step 4 Enter a password.

Step 5 Choose whether or not to update the password in AD.

Step 6 Click **Apply**.

If previously selected, the Service Account Manager updates the password in AD. It updates the service on the server with the new account information.

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

Note: If the Service Account Manager fails to put the account in domain security group, the application asks you to rerun the application 20 minutes later to give AD time to replicate the account.

How to create new accounts for more than one service

Step 1 Select multiple services or click **Select All**.

Note: Use the normal Windows conventions for selecting all or multiple services.

Step 2 Click **Edit Service Account**.

The Edit Service Account dialog box opens.

The Service Name column lists all services. Since multiple services are selected, **Use Existing Account** is selected by default.

Step 3 Click **Create New Account**.

A separate service account is created for each service.

Step 4 Enter a password, or have one generated randomly.

If you choose to enter a password, then the same password is shared across all accounts.

If you choose to randomize the password, a separate random password is generated for each account.

Step 5 Click **Apply**.

The Service Account Manager creates multiple accounts in AD with the password. The application associates each account with the respective service on the server. It places the accounts in the required domain security group and local security group, and sets the required permissions.

Note: If the Service Account Manager fails to put the account in domain security group, it asks you to rerun the application 20 minutes later to give AD time to replicate the account.

How to update an existing account for more than one service

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.

The Service Name column lists all services. Since multiple services are selected, **Use Existing Account** is selected by default.

Step 3 Enter an account name.

Step 4 Enter a password.

Step 5 Choose whether or not to update the password in AD.

Step 6 Click **Apply**.

If previously selected, the Service Account Manager updates the password in AD. It updates the service on the server with the new account information.

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

Note: If the Service Account Manager fails to put the account in domain security group, the application asks you to rerun the application 20 minutes later to give AD time to replicate the account.

How to fix the group membership issue of one or more accounts in the "Group Membership Missing" health state

Fix Group Membership is only enabled when an account in the "Group Membership Missing" health state is selected.

Step 1 Select the unhealthy accounts displaying the "Group Membership Missing" state.

Step 2 Click **Fix Group Membership**.

If any of the selected account is not in the "Group Membership Missing" state, **Fix Group Membership** is disabled.

Step 3 Click **Apply**.

The Service Account Manager then places the account in required domain security group and local security 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

How to Prepare to Work with Active Directory

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" by following the procedures in the section Creating the Root OU (page 92) . 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.

Step 1 Review the system software staging guidelines (page 103).

Step 2 Ensure that you have installed Microsoft Windows.

Step 3 If you are installing a Logger or Distributor/HDS Administration & Data Servers, ensure that you have already installed Microsoft SQL Server with the required service pack.

See Also

For more information on supported Windows and SQL Server versions, see *Cisco ICM/IPCC Enterprise & Hosted Editions Release 8.0(1) Hardware and System Software Specifications (Bill of Materials)* available at **www.cisco.com** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

Domain Manager and the 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 installing or upgrading the first server.
  - Then, choose an existing Instance from that hierarchy.

    Note: For Windows 2008 R2 Users only: When adding an instance, you are adding that instance's Setup security group to the local Administrators group on that machine. When removing an instance this security group is also removed.

- Integrated use of the Domain Manager

When Instance OUs are created by the Domain Manager, user accounts in old Unified ICM/Unified CCE security groups are automatically copied to new security groups in the Unified ICM/Unified CCE 8.0 instance OU. The old groups are not modified.

Domain Manager Functions

See About the Domain Manager (page 85) for the detailed steps for the following functions :

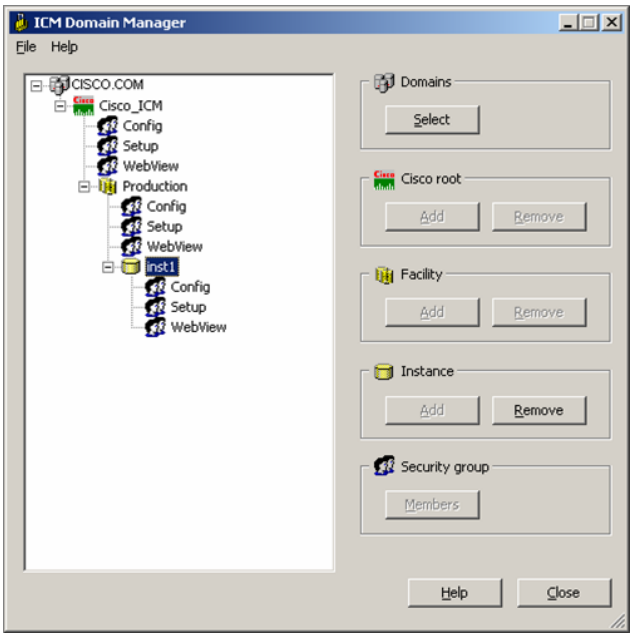
- Open the Domain Manager (page 87).
- View Domains (page 90)
- Add a Domain to a View (page 91)
- Remove a Domain from a View (page 91)
- Create (Add) the Cisco Root OU (page 92)
- Remove the Cisco Root OU (page 93)
- Create (Add) a Facility OU (page 94)
- Remove a Facility OU (page 94)
- Create (Add) an Instance OU (page 95)
- Remove an Instance OU (page 96)
- Add members to a Security Group (page 97)
- Remove members from a Security Group (page 99)

Chapter 7

About the Domain Manager

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

Figure 22: ICM Domain Manager



The Domain Manager also allows you to:

- Assign users to groups
- View existing service logon accounts
- Get extended security group information
- Get detailed permission information

- Run integrated with setup or stand alone
  - Installed with each component
  - Program group shortcut on Administration & Data Servers

This chapter contains the following topics:

Domain Manager Tool Functionality

Note: Webview is not supported in Release 8.5(x) or later and is not supported on Windows Server 2008 R2.

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 three domain local security groups:
  - Cisco_ICM_Config
  - Cisco_ICM_Setup
  - Cisco_ICM_Webview

  The Cisco_ICM_Setup group is added to the Cisco_ICM_Config and Cisco_ICM_Webview groups, because the setup group needs the permissions for both the the config and WebView group.

- Creates a facility OU under the Cisco Root OU, and creates three domain local security groups:
  - <Facility name>_Config
  - <Facility name>_Setup
  - <Facility name>_Webview

  The Domain Manager adds the <Facility name>_Setup group to the <Facility name>_Config and <Facility name>_Webview groups, because the setup group needs the permissions for both the the config and WebView 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
  - Adds Cisco_ICM_WebView group to <Facility name>_WebView
- Creates an instance OU under each facility OU, and creates four domain local security groups:
  - <Facility name>_<Instance name>_Config
  - <Facility name>_<Instance name>_Setup
  - <Facility name>_<Instance name>_Webview
  - <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 and <Facility name>_<Instance name>_Webview, because the setup group needs the permissions for both the the config and WebView group.
  - <Facility name>_Config group to <Facility name>_<Instance name>_Config
  - <Facility name>_Setup group to <Facility name>_<Instance name>_Setup
  - <Facility name>_Webview group to <Facility name>_<Instance name>_Webview

  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 on OUs, see Chapter 3, About OUs (page 39).

How to Open the Domain Manager

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

You can open the Domain Manager in the following ways:

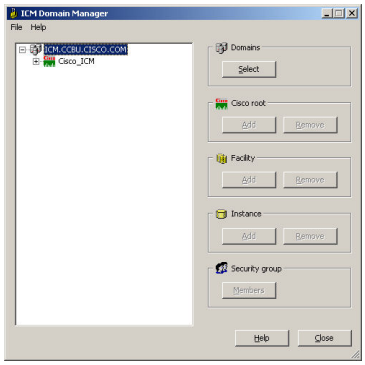
- Open the Domain Manager application from the Cisco Unified CCE Tools folder.
- Access through **Start > Programs > Cisco Unified CCE Tools > Domain Manager**.

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 23: 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. Multiple domains can be displayed 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 is displayed 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 8: 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 (page 90) appears.
Cisco Root	To add the Cisco Root when a domain is selected that does not already have the Cisco Root, click **Add**. The Select OU (page 92) dialog box appears. 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 (page 94) dialog box appears. 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 (page 95) dialog box appears. To remove the selected instance, click **Remove**.
Security group	Click Members to display the Security Group Members dialog box (page 98) where you assign users to security groups.

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.

From the Domain Manager dialog box, you can perform the following tasks:

- View Domains (page 90)
- Add a Domain to a View (page 91)
- Remove a Domain from a View (page 91)
- Create (Add) the Cisco Root OU (page 92)
- Add a Facility OU (page 94)

- Remove a Facility OU (page 94)
- Add an Instance OU (page 95)
- Remove an Instance OU (page 96)
- Add members to a Security Group (page 97)
- Remove members from a Security Group (page 99)

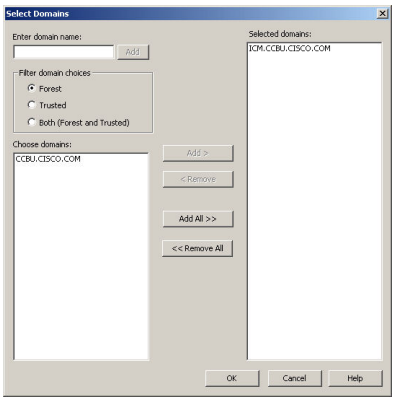
How to View Domains

Step 1 Open the Domain Manager (page 85).

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

The Select Domains dialog box (page 90) opens.

Figure 24: Select Domains Dialog Box



You can now add (page 91) or remove (page 91) domains for use with the system software.

Table 9: Select Domain dialog box Properties

Property	Description
Enter domain name:	Allows you to enter fully qualified domain name. Once the qualified domain name is entered, 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:	DChoose a domain from the displayed list:

Property	Description
	• **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.

How to Add a Domain to a View

You can add domains by using the controls in the Select Domains (page 90) dialog box. Follow these steps to add a domain:

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 (page 88). You can then add the Cisco Root OU (page 92).

How to Remove a Domain from a View

You can remove domains by using the controls in the Select Domains (page 90) dialog box. Follow these steps to remove a domain:

Step 1 In the Select Domains (page 90) 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.

How to Create/Add the Cisco Root

You can create the Cisco Root OU (page 40) 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.

Step 1 Select the domain you want to add.

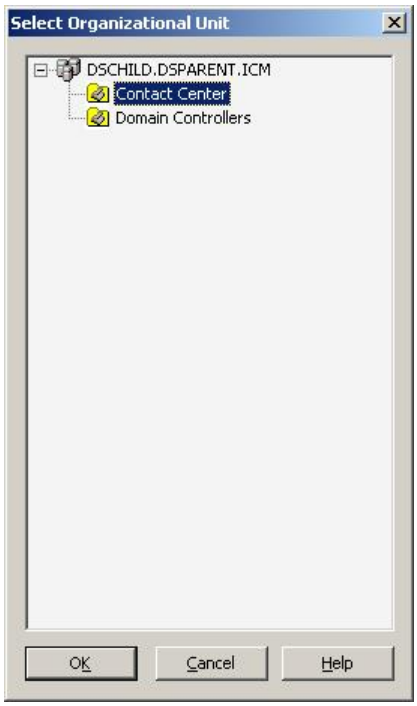
If the current domain, which the Domain Manager loads by default, is not the domain to which you want to add a root, then Add a domain you want (page 91)

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

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

This displays the Select Organizational Unit dialog box.

Figure 25: 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 (page 94) and configure security groups (page 97).

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.

Figure 26: Select OU Dialog Box After Creating the Cisco Root OU

See Also

What is the Cisco Root OU? on page 40

How to Remove the Cisco Root

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

Step 1 Open the Domain Manager (page 85).

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.

How to Create/Add a Facility OU

You create a Facility OU (page 41) to group one or more Instance OUs (page 41).

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

Before you can create a Facility OU, you must have created the Cisco Root OU (page 92) for the domain.

Step 1 Open the Domain Manager (page 85).

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 27: 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.

How to Remove a Facility OU

Note: Only users with administrative control at the level above the Facility OU might delete the Facility OU. To remove a Facility OU:

Step 1 Open the Domain Manager (page 85).

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.

How to Create/Add an Instance OU

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

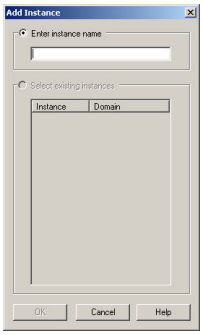
Step 1 Open the Domain Manager (page 85).

Step 2 In the tree view in the left pane, navigate to and select the Facility OU (page 41) under which you want to create the Instance OU.

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

The Add Instance dialog box (page 95) opens.

Figure 28: 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.

How to Remove an Instance OU

To remove an Instance OU:

Step 1 Open the Domain Manager (page 85).

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 29: Security Group Members Dialog Box

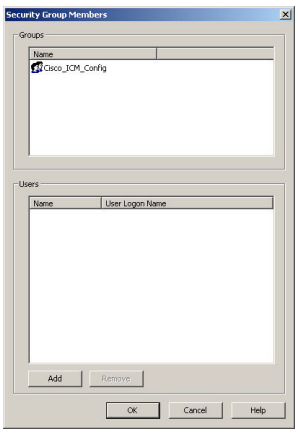


Table 10: Security Group Members dialog box Properties

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 Security Group (page 98).
Remove	Use this option to remove the selected users from the Users list.
OK	Use this option to save changes and return to Domain Manager (page 85).

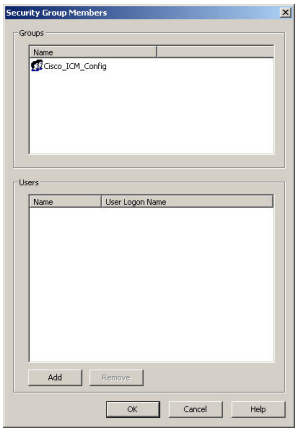
How to Add Users to a Security Group

Step 1 In the Domain Manager (page 85), 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.

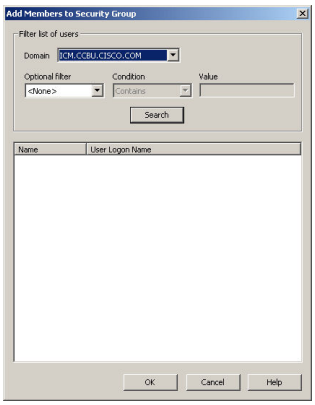
Figure 30: Security Group Members Dialog Box



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

The Add Members to Security Group dialog box appears.

Figure 31: 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 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.

How to Remove Members from a Security Group

Step 1 In the Domain Manager (page 85), select the Security Group you want to remove members from.

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

The Security Group dialog box appears.

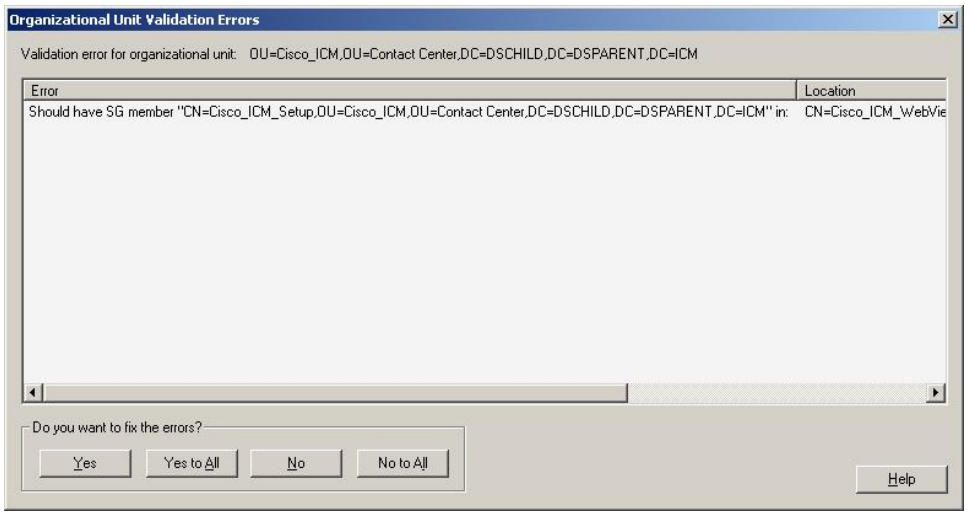
Step 3 In the Users pane, select the member you want to remove from the Security Group, from the displayed list.

Step 4 Click **Remove**.

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

Organizational Unit Validation Errors dialog box

Figure 32: Organizational Unit Validation Errors Dialog Box



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

Table 11: 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 additional errors are found, you are returned 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 additional errors are found, you are returned 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

Handling the User List Tool and Agent Explorer in Multi-Instance Situations

LimitUserAssociationByInstance

As of 8.0(1), the feature to restrict associating or adding a duplicate user to multiple instances has been set up. To turn on/ off this feature, you must change the registry value of *LimitUserAssociationByInstance*. This registry key is added when User List tool, Agent Explorer, or the ICM Installer is run.

The registry key is in: “HKEY_LOCAL_MACHINE\ SOFTWARE\Cisco Systems, Inc.\ICM\<*Running Instance Name*>\AW*LimitUserAssociationByInstance*” and by default is turned off (set to 0). To turn on this feature, use *regedit* to manually set this registry key to "1".

When *LimitUserAssociationByInstance* is set to 1, the feature is turned on and when using either the User List Tool or Agent Explorer, the following occurs:

- When you try to create a new user or associate a user who is already a member of different instance, the following message appears: “Cannot associate <*username*>, user account already exist in <*domain name*> domain”, where <*username*> and <*domain name*> will be populated dynamically with the actual values."

- When you get this error message, you must create a new user with a different name.

  Example: You are trying to create or associate a user called JohnSmith and this user already exists in a different Unified ICM instance than the instance you are in. When the error message is displayed, you can enter the username as JohnMSmith to make it unique.

  Note: To prevent users from acting on users from other customers, you need to prevent access to the Domain manager tool, and to any other third party AD tools which can access users in different Unified ICM instances.

Part 2: Staging Guidelines

Chapter 9

About Staging Prerequisites

System Design Specification

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

Persons creating and approving this specification must be:

- Familiar with Windows Operating System
  - AD
  - Security concepts
  - Network configuration and operation
- Familiar with SQL Server
  - Enterprise Manager
  - Query Analyzer
  - SQL scripting
- Unified ICM/Cisco Unified Contact Center Enterprise Knowledge
  - Unified ICM/Cisco Unified Contact Center Enterprise Nodes (Router, Logger, Administration & Data Server, PGs)
  - HDS Schema knowledge
  - Deployment models (including WebView)

  - Have read the Cisco Unified ICM/CCE/CCH *Hardware & System Software Specification (Bill of Materials)* and *SRND* for Release 8.0(1).

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's Best Practices) 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 deployment, you define the hardware specifications and third-party software requirements. You can find the Cisco guidelines for hardware and software requirements for Unified ICM in the *Hardware & System Software Specification (Bill of Materials) for Cisco Unified ICM/Contact Center Enterprise & Hosted*, available at **www.cisco.com** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

For additional information, see the *Cisco Unified Contact Center Enterprise (Unified CCE) Software Compatibility Guide* , available at **www.cisco.com** (http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_device_support_tables_list.html)

How to Set the Staging Environment

Follow these steps to set the staging environment:

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

Step 2 Ensure that there are at least two phone lines for testing dial-up modem access. (Optional)

Step 3 Ensure that all software CDs, driver software, and documentation is in the work area.

Step 4 Ensure that you have all software license numbers available.

Step 5 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 is IP connectivity between all subnets
- Required ethernet connections are in place between ICM software servers and LAN switches
- Required packet prioritization is configured on IP Routers

Step 6 Ensure that assigned engineers follow the System Design Specifications in the **Hardware & System Software Specification (Bill of Materials) for Cisco Unified ICM/Contact Center Enterprise & Hosted** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/

products_user_guide_list.html) and the *Unified Contact Center Enterprise Detail Design Template*.

Chapter 10

About Windows Server 2003 and 2008 R2 Staging

Note:

- This section does not provide step-by-step instructions for all tasks related to Microsoft Windows. For such information, see Microsoft documentation or the Windows online help.
- Webview is not supported in Release 8.5(1) or later and is not supported on Windows Server 2008 R2.

This chapter contains the following topics:

Drive Partitioning 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 and Administration & Data Server HDS Partitioning 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 space, core Unified ICM, Microsoft SQL Server, and SQL Server's log and temp files.
- Use the D drive to store the Logger or Historical Data Server database.

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

Router, Peripheral Gateway, Administration & Data Server, CTI Server, and CTI OS Server Partitioning Guidelines

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 space, core Unified ICM software, the Administration & Data Server database, Microsoft SQL Server, and SQL Server's log and temp files.

CD-ROM Drive

Assign the letter Z to the CD-ROM drive. While this is not mandatory, it provides consistency.

Windows Server 2003 & 2008 R2 Setup Guidelines

Note:

- For additional information on installing Microsoft Windows Server 2003, see the **Windows Server 2003 homepage** (http://www.microsoft.com/windowsserver2003/default.mspx)
- For additional information on installing Microsoft Windows Server 2008 R2, see the **Windows Server 2008 R2 homepage** (http://www.microsoft.com/windowsserver2008/en/us/default.aspx)

Use the following guidelines when setting up a Windows Server 2003 SP2 and Window Server 2008 R2 for Unified ICM :

- Enable the necessary Management and Monitoring Tools for Windows Server 2003 (page 112). These tools are automatically enabled for Windows Server 2008 R2 (page 112) by the UCCE installer..
- Do not install Internet Information Services unless the server will host WebView or Unified ICM multichannel options.

Note: Webview is not supported in Release 8.5(x) or later and is not supported on Windows Server 2008 R2.

- When setting the time zone, ensure all Central Controller systems are set for the same time zone regardless of their physical location.
- For Network Settings, select **Custom Settings**, and enter the server's respective IP and DNS data according to the System Design Specification.
- For the Visible Ethernet Card, perform the following tasks:
  - Set the properties for File and Printer Sharing for Microsoft Networks to maximize data throughput for network applications.
  - Enter the data for visible IP addresses, subnet mask, default gateway and preferred and alternate DNS servers for the server.
  - 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, 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.

    Note: See Persistent Static Routes (page 115) for information about configuring a default gateway for the private network.
  - In the **DNS** tab, leave the address space empty and uncheck **Register**.

    Note: After you complete the previous tasks, by default, the card appears as an unidentified network and is blocked by firewall settings. To correct this, configure the unidentified network as private.
- Configure the unidentified network as private.
  - Select **Start** > **Run**.
  - In the **Open** box, type **mmc** and then click **OK**.
  - In the **MMC** console, from the **File** menu, select **Add/Remove Snap-in**.

- In the **Available Snap-ins** list, click **Group Policy Object Editor** and click **Add**.
- Select **Local Computer** and then click **OK**.
- Click **OK** again.
- In the left pane, navigate to **Local Computer Policy** > **Computer Configuration** > **Windows Settings** > **Security Settings**.
- In the right pane, double-click **Network List Manger Policies**.
- Right-click **Unidentified Networks** and select **Properties**.
- For **Location type**, select the **Private** option.
- To grant users permission to change location, select the **user can change location** option.
- Click **Apply** and then click **OK** to close the **Properties** dialog box.
- To save the console changes, in the console window, click **File** > **Save**.

Enable SNMP Management on Windows Server 2003

To setup Windows Server 2003, choose **Start > Control Panel > Add or Remove Programs** then click **Add/Remove Windows Components**.

Select the necessary Management and Monitoring Tools:

- **Simple Network Management Protocol (SNMP)**
- **WMI Windows Installer Provider**

Note: See SNMP Management (page 115) for additional information.

Enable SNMP Management on Windows Server 2008 R2

Note: This step is completed automatically by the Release 8.0(1a) installer. The following steps are for reference.

To setup Windows Server 2008 R2, choose **Start > Control Panel** then click **Programs** then click **Turn Windows features on or off**.

Select the necessary Management and Monitoring Tools by clicking **Features** in the left pane, and clicking **Add Features** in the right pane. Check the **SNMP Services** which selects the following:

- **SNMP Service**
- **SNMP WMI Provider**

Click **Next** then **Install**.

Note: See SNMP Management (page 115) for additional information.

How to Join Standalone Servers to the Domain in Windows Server 2003

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

- Logger
- CallRouter
- Administration & Data Servers
- WebView Server

Note:

- WebView must be installed on the same domain as the Administration & Data Server/HDS.
- Webview is not supported in Release 8.5(x) or later and is not supported on Windows Server 2008 R2.

Step 1 Right-click **My Computer** and choose **Properties** > **Network Identification Tab** > **Properties**.

Step 2 Click **Domain**, then enter the Fully Qualified Domain Name and click **OK**.

Step 3 Enter the Domain Administrator's username and password.

Step 4 Reboot the server and login to the domain.

How to Join Standalone Servers to the Domain in Windows Server 2008 R2

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

- Logger
- CallRouter
- Administration & Data Servers

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 login to the domain.

Network Card Settings

Note: These instructions pertain to Windows Server 2003. Consult your Microsoft Documentation for Windows Server 2008 R2.

To setup the network card settings, choose **Start > Control Panel > Network Connections** then, in the menu bar, click **Advanced > Advanced Settings**, the Advanced Settings dialog box appears.

Use the following guidelines to configure network card settings:

- Rename each Local Area Connection to *private*, *visible*, and *san* as required.
- In the **Advanced** tab of the connection properties, configure the network (link) speed and duplex mode as follows:
  - **100 Mb NIC**: set both the NIC and the switch to **100/Full**
  - **100 Mb switch**: set both the NIC and the switch to **100/Full**
  - **100 Mb NIC and 100 Mb switch**: set both to **100/Full**
  - **Gigabit NIC and Gigabit switch**: ensure both are set to **Auto/Auto**
- In the Advanced tab, perform the following tasks:
  - In the Connection section of the Adapters and bindings tab, sort the section so that the Visible connection is at the top, the Private connection is second, and any remaining connections follow.
  - For the Private connection, uncheck File and Printer Sharing for Microsoft Networks and Client for Microsoft Networks.
  - Move any disabled Bindings for all connections to the bottom of the list.
  - Uncheck Register this connection's addresses in DNS.
- Click **Default** on the Netbios setting to ensure it is enabled (causing LicenseAdmin.exe for CAD to launch).

Persistent Static Routes

For geographically distributed Unified ICM Central Controller sites, duplexed CallRouter and Logger components have a Private IP WAN connection, used to communicate between Side A and Side B. Because Windows only allows one default gateway for each server (which sends the Private Network traffic to the Visible Network), you must add a set of Static Routes to all the servers running the CallRouter and Logger.

On the Side A CallRouter and Logger servers, enter **`route add<network number>mask<subnet mask><gateway IP> -p`**.

For example:

- On Side A servers, enter **`route add 192.168.142.42 mask 255.255.255.192 192.168.141.126 -p`**.

  On Side B servers, enter **`route add 192.168.141.64 mask 255.255.255.192 192.168.142.126 -p.`**.

- Where
  - The network number of the remote Private Network is 192.168.142.42
  - The subnet mask for this remote network is 255.255.255.192
  - The gateway address for the Private Network Adaptor is 192.168.141.126

Note: The -p option sets the route as persistent.

SNMP Management

SNMP management support is installed and enabled by default on Unified ICM/CCE/CCH servers. However, to ensure seamless integration with the Microsoft native SNMP components, installation of the Microsoft Management and Monitoring Tools subcomponents is required.

Note: These instructions pertain to Windows Server 2003 only. For Windows Server 2008 R2, to view the SNMP Agent Management snap-in, you must use the 32-bit Microsoft Management Console Snap-In. To launch the 32-bit Snap-in, run **mmc /32**. For detailed instructions for Windows Server 2008 R2, consult your Microsoft Documentation.

If SNMP management support has already been installed and configured for this server, the existing configuration parameters must be collected so they can be used to configure the components installed by the WEB SETUP. These parameters can be found on the property sheets associated with the Microsoft SNMP Service.

To collect existing SNMP properties:

1. On the Services MMC console, locate and select the **SNMP Service** in the list.

   -or-

   Choose **Start** > **Programs** > **Control Panel** > **Services**.

2. Click **Properties** (or select the Properties context menu).

3. 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 and/or IP addresses configured in the associated list box.

     Note: If host names (vs. IP addresses) have been configured, you need to determine the actual IP address of that host in order to configure the Cisco SNMP agents. For security reasons, using static addresses for management stations is preferred.

4. 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, you need to determine the actual IP address of that host.

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

   Collect the information from the Contact and the Location fields.

If the server has not been configured for SNMP manageability, engage in a dialog box with the customer IT professionals to:

1. Determine whether the customer desires SNMP manageability.

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 & Hosted* for more details.

Installing the Windows Firewall on Windows Server 2003

Note: These steps are not required for Windows Server 2008 R2. The firewall is installed automatically and Unified CCE setup makes the required changes for UCCE compatibility.

Load the appropriate Service Pack. Do not manually configure the firewall, use the CiscoICMfwConfig application, this installs and configures the Windows firewall.

See Also

- For additional information, see *Security Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 9.x(y)* available on **www.cisco.com** (http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_technical_reference_list.html).
- For detailed information on supported platforms for Unified ICM, see the *Hardware & System Software Specification (Bill of Materials) for Cisco Unified ICM/Contact Center Enterprise & Hosted* available on **www.cisco.com** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).
- For additional information on the Windows Firewall, see *Windows Server 2003 Windows Firewall (WF)* available on **www.microsoft.com** (http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/wf.mspx), and *Help: Windows Firewall How To...* available at **www.microsoft.com** (http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/005d7651-fefa-4e00-8f55-714fc0175fe1.mspx)

Configuring Windows Server 2003 Firewall to Communicate With AD

Note: These steps are not required for Windows Server 2008 R2. The firewall is installed automatically and Unified CCE setup makes the required changes for UCCE compatibility.

You need to open up the ports used by domain controllers (DCs) for communication via LDAP and other protocols to ensure AD is able to communicate through a firewall.

Be sure to consult the Microsoft Knowledge Base (KB) **KB179442** (http://support.microsoft.com/kb/179442/en-us) for important information about configuring firewall for Domains and Trusts.

To establish secure communications between DCs and Unified ICM Services you need to define the following ports for outbound and inbound exceptions on the firewall:

- Ports that are already defined
- Variable ports (high ports) for use with Remote Procedure Calls (RPC)

Configuring Domain Controller Ports

The following port definitions must be defined on *all* DCs within the demilitarized zone (DMZ) that might be replicating to external DCs. It is important that you define the ports on all DCs in the domain.

Restrict FRS Traffic to a Specific Static Port

Be sure to consult the Microsoft Knowledge Base (KB) **KB319553** (http://support.microsoft.com/kb/319553/en-us) for more information about restricting File Replication service (FSR) traffic to a specific static port.

Step 1 Start **Registry Editor** (Regedt32.exe).

Step 2 Locate and then click the following key in the registry:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTFRS\Parameters

Step 3 Add the following registry values:

- New: **Reg_DWORD**
- Name: **RPC TCP/IP Port Assignment**
- Value: **10000 (decimal)**

Restrict AD replication traffic to a specific port

Be sure to consult the Microsoft Knowledge Base (KB) **KB224196** (http://support.microsoft.com/kb/224196/en-us) for more information about restricting AD replication traffic to a specific port.

Step 1 Start **Registry Editor** (Regedt32.exe).

Step 2 Locate and then click the following key in the registry:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

Step 3 Add the following registry values:

- New: **Reg_DWORD**
- Name: **RPC TCP/IP Port**
- Value: **10001 (decimal)**

Configure Remote Procedure Call (RPC) port allocation

Be sure to consult the Microsoft Knowledge Base (KB) **KB154596** (http://support.microsoft.com/kb/154596/en-us) for more information about configuring RPC port allocation.

Step 1 Start **Registry Editor** (Regedt32.exe).

Step 2 Locate and then click the following key in the registry:
HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc

Step 3 Add the **Internet** key.

Step 4 Add the following registry values:

- Ports: **MULTI_SZ: 10002-10200**
- PortsInternetAvailable: **REG_SZ : Y**
- UseInternetPorts: **REG_SZ : Y**

Windows Server 2003 & 2008 R2 Firewall Ports

Be sure to consult the Microsoft Knowledge Base (KB) **KB179442** (http://support.microsoft.com/kb/179442/en-us) for a detailed description of the ports that are used to configure a firewall for domains and trusts.

Server Port	Protocol	Protocol	Service
135	TCP	RPC	RPC Connector Helper (machines connect to determine which high port to use)
137	TCP	UDP	NetBIOS Name
138		UDP	NetBIOS NetLogon and Browsing
139			NetBIOS Session
123		UDP	NTP
389	TCP		LDAP

Server Port	Protocol	Protocol	Service
636	TCP	UDP	LDAP SSL
3268			LDAP GC
3269			LDAP GC SSL
42			Wins Replication
53	TCP	UDP	DNS
88	TCP	UDP	Kerberos
445	TCP	UDP	SMB over IP (Microsoft-DS)
10000	TCP		RPC NTFRS
10001	TCP		RPC NTDS
10002 - 10200	TCP		RPC - Dynamic High Open Ports
	ICMP		

Testing Connectivity

To test connectivity and show the FRS configuration in AD, use the Ntfrsult tool.

Step 1 From the command line, run the Windows File Replication utility: **Ntfrsutl version** <server_name>.

When communications between the domain controllers are configured properly, the ntfrsutl output shows the FRS configuration in AD.

Validating Connectivity

To validate connectivity between the domain controllers, use the Portqry tool.

Visit the following Microsoft Web site: **http://download.microsoft.com/download/3/f/4/3f4c6a54-65f0-4164-bdec-a3411ba24d3a/PortQryUI.exe (http://download.microsoft.com/download/3/f/4/3f4c6a54-65f0-4164-bdec-a3411ba24d3a/portqryui.exe)** to obtain the tool.

Step 1 Download the **PortQryUI.exe** and run the tool.

Step 2 Select the destination CD or PDC.

Step 3 Select **Domains and Trusts**.

Step 4 Use the response from PortQry to verify whether the ports are open.

Be sure to consult the Microsoft Knowledge Base (KB) **KB832919** (http://support.microsoft.com/kb/832919/en-us) for more information about PortQry features and functionality.

Display Settings

Through the Windows Control Panel Display dialog box:

- Ensure that no window 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

Through the Windows Control System dialog box Advanced tab:

- When setting virtual memory, set the initial and maximum total paging file sizes to the values required by the system.
- For Startup and Recovery settings, set the value of the **Time to display list of operating systems** to **3** seconds.
- On the Advanced tab of the System Properties dialog box, set the Performance Options to either **Programs** or **Background Services**.

Event Viewer Configuration

Configure the Event Viewer:

- For each type of event, set the **Maximum log size** to **8192 KB**.
- Select **Overwrite events as needed**.

Note: These settings are configured by the Security Template provided with automated hardening on Windows Server 2003. See the *Security Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 9.x(y)* available on **www.cisco.com** (http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_technical_reference_list.html) for additional information.

Connectivity Validation

Before you begin the Unified ICM installation process, you must 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.

Note: See the System Design Specification (page 105) to confirm that the system topology is correct.

Chapter 11

About Microsoft SQL Server Staging

Unified ICM requires that you install Microsoft SQL Server on each server that hosts a Logger or Administration & Data Server (Real Time Distributor and HDS only) component.

This section contains guidelines for setting up Microsoft SQL Server for use with the system's Logger and Administration & Data Server components.

Note: Unified ICM/CCE/CCH Release 8.0(1) supports SQL Server 2005 with SP3+ for new installs and upgrades on Windows Server 2003. If you are using Windows Server 2008 R2 then you must install SQL Server 2005 with SP4+. Systems with SQL 2000 must upgrade to SQL 2005 SP3 before upgrading Unified ICM.

For more information about specific versions and patches of Microsoft SQL Server supported by system software, see *Hardware & System Software Specification (Bill of Materials) for Cisco Unified ICM/Contact Center Enterprise & Hosted* available on **www.cisco.com** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

Note: This section does not provide step-by-step instructions for tasks related to Microsoft SQL Server. For such information, see Microsoft documentation.

This chapter contains the following topics:

SQL Server Component Installation

This section contains the following topics:

- Authentication Mode (page 126)
- Character Set and Sort Order (page 126)
- Database and Log File Size (page 126)

Custom Setup Requirements

During the installation process, you must select **Custom** for the setup type.

Follow these guidelines for customizing the installation:

- In the Components dialog box, accept the defaults.
- For SQL Server Service Account, select the following options:
  - **Customize**
  - **Use a Domain Account**

    Note: The Domain account must be created prior to installing SQL Server according to Microsoft recommendations.

The MS SQL Server Agent services, MSSQLServer and SQLServerAgent, must not be run under the administrator or local system accounts. Cisco recommends that a domain user account be used. The service account will not be a member of the local or domain administrators group. The service account must be denied the interactive logon right and be added to the SQL Server SYSADMIN role if Enterprise Manager is used to setup the startup service account otherwise this is done automatically during SQL Server installation.

The goal here is to limit the privileges of the SQL Server service. After creating the domain account and assigning it the required permissions as listed below, use it to customize the installation of SQL Server.

Note that this user account (for example SQLServiceAcct) must be created with the following properties:

- User cannot change password
- Password never expires

The SQL Server Agent service account requires the following rights to be set on the host's Local Security Policy Settings:

- Access this computer from network
- Act as part of the operating system
- Adjust memory quotas for a process (Windows Server 2003 and 2008)

- Deny log on locally
- Log on as a batch job
- Log on as a service
- Replace a process-level token

Caution: If you use the Services applet that is in Control Panel or in Administrative Tools to change the startup account information for the MSSQLServer service or the SQL Server Agent service, there are additional permissions and user rights that must be set manually.

See the **Security Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.0(1)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html) for details on configuring SQL Server to use a domain user account to run the MSSQLServer service after it has been installed using the default Local System Account.

Basic SQL Server 2005 with SP3 or SP4 Component Installation Options

This section provides an overview of the basic SQL Server component installation options.

Do the following when starting the SQL Server setup application:

1. On the Start window, select **Server components, tools, Books Online, and samples**.
2. Install the following components: **SQL Server Database Services**, **Workstation components**, and **Books Online and development tools**.
3. For the Instance Name, select **Default instance**.
4. Select **Use a domain user_account** for the Service Account.
5. Select **Window Authentication Mode** or **Mixed Mode (Windows Authentication and SQL Server Authentication)**, as appropriate.
6. For the Collation settings, select **Collation designer and sort order**, then **Latin 1_General** and **Binary**.
7. When the SQL 2005 Installation is complete, select **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager**.
8. Expand **SQL Native Client Configuration** and select **Client Protocols**.
9. A list of the client protocols displays.

   The correct order and states are:

   – **Shared Memory** - Enabled

   – **Named Pipes** - Enabled

– **TCP/IP** - Enabled

– **VIA** - Disabled

10. If the order and associated states are not as indicated in the previous step, right-click **Client Protocols** and select **Properties**.

    The Client Protocol Properties dialog appears. Use the dialog controls to ensure that the client protocols are in the correct position.

11. Click **OK**.

    The Client Protocol Properties dialog closes.

12. Expand the **SQL Server Network Configuration** and select **Protocols for MS SQL Server**.

13. Ensure that **Named Pipes** and **TCP/IP** are in the **Enabled Protocols** section. If either is not, right-click the disabled protocol name and select **Enable**. Ensure **VIA** is in the Disabled Protocols section.

14. On the Menu bar, select **File** > **Exit**.

    The SQL Server Configuration Manager closes.

Authentication Mode

For the Authentication Mode, select **Windows Authentication Mode** and select a **strong password** for the 'SA' account.

Note: Environments integrated with the Cisco Interaction Manager (CIM) product suite require selecting **Mixed Authentication Mode**, as CIM applications does not support Windows authentication mode. In addition, some environments have custom applications that access the Unified ICM Logger and/or HDS databases; these applications require selecting **Mixed Authentication Mode** because these applications do not support Windows Authentication.

Character Set and Sort Order

You must:

- Set the Collation Designator to **Latin1_General**.
- Check **Binary** for the sort order.

Database and Log File Size

Use the Microsoft SQL Server Enterprise Manager to increase the database and log sizes.

For the Tempdb, follow these guidelines:

- For Data Files:
  - Set the **Space Allocated** to **1400 MB**.
  - Set **Automatically grow files**.
  - Set **Unrestricted file growth**.
- For Transaction Log Files:
  - Set the **Space Allocated** to **400 MB**.
  - Set **Automatically grow files**.
  - Set **Unrestricted file growth**.
  - In the Options tab, clear the following options: **ANSI NULL**, **Recursive triggers**, **Auto close**, **Auto shrink** and **Use quoted identifiers**.

Installing SQL Service Packs

Install the latest supported SQL service pack as indicated by the **Cisco ICM/IPCC Enterprise & Hosted Editions Release 8.0(1) Hardware and System Software Specifications (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

How to install SQL Server service packs:

1. Download the appropriate SQL Server service pack from the Microsoft web site.
2. Following the instructions provided with the service pack, install it.

Verifying SQL Protocol Order

Verify the Enabled Protocols order is Named Pipes, then TCP IP using the MS SQL Client Network Utility (**Start > All Programs > MS SQL Server > Client Network Utility**).

Appendix A

Installing the Domain Controller on Windows Server 2003 SP2

How to Install the Domain Controller on Windows Server 2003 SP2

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

Step 1 Choose **Start** > **Run** > and enter **`dcpromo.exe`**.

Step 2 Click > **OK**.

Step 3 Click **Next** through the Active Directory Wizard windows until you reach the *Domain Controller Type* window.

Step 4

If: Installing the first server,

Then: Select the **Domain controller for a new domain** radio button.

For any additional servers installed. select the **Additional domain controller for an existing domain**.

Step 5 Click **Next**.

The *Create New Domain* window appears.

Step 6

If: Creating a new domain for an Enterprise or NAM instance,

Then: Select the **Domain in a new forest** radio button.

If: Creating a new domain for an Enterprise instance in a child domain,(where the Hosted NAM would be the parent and CICM Instances are given their own domain),

Then: Select the **Child domain in an existing domain tree** radio button.

Note: See Supported Domain Models (page 21).

Step 7 Click **Next**.

The *New Domain Name* window appears.

Step 8 Enter the DNS name. The DNS name must have a suffix. You might use whatever you want for a suffix (examples, .com, .icm, .ipcc, .lab - if this is a corporate domain installation, follow these guidelines).

Step 9 Click **Next**.

The *NetBIOS Domain Name* window appears.

Step 10 Enter the NetBIOS Domain Name.

Note: The NetBIOS name must be the prefix of the DNS name, for example, if the DNS name is "Cisco.com", the NetBIOS name would be "Cisco".

Step 11 Click **Next** until the *DNS Registration Diagnostics* window appears.

Note: Accept the default values for the Database and Log Folders and the Shared System Volume windows unless instructed otherwise.

Step 12 Always select **Install and configure DNS server on this computer**, and set this computer to use this DNS server as its preferred DNS server.

Note: AD DNS servers must be in the DNS path for each server. This is accomplished by pointing directly to the AD servers or by having other DNS servers forward to the DNS servers.

Step 13 Click **Next** through the end of the wizard, then click **Finish**.

Step 14 When prompted, restart Windows.

Appendix B

Moving the Cisco Root OU

Introduction

This section describes the instructions to safely move the Cisco Root OU from one OU to another within the same domain. This is accomplished by 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.

This document is relevant for Release 8.0(1) of Unified ICM .

Definitions

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

Cisco Root OU

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

Domain Manager

A tool for creating all Cisco OUs along with their associated groups and permissions. This help 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.
- All Unified ICM Services and applications must be stopped while following these instructions. For duplexed systems, both the primary and secondary systems must be stopped.
- Obtain and record the Instance Number of each Unified ICM instance on the system.

Best Practices to Avoid Problems

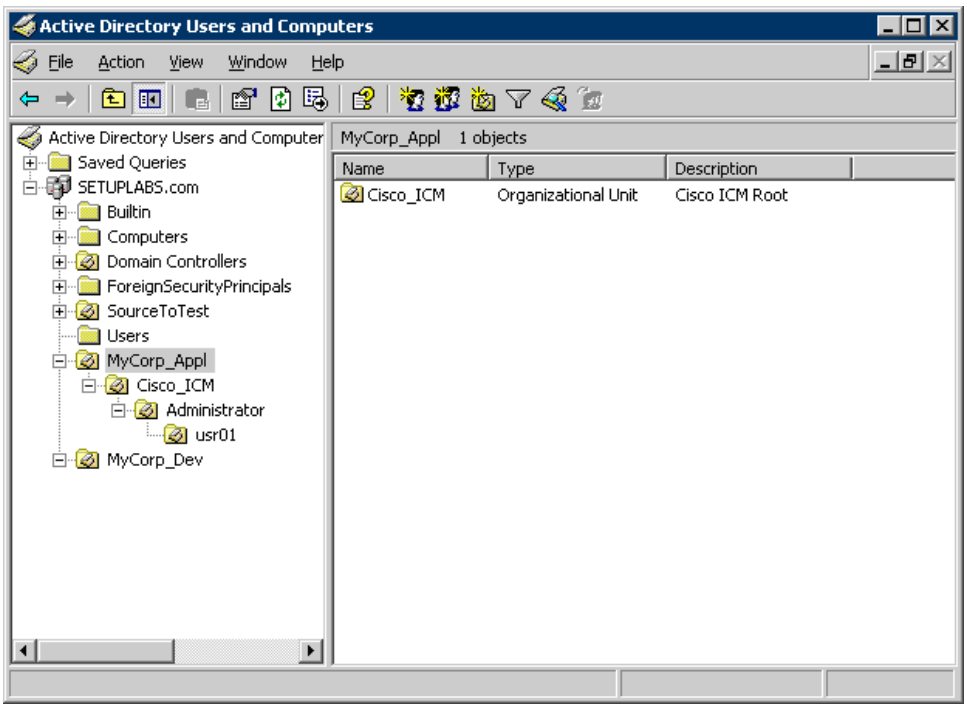
Perform the following to avoid problems:

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.

How to transfer the 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 new OU called MyCorp_Dev.

Figure 33: SETUPLABS Domain



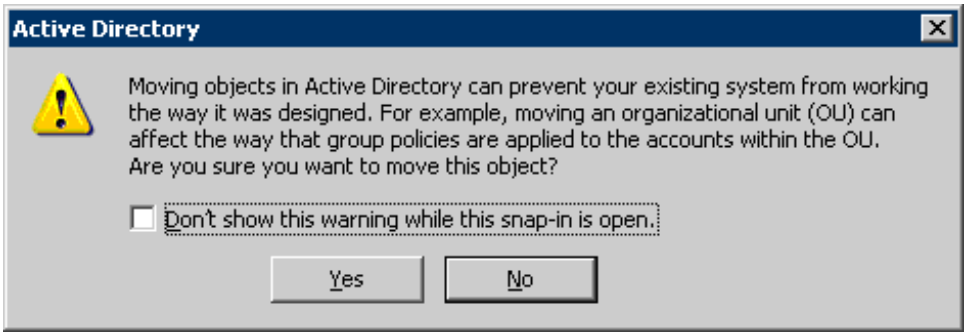
Step 1 On the Domain, find the OU in which the Cisco Root OU is contained.

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.

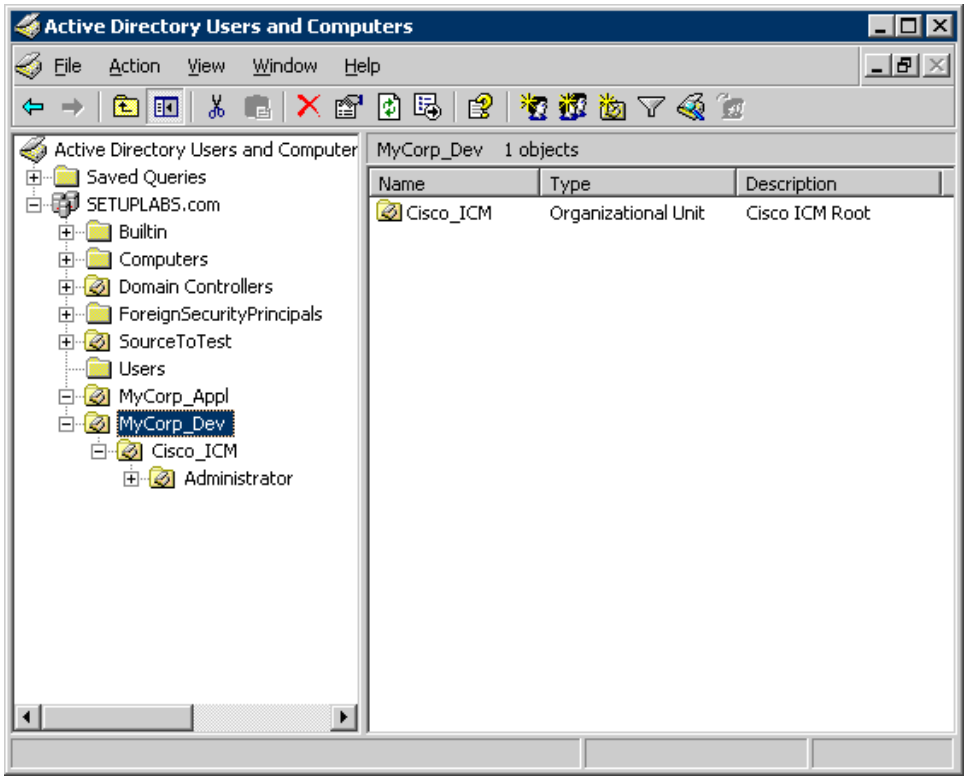
Figure 34: AD Moving Objects Error Message



Step 4 Click **Yes** to continue.

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

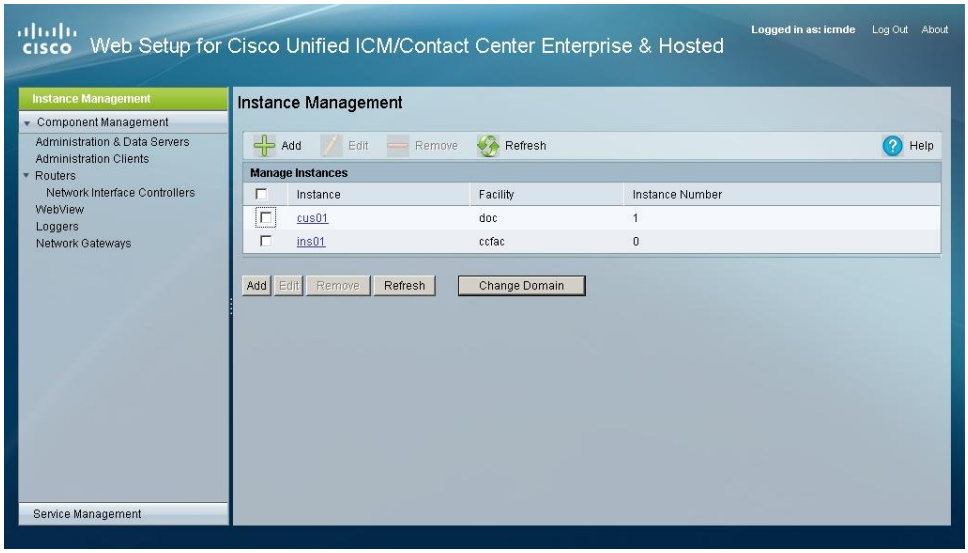
Figure 35: Cisco Root OU Location



Step 5 Click **OK**.

Run Web Setup. Open the Instance Management page.

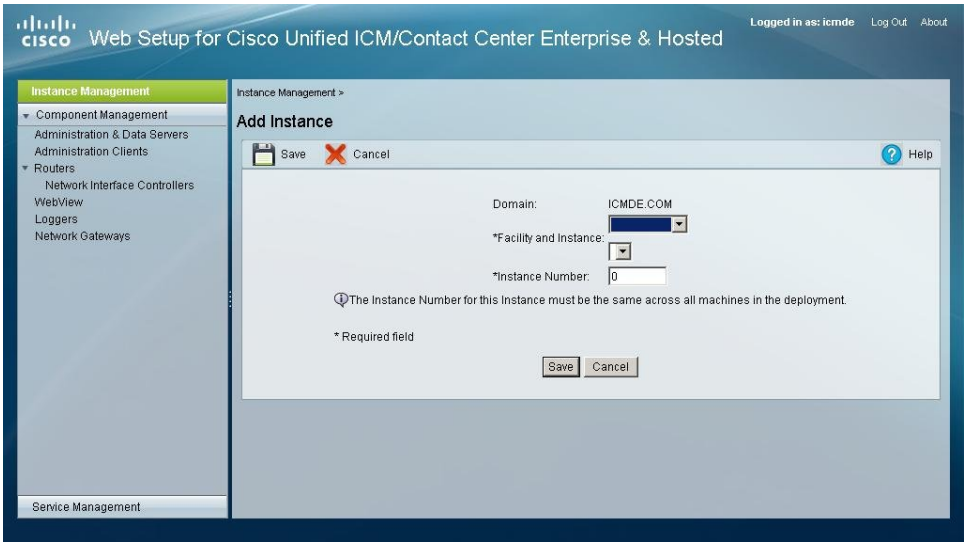
Figure 36: ICM Setup Dialog Box



Step 6 Click **Add**.

The Add Instance page opens.

Figure 37: Add Instance Dialog Box



Note: You can add instances based on your Setup privileges for instances. Setup privileges can be granted at the Instance level, the overall ICM root level, or at the domain level.

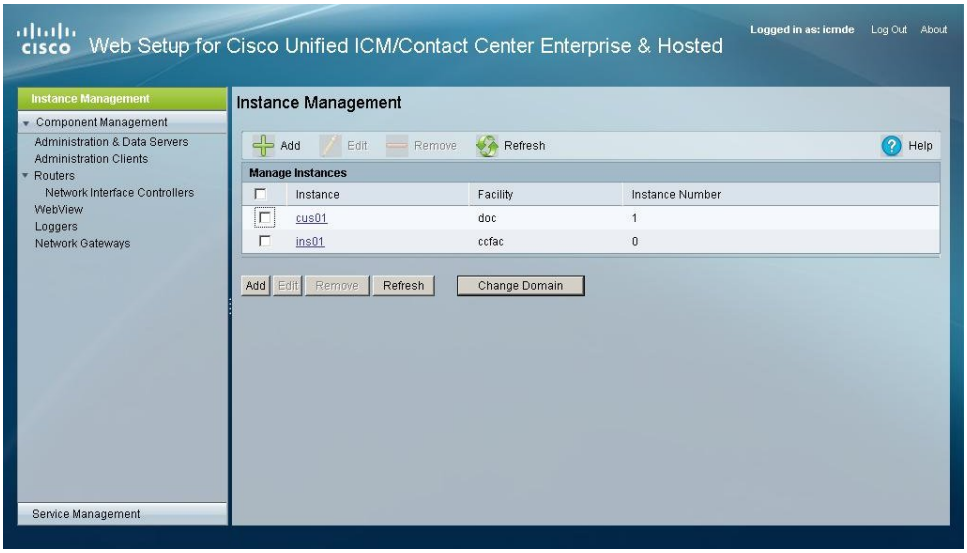
Step 7 From the drop-down lists, select a facility and then select an instance.

There can be more than one occurrence of an instance name in a domain, so the instance number provides the uniqueness. The instance number must be a whole number greater than or equal to zero. The instance number must match for the same instance across your entire deployment

Step 8 Click **Save**. You are returned to the Instance List page.

Step 9 Return to the Instance Management page.

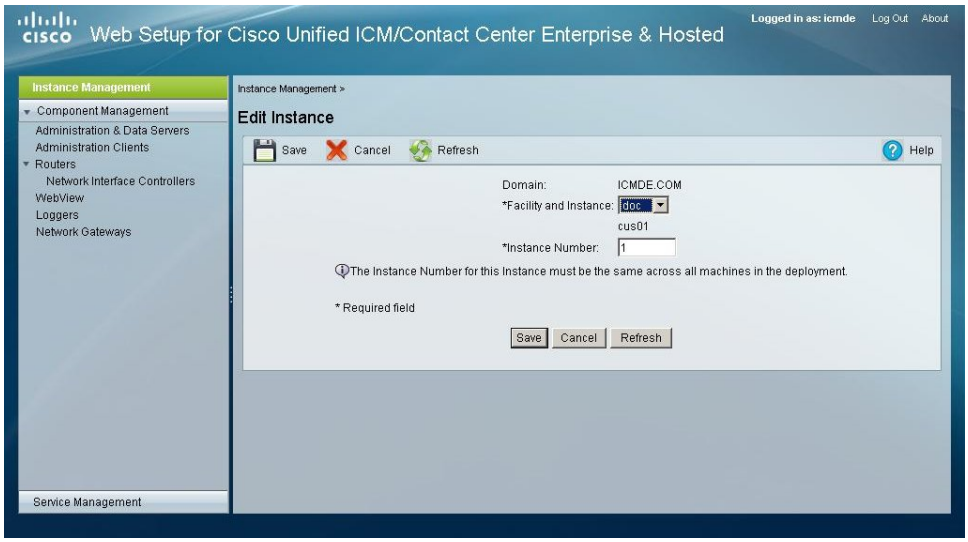
Figure 38: ICM Setup Dialog Box



Step 10 Click **Edit**.

The Edit Instance dialog box is displayed.

Figure 39: Edit Instance Dialog Box



Step 11 Edit the **Facility** and/or the **Instance Number** fields. (You cannot edit the Domain field.)

Step 12 After making any desired changes, click **Save**. You are returned to the Instance List page.

Step 13 Start all Unified ICM Services.

Step 14 Run the **Configuration Manager** tool.

Step 15 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 to ensure all the users in the User List Tools have the correct permissions.

Index