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

Release 7.x(y)

May 2011

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 Enterprise and Hosted ICM. Those Models are:

- Enterprise ICM Dedicated Forest/Domain Model
- Enterprise ICM Child Domain Model
- Hosted NAM/CICM Model

Audience

This document is intended for the individuals responsible for staging deployments of Cisco Unified ICM/Contact Center, Enterprise & Hosted, as well as Cisco Unified System CCE. Individuals must be trained on the use and functions of ICM as well as Windows 2003, Active Directory and DNS. This document does not provide detailed Enterprise ICM, Hosted NAM/CICM or Windows 2003 specific information. This information can be found elsewhere in specific documentation from Cisco and/or Microsoft.

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

- Hosted NAM/CICM Model
- Cisco ICM Scripting and Configuration Tools
- Cisco ICM WebView and third party software (if installed)

- Windows 2003 system administration
- Microsoft SQL Server administration.

Organization

Chapter	Description
Chapter 1: About Active Directory for ICM Software (page 9)	Provides an overview of Active Directory, the benefits of using it, and the versions supported by ICM.
Chapter 2: Domain Requirements and Supported Topologies (page 13)	Provides the domain and Active Directory requirements for the ICM software. Discusses ICM requirements for Group Policy in Active Directory, DNS requirements, and the supported domain topographies. Provides the steps necessary to configure Active Directory 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, the OU hierarchy, the Cisco Root OU, Facility and Instance OUs, and how they relate to the 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.
Chapter 6: About ICM Software Setup and Active Directory (page 89)	Covers how to prepare to work with Active Directory; how Setup, the Domain Manager, and the OU hierarchy relate, and a listing of the functions of the Domain Manager.
Chapter 7: About the Cisco ICM Domain Manager (page 91)	Discusses the theory of operation and use of the Cisco Domain Manager.
Chapter 8: About the IPCC Machine Initializer Utility (page 109)	Discusses the IPCC Machine Initializer utility. Provides the steps to create the IPCC Root and Facility, and how to use the Machine Initializer utility. Also provides the mapping between System IPCC and ICM components.
Chapter 9: Handling the User List Tool and Agent Explorer in Multi-Instance Situations (page 113)	Discusses the LimitUserAssociationBy Instance registry key and how it implements the ability to restrict associating, or adding, a duplicate user to multiple instances.
Chapter 10: About Staging Prerequisites (page 117)	Discusses system design specification, the hardware and software platform requirements, and how to set the staging environment.
Chapter 11: About Windows Server 2003 Staging (page 121)	Provides the information necessary to properly stage a Windows Server 2003 system in preparation prior to installing Windows Server 2003.
Chapter 12: About Microsoft SQL Server Staging (page 135)	Provides the information necessary to properly stage a system in preparation for installing Microsoft SQL Server 2000 or SQL Server 2003. Discusses the steps required to perform a SQL Server 2000 or a SQL Server 2000 installation.
Chapter 13: Active Directory and Domain Troubleshooting (page 149)	Provides troubleshooting references and hints; and lists and describes the various tools available to troubleshoot Active Directory and Domain issues.

Chapter	Description
Appendix A: How to Install the Domain Controller on Windows 2003 (page 167)	Discussed the steps required to install the Domain Controller on Windows 2003.
Appendix B: Moving the Cisco Root OU (page 169)	Provides the necessary information and steps required to move the Cisco Root OU from one OU to another within the same domain.
Appendix C: Migrating ICM Servers from Multiple Forest to Single Forest for ICM/IPCC 5.0(0) Hosted (page 177)	Provides the steps required to migrate ICM/IPCC 5.0(0) Hosted system components from a multi-forest to a single forest.
Glossary (page 189)	Provides a list of Unified ICM/Contact Center terms and definitions/explanation.

Related Documentation

Documentation for Cisco Unified ICM/Unified Contact Center (IPCC) Enterprise & Hosted, as well as related documentation, is accessible from Cisco.com at **http://www.cisco.com/web/psa/products/index.html** (http://www.cisco.com/web/psa/products/index.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 IP IVR, Cisco Support Tools, and Cisco Remote Monitoring Suite (RMS).

  For documentation for these Cisco Unified Contact Center Products, go to **http://www.cisco.com/web/psa/products/index.html** click on **Voice and Unified Communications**, then click on **Cisco Unified Contact Center Products** or **Cisco Unified Voice Self-Service Products**, then click on the product/option you are interested in.

- Also related is the documentation for Cisco Unified Communications Manager, which can also be accessed from **http://www.cisco.com/en/US/support/index.html** (http://www.cisco.com/web/psa/products/index.html)

- 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 Unified ICM/Contact Center Enterprise & Hosted, Release 7.x** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html) before staging your Windows 2003 environment. The Security Best Practices document contains important guidelines for creating a secure Windows Server environment.

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. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*) • A book title. Example: See 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. Example: `<html><title>Cisco Systems,Inc. </title></html>`
< >	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Obtaining Documentation and Submitting a Service Request

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

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

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

Documentation Feedback

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

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.

Documentation Feedback

Part 1: Active Directory and ICM Software

Chapter 1

About Active Directory for ICM Software

What is Active Directory for ICM Software?

Microsoft Windows Active Directory is a Windows Directory Service that provides a central repository for managing network resources. ICM software uses Active Directory to control users' access rights to perform setup, configuration, and reporting tasks. Active Directory also grants permissions for different components of ICM software to interact; for example, it grants permissions for a Distributor to read the Logger database.

This document provides details of how ICM software uses Active Directory.

Note: This document does not provide more general information on Active Directory. It is therefore recommended that ICM Administrators be familiar with Microsoft's Active Directory documentation.

See Also

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

What Versions of Active Directory are Supported by ICM Software?

ICM software supports Active Directory for **Windows 2000** and **Windows Server 2003**. Also, ICM software version 7.5(4) and later supports Active Directory for **Windows Server 2008**.

See Also

For detailed information on supported platforms for ICM software, see the **Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)

What are the Benefits of Using Active Directory?

Support for Corporate Domain Installations

In releases prior to Release 7.0, you had to install ICM software in a separate, dedicated Windows AD domain. Installation into the corporate domain was not allowed. This requirement caused additional administration overhead.

Starting with Release 7.0, you can install ICM software in an existing Windows domain, including the corporate domain, and utilize the Active Directory functionality your network already supports to control access to ICM functions.

Note: You cannot collocate ICM components with the domain controller.

You decide where in your Organizational-Unit (page 39) hierarchy to place ICM resources.

No Domain Administrator Requirement

In releases prior to Release 7.0, you had to have domain administration privileges to perform installation-related tasks. This is no longer a requirement. As of Release 7.0(0), in order to run ICM Setup you must be a local machine administrator and belong to the setup group for any instance for which you are installing a component. The System IPCC Installer can only be run by a user that is both a local machine administrator and logged in as a domain user with rights to create Organizational Units (OUs).

Starting with ICM/Contact Center Release 7.0, you can determine which users in your corporate domain have access rights to perform specific tasks. You do this with the Domain Manager tool (page 92), which is integrated with the ICM Setup program. For System IPCC, use the Active Directory tools to perform these functions.

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 Active Directory user.

Streamlined Administration

In releases prior to Release 7.0, you could grant users permissions both through the dedicated Windows domain and through the ICM Configuration Manager User List tool. The problem was that some rights were granted only through the User List tool, while others were granted when using Microsoft tools to create users on the domain.

Starting with Release 7.0, ICM software uses Active Directory to control permissions for all users. Administrators no longer need to enter redundant user information. ICM software relies on Active Directory for setup, configuration, and reporting permissions; the use of the User List tool is reduced.

Standard Windows Naming Conventions

Active Directory supports standard Windows naming conventions; starting with Release 7.0, there are no longer specific naming requirements for the ICM software user names or the domain name.

Chapter 2

Domain Requirements and Supported Topologies

This chapter contains the following topics:

Ensuring a Healthy Active Directory Environment for ICM 7.0

When preparing to install ICM in a new, or existing, Active Directory environment, it is imperative that the environment be sound. As a general rule, for all domain controllers in a forest, you should 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 Active Directory, see Active Directory Management Pack Technical Reference for MOM 2005 on the Microsoft TechNet website.

Microsoft provides several tools to ensure AD health and connectivity that you can use to verify that your AD environment is ready for ICM. These include the tools listed in the following table.

Table 1: Microsoft Active Directory 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 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 2000/2003 Support Tools are not already installed, install them now. If you do not have a Windows installation disk available, download the **Windows Server 2000/2003 Support Tools** (http://www.microsoft.com/downloads/details.aspx?familyid=6EC50B78-8BE1-4E81-B3BE-4E7AC4F0912D&displaylang=en) .
- After installing the Windows Server 2000/2003 Support Tools, you must either log off, then log back on; or reboot your system in order to set the path.

Once the tools are installed, run the following:

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

How to run dcdiag.exe

Step 1 Click **Start**.

Step 2 Click **Run**.

Step 3 Type **cmd**.

Step 4 Press **Enter**.

A command console opens.

Step 5 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 idividual domain controller.

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

Step 6 Open the text file and note any items prefaced with "Warning" or "Error".

Step 7 Correct all the issues, then re-run dcdiag.exe to ensure there are no remaining issues.

How to run netdiag.exe

Step 1 Click **Start**.

Step 2 Click **Run**.

Step 3 Type **cmd**.

Step 4 Press **Enter**.

A command console opens.

Step 5 At the prompt enter: **netdiag.exe /fix /v /l** .

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

Step 6 Open the text file and note any items prefaced with "Warning" or "Error".

Step 7 Correct all the issues, then re-run netdiag.exe to ensure there are no remaining issues.

How to run repadmin.exe

Step 1 Click **Start**.

Step 2 Click **Run**.

Step 3 Type **cmd**.

Step 4 Press **Enter**.

A command console opens.

Step 5 At the prompt enter: **repadmin.exe /showrepl * /csv >showrepl.csv**.

Note: The acronym csv stands for comma separated values. Move the csv file created running repadmin to a machine with MS Excel installed.

Step 6 Open MS Excel and select **File > Open**.

Step 7 In the "Files of type" section, click **Text Files (*.prn;*.txt;*.csv)**.

Step 8 In the "Look in" section, navigate to *showrepl.csv*, then click **Open**.

Step 9 In the MS Excel spreadsheet, right-click the column heading for showrepl_COLUMNS (column A), then click **Hide**.

Step 10 In the MS Excel spreadsheet, right-click the column heading for Transport Type, then click **Hide**.

Step 11 Select the row just under the column headings, then select **Windows > Freeze Pane**.

Step 12 Click the upper-left corner of the spreadsheet to highlight the entire spreadsheet. Select **Data > Filter > AutoFilter**.

Step 13 In the heading of the Last Success column, click the **down arrow**, then click **Sort Ascending**.

Step 14 In the heading of the Source DC column, click the **down arrow**, then click **Custom**.

In the Custom AutoFilter dialog, 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 15 In the heading of the Last Failure column, click the **down arrow**, then click **Custom**.

In the Custom AutoFilter dialog, 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 16 Use Autofilter in Excel to view the replication health for the:

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

You can observe the replication partners that are replicating successfully.

Step 17 Locate and resolve all errors.

Step 18 Re-run repadmin.exe to ensure no issues remain.

Domain Requirements

Warning: The Domain Controller and DNS servers can not be collocated on any ICM component and must be installed with a separate server.

The following are domain requirements:

- Choose a supported domain model in this guide.
- Active Directory on Windows 2000:
  - Native mode
- Active Directory on:
  - Windows 2000 Native functional level

    -or-

  - Windows Server 2003 functional level
- Location of Time Source (DNS name).

ICM Requirements for Active Directory

- Authenticated users require read access to the contents of Active Directory.
- Microsoft Active Directory tools or ICM Domain Manager are the only supported tools for provisioning Active Directory.

  Note: Permissions are needed during setup for creation of Service Logon accounts.

- ICM servers can not be created in the ICM OU hierarchy.
- Only the ICM group policy template can be applied to OUs containing the ICM servers.
- Single-label DNS domain names (such as "ICM") are not supported when used with ICM/IPCC. Multi-part names such as ICM.org, ICM.net, ICM.com, or sales.ICM.org are acceptable.

  Note: For additional information, refer to: **Information about configuring Windows for domains with single-label DNS names** (http://support.microsoft.com/kb/300684/en-us)

No Active Directory schema changes are required. Authenticated users require read access to the contents of Active Directory.

ICM Requirements for Group Policy in Active Directory

Group Policy plays a pivotal role in Active Directory management and directly affects the function of distributed applications like ICM. This section is designed to explain Group Policy and define requirements to ensure proper functioning of your Cisco applications, primarily as it regards the ICM servers.

Group Policy Overview

Administrators can manage computers centrally through Active Directory 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 allowed actions for users and computers. It can create desktops that are tailored to users' job responsibilities and level of experience with computers. 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 ICM and the ICM servers ability to function. As such, it is necessary to control the OU structure for ICM components and ensure a standard is adhered to.

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 contained in a Group Policy object (GPO), which is in turn linked to Active Directory containers (such as sites, domains, or OUs). In this way, Group Policy settings are applied to the users and computers in the Active Directory containers. For additional information refer to: **Group Policy management and the Group Policy Management Console** (http://www.microsoft.com/windowsserver2003/gpmc/default.mspx#EOC).

ICM Requirements

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

ICM Server Requirements

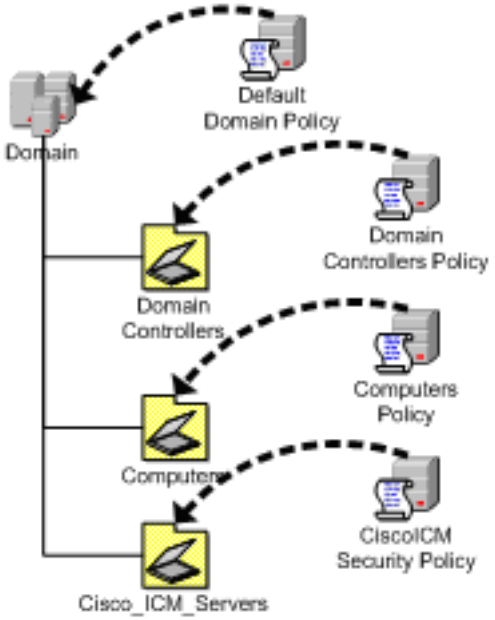
All ICM servers can be moved into a separate OU to ensure proper functioning of the ICM application and to improve security. The OU must be clearly identified as Cisco_ICM_Servers (or a similar clearly Identifiable name) and documented in accordance with your corporate policy.

Note: This OU must be created either at the same level as the computer's container or the Cisco_ICM Root OU.

You have the option of installing a Cisco customized security template file to the local machine while running the Cisco ICM/ IPCC setup or the System IPCC Installer applications. This .inf file is located in the Security Templates folder on the ICM CD and documented in the **Security Best Practices Guide for ICM and IPCC Enterprise & Hosted Editions, Release 7.0(0)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html). Add the provided security template using an existing Group Policy infrastructure as shown in the following diagram.

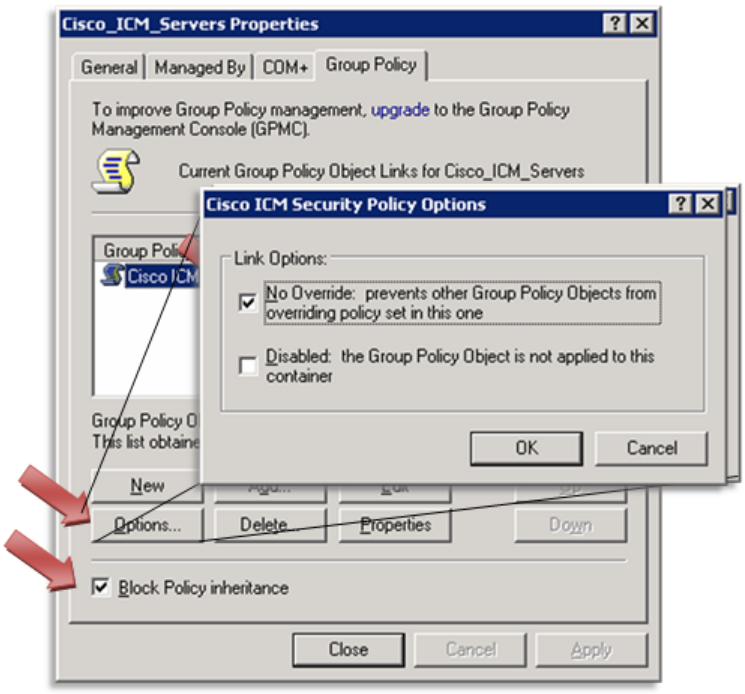
Note: If you are unfamiliar with Active Directory please engage your Domain Administrator to assist you with Group Policy deployments.

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 **Block Policy inheritance**. You must also prevent improper policies from being used on the machines directly. This can be accomplished by clicking **Options** and checking **No Override**.

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

Administrative Workstation (AW) Requirements

If you are setting up an Administrative Workstation (AW) in a domain other than that of the Central Controller domain, perform the following to update the NAM ICM Active directory OU environment so that the AW is pointing at the CICM Central Controller.

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

To ensure the permissions are set up correctly:

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

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

2. Run the Domain Manager on an 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 as 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 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:

- Active Directory Integrated Zone for both forward and reverse lookup zones.
- Enterprise level Standard Secondary Zone for the Enterprise ICM/IPCC Child Domain model or the Hosted ICM/IPCC Domain model.
- Add all additional addresses manually (high, privates, private highs, etc.) to the forward lookup zone in DNS along with associated PTR records.
- 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.

Global Catalog Requirements

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

Supported Topologies

Introduction

The following Active Directory topologies are supported for Enterprise ICM/IPCC systems:

- Single Domain
  - ICM/IPCC in the Corporate domain

  - ICM/IPCC in a child domain of the Corporate domain
  - ICM/IPCC as a standalone domain
  - ICM/IPCC as a tree root

The following Active Directory topologies are supported for Hosted ICM/IPCC 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

Using the following example(s), make a determination as to what your domain structure will look like prior to installing the Domain Controller.

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

This information is intended for the individuals responsible for:

- Configuring the Active Directory Domain/Forest Topologies
- Staging new deployments of Cisco Enterprise ICM or Hosted NAM/CICM on Windows 2000/2003

The administrators of your ICM system must be trained on the use and functions of:

- ICM
- Windows 2000/2003 Servers
- Active Directory
- DNS

This section does not provide detailed Enterprise ICM, Hosted NAM/CICM or Windows 2003 specific information. This information can be found elsewhere in specific documentation from Cisco and/or Microsoft. Individuals utilizing this document must have at least intermediate knowledge and experience with Active Directory.

The ability to integrate ICM into existing infrastructures is one of the premises of ICM Release 7.0. The impact the unique environments in these existing infrastructures have on ICM can be mitigated with minor adjustments in the support schema.

The initial release of Cisco Enterprise ICM version 7.0(0) 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 Cisco Enterprise ICM are specified in detail.

A forest is a collection of Active Directory domains that provide a namespace and control boundary within Active Directory. Multiple forests means two or more forests in a given environment that share resources through manually created trust relationships.

Multiple Forests Are No Longer Supported

After careful review, the position of Cisco Systems, Inc. is that it is necessary to constrain the deployment scenarios and ensure customers use only single forest topologies. Multiple forest topologies (in regards to ICM) are not supported. All 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 recommended solution will simplify, or limit, the exposure to topology based deployment problems.

Problems using multiple forest:

- In lab environments, it was found that the use of multiple forests may contribute to the following problems:
  - It could take a considerable amount of time to replicate the user account created
  - Startup and configuration operations could take excessive time during installation and subsequent startups
  - The inability for ICM components to connect to each other and/or network resources
  - Some multiple forest problems are expensive to resolve, while others can not be resolved for real time environments such as ICM/IPCC
- Microsoft's best practices document recommends using the single forest model by stating:
  - *"…you should strive for a single forest design for your organization,"*
  - *"merge … autonomous divisions into a single forest to reduce the cost of designing and operating their own Active Directory or to facilitate resource sharing."*
  - *"A single forest is ideal… it represents the least possible administrative overhead"*

  For additional information refer to: **Best Practice Active Directory Design for Managing Windows Networks** (http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/plan/bpaddsgn.mspx)

- Multiple forests:
  - Have a very large deployment footprint
  - Are very complex to deploy, especially as the number of forests increases
  - Are expensive to administer and prone to configuration errors that are difficult to troubleshoot
  - Have high support costs
  - Correctly setting up and maintaining multiple forest environments, and then forcing applications such as ICM to work around the inherent security of these environments is intrinsically complex
  - Much ICM functionality is directly dependant on the links designed as the fail-safe points for forest integrity
- This guide defines the supported scenarios, and discusses deployment variations. Topologies not in a supported format must procure customer obtained AD expertise.
- Cisco Systems, Inc. *strongly* recommends the procurement of Microsoft Support Services to mitigate any Microsoft specific issues that may arise, as domain topologies vary.

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

Single Forest, single tree, single domain

- Benefits
  - Simplest implementation
  - Most 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 implementation 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. Active Directory changes this. It has been simplified and its ability to span multiple domains in a single forest has been improved.

Choosing the Single Domain Model

The single domain model is ideal for many ICM deployments. A single domain structure possesses multiple advantages, the first and foremost being simplicity. The simplest design often works the best. Adding unnecessary complexity to a system architecture introduces potential risk and makes troubleshooting these systems more difficult. Consequently, consolidating complex domain structures such as those found in NT 4.0 into a simpler single Active Directory 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, Active Directory and the single domain model allow for a high level of administrative control and the ability to delegate tasks to lower sets of administrators is available.

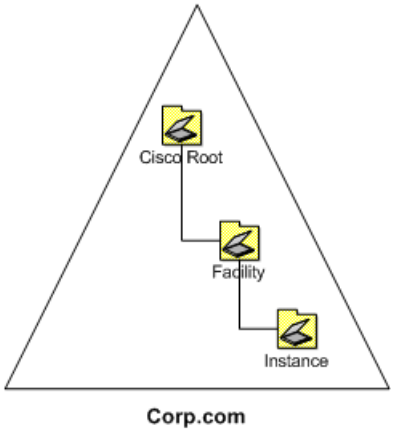
ICM benefits from this design because Active Directory traversal queries are limited to the single domain. As a result, request processing time is significantly reduced. Active Directory controls access and provides security. This dramatically improves the overall performance of ICM.

Designing a Single Domain Topology

Design is the single most important aspect of any Active Directory deployment. It is suggested that you follow the Microsoft Planning guide to ensure a smooth transition.

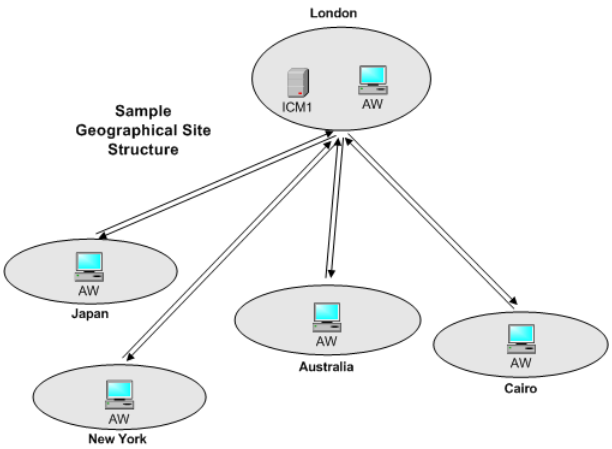
Delegation of password-change control and other local administrative functions can be granted to individuals in each specific geographical OU. This provides administrators permissions specific only for resources within their own group but maintains central administrative control in the root OU. A detailed discussion of organizational unit design is covered in About Organizational Units (page 39).

Figure 3: Sample Single Domain Layout



Several Active Directory 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

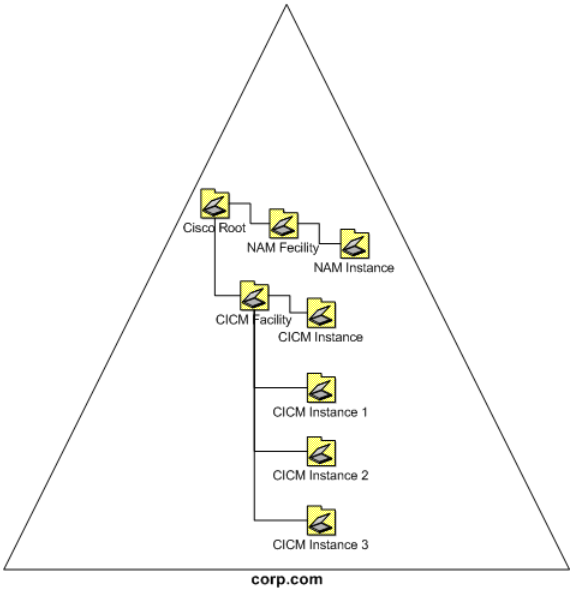


Creating separate sites helps throttle replication traffic and reduces the load placed on the WAN links between the sites. For more details about site links and replication, refer to **How Active Director Replication Topology Works** (http://technet2.microsoft.com/WindowsServer/f/?en/library/1f3bb1c1-ba8a-4b4e-9f23-f240566e3d661033.mspx)

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, significantly reducing the reasons for organizations use multiple domains.

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

Figure 5: Hosted OU Structure for Single Domains



This allows Active Directory to manage access utilizing Group Policies, Kerberos, and ACLs. This greatly simplifies administrative overhead, and provides an increased ROI for the entire organization.

Single Tree Multiple Child Domains

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

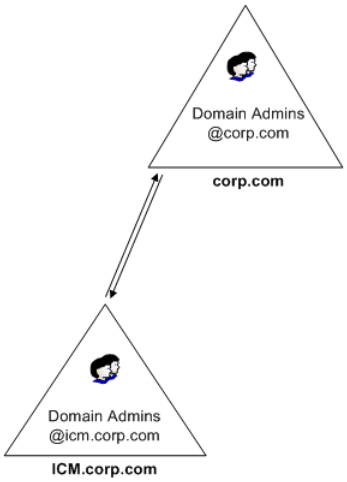
By default, two-way transitive trusts exist between the child domain and the parent domain in Active Directory. However, this does not mean that resource access is automatically granted to members of other domains. For example, a user in the child domain is not automatically granted any rights in the 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 may become necessary if the need for decentralized administration exists within your infrastructure. If your organization requires 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 may be useful. Each domain acts as a security boundary for most types of activity and can be set up to disallow administration from escaping the boundaries of the domains. 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 Active Directory because you gain more AD advantages (for example: centralized management, a simpler deployment model, user and group management is simplified, and enhanced operability). The following figure demonstrates the boundary as it

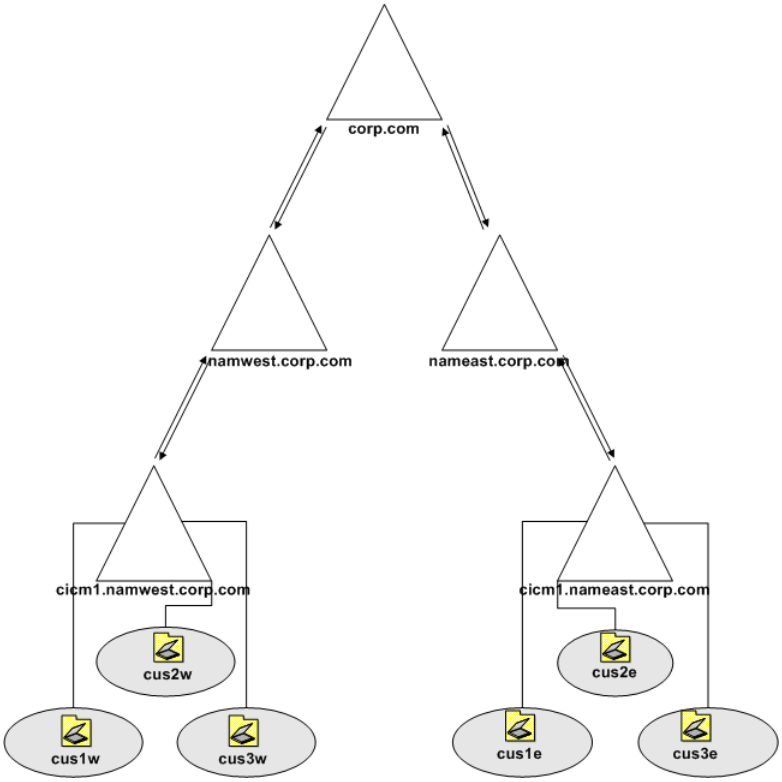
exists by default in this topology. In order to give the user access to resources in the parent domain, the rights must be assigned.

Figure 6: Active Directory Boundaries



If there are geographic limitations (for example, if extremely slow or unreliable links), segment the user population into separate groups. This helps to limit replication activity between domains, and also makes it easier to provide support during working hours in distant time zones. Be aware that slow links by themselves do not necessitate the creation of multiple domains, as Active Directory 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 the North American administrator.

Figure 7: Regional Domains

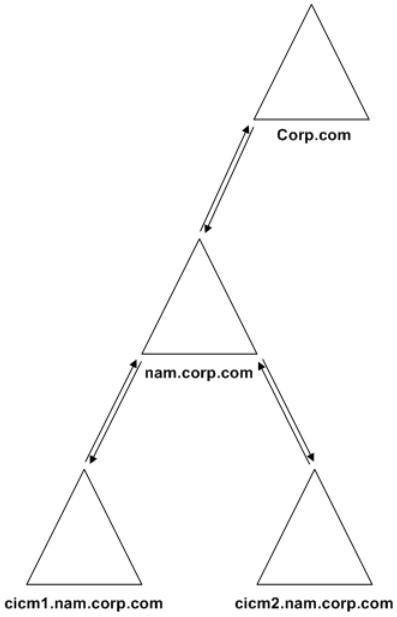


This model allows each region to perform its own administration, creating an easily distributed, and extremely flexible, topology. This allows for a very wide support base with immediate incident response. It also keeps the deployment clean and logical.

For ICM, the addition of multiple child domains retains some of the old familiarity of NT4 topologies but gives an ease of delegation. For some service providers this topology would be appealing because the logical boundary of the domains can provide a clear delineation in the NAM/CICM relationship, while maintaining AD functionality.

This topology provides a contiguous namespace. That means that the DNS domain names are related by the naming convention. For additional information refer to Domain Name System (DNS) (page 34).

Figure 8: Contiguous Namespace



The flexibility in this model is very apparent, however it is important to be familiar with your organization's requirements for a distributed, collaborative application such as 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 Active Directory topology as 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 Active Directory 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.

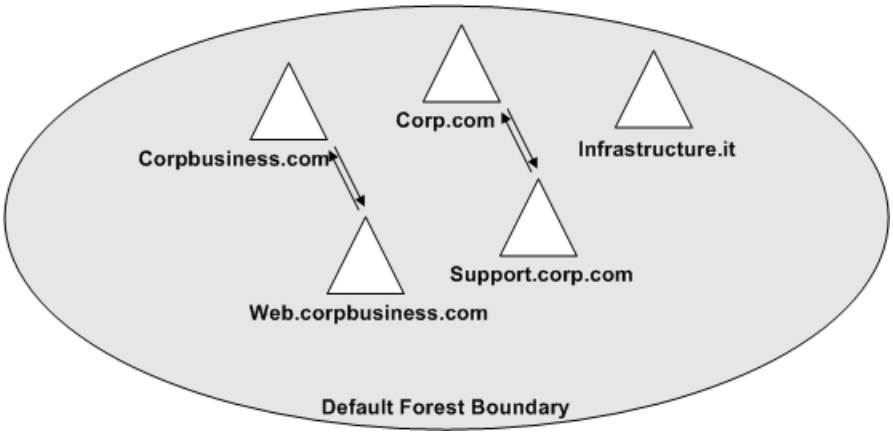
Any domains added to the forest that maintain a unique namespace form a new tree in the forest. An Active Directory forest can consist of one or many trees in a single forest. In some instances, multiple trees are required so that a company can meet its business requirements.

Multiple Trees in a Single Forest Model

Let us say that your organization has decided to move to an Active Directory environment and, in addition, wants to use an external namespace for its design. Your current environment uses multiple DNS namespaces and needs to integrate them into the same design. Contrary to popular misconception, the external namespaces can be integrated into a single AD forest. This is accomplished through the use of multiple trees existing in a single forest.

One of the most misunderstood characteristics of Active Directory is the difference between a contiguous forest and a contiguous DNS namespace. Multiple DNS namespaces can be integrated into a single Active Directory 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

When planning a domain structure, simplicity is always best. 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. Again, only a thorough assessment of the business will determine whether this is necessary. When considering a multiple tree structure, keep the following requirements in mind.

DNS Names

If a business is comprised 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 Active Directory structure based on a new namespace that is contiguous throughout your organization. Consolidating your Active Directory under this single domain simplifies the logical structure of your environment while keeping your DNS namespaces separate from Active Directory.

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 ICM in a corporate environment. As other considerations may 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(s):

- The domain administrator of the root domain has complete power over the Active Directory 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 very 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. Active Directory, however, provides layers of actual security. These layers are all customizable, and can be implemented 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. ICM is a very robust application and may 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 Active Directory 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 ICM. The procedures detailed in this guide delineate the best possible methods of deploying and maintaining ICM. Please 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)

Active Directory (AD) is integrated with the Domain Name System (DNS) in the follow ways:

- AD and DNS have the same hierarchical structure.

  Although separate and implemented 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 ?) and netdiag.exe (page ?) to troubleshoot client computers that cannot locate a domain controller. These tools can help determine both server and client DNS misconfigurations.

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.

- Active Directory 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 MS best practices for AD to create lookup zones and configuring DNS servers.

- Select **Active Directory 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.
- ICM servers must have a primary DNS server in the same Active Directory site where they reside.

How to Install and Configure DNS on an Additional Domain Controller

Step 1 Click **Settings > Control Panel > Add/Remove Programs**.

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

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

Step 4 Browse to the Windows 2003 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, then select **Properties**.

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

For an Enterprise ICM 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 Active Directory Sites

On ICM Root Domain Controller:

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

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

a. For a geographically separated DC, right-click on **Sites**.

b. Select **New Site**.

c. Enter the site name of the additional domain controller as per the ICM System Diagram.

Step 3 Create subnets for each DC site:

a. Right-click on 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**. Make sure 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 ICM System Diagram and the ICM/IPCC System Design Specification for your implementation:

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 ICM System Diagram and the ICM/IPCC System Design Specification for your implementation.

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 may 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: **`W32tm -s <DNS Name of Time Source>`**

How to Change Domain Controllers to Native Mode

Active Directory on Windows 2000 requires Native mode.

Active Directory on Windows 2003 requires either Windows 2000 Native functional level or Windows Server 2003 functional level.

On Enterprise, NAM, CICM, and Customer AW Domains Controllers:

Step 1 Open Active Directory Domains and Trusts.

Step 2 Right-click the domain node for the domain you want to administer and then click **Properties**.

Step 3 In the **General** tab, select the appropriate mode.

How to Configure DNS Server on Forest Root Domain Controller

Step 1 Click **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 receive 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 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 Active Directory 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 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 screen, 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 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 ICM 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 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 ICM using hostname resolution in the Forward Lookup Zone.

Chapter 3

About Organizational Units

What is an Organizational Unit (OU)

An Organizational Unit (OU) is a container in the Active Directory 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 implementing security groups (page 42).

Permission to create an OU is controlled by Active Directory. 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.

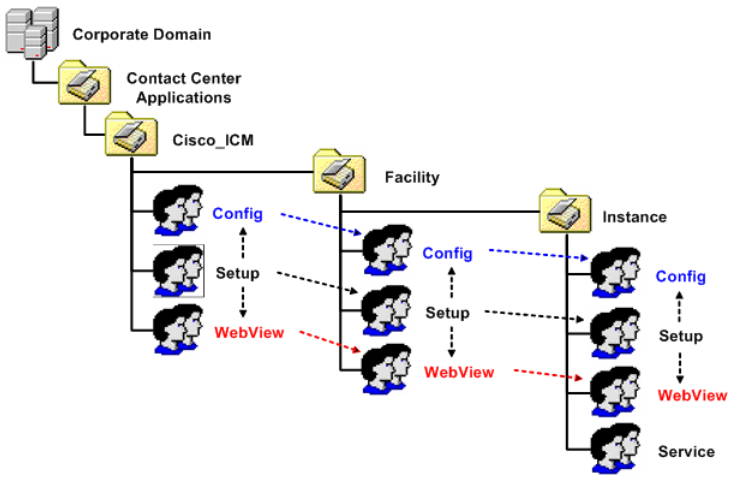
Organizational Unit Hierarchies

How are Organizational Units Organized?

ICM uses the following hierarchy of Organizational Units:

- 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 the ICM requires are created in OUs on the domain. The OU hierarchy created by the 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:

- ICM 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 ICM in the corporate domain is now a supported environment.

What is the Cisco Root Organizational Unit?

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 Organizational Unit?

- ICM software always uses a Cisco Root OU named "Cisco_ICM".
- The OU containing all ICM created domain resources.
- Defines permissions for all ICM Instances.
- Only one Cisco Root OU can exist in each domain

Note:

- For information on how to move the Cisco Root OU, refer to Appendix B (page 169).

- See How to Create (Add) the Cisco Root Organizational Unit (page 99).

What are Facility Organizational Units?

A Facility Organizational Unit 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 ICM instances. For example, you may have different Facility OUs for Lab and Production ICM instances; or in a ICM Hosted deployment, you may 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 Organizational Units?

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 ICM Instance Organizational Units?

An ICM Instance is a single installation of ICM software. It consists of several components (including the CallRouter, the Logger, Administrative Workstations, and Peripheral Gateways), some of which may be duplexed.

An Instance Organizational Unit:

- Is the representation of an ICM instance.
  - Each 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

Security Groups and Organizational Units

Each Organizational Unit 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.

Note: If you create new user accounts in the old ICM/IPCC 5.0 or ICM/IPCC 6.0 system after the new ICM/IPCC 7.0 instance OUs were created, these accounts will not be valid in the new ICM/IPCC 7.0 system.

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. Refer to Microsoft, 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 should 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 ICM software.

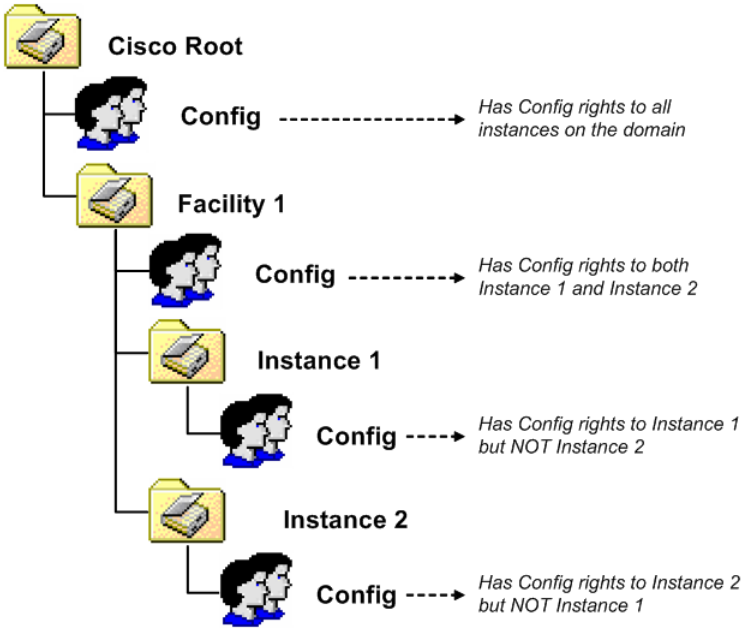
For each security group, you add domain users (page 106), who are granted privileges to the functions controlled by that security group. Users are given membership in the security groups to enable permission to the application. These users can be created in other OUs in this domain, or in any trusted domain.

Note: The user who creates the Cisco Root Organizational Unit automatically becomes a member of the Setup Security Group for the Cisco Root OU. In effect, this user is granted privileges to all 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 Active Directory 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 Active Directory. 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 ICM software 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 Active Directory operations using the User List tool (provided they have Active Directory 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 AW DB.

  Note: For AW DBs only. Not for Logger DBs and HDSs.

- IPCC Web Administration

  Note: Config Security Group members also have access to IPCC Web Administration in the System IPCC model.

What is the WebView Security Group?

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 Setup
- Configuration Manager
- WebView

Users who are members of the Setup Security Group can:

- Run Setup to install ICM instances and software components.
- Add users to security groups
- Create service accounts.

  Note: Refer to the Service Account Manager (page 67) chapter for additional information.
- Manage OUs, groups, users, and permissions.
- Have access to the Web Administration tool in the System IPCC deployment model.
- Can run the System IPCC Installer/upgrade.

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

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

Figure 12: Setup Security Group Permissions

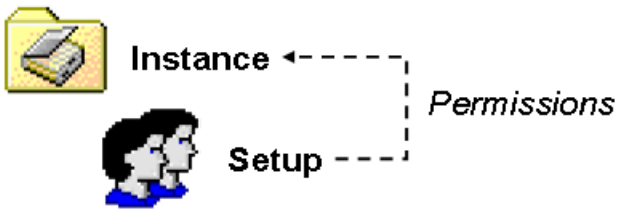


Table 2: Setup Security Group Active Directory Permissions

Tasks	OU Hierarchy Level
Delete Subtree	Child objects only
Modify Permissions	Child objects only
Create/Delete OU Objects	This object and all child objects

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

How Do Organizational Unit Hierarchies and Security Relate?

Organizational units are nested as described above, with the Root OU containing Facility OUs (page 41), which contain Instance OUs (page 41). In the case of the 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

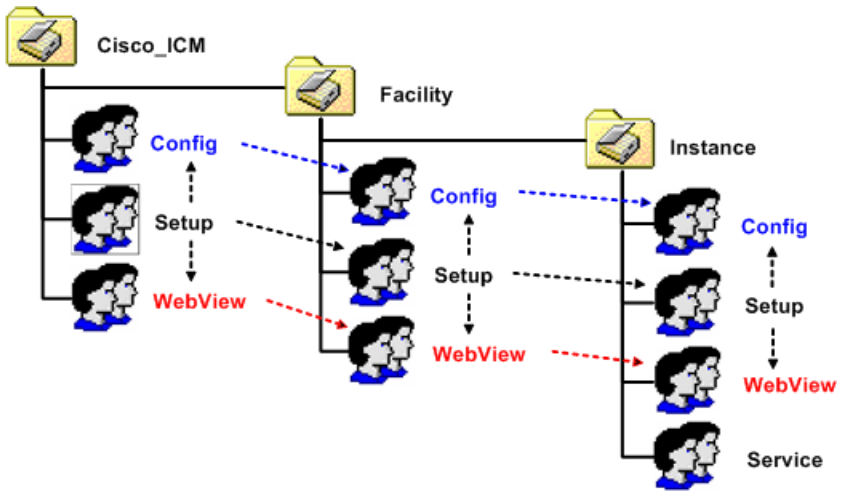
- Permissions/access rights in the Root WebView security group.

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

  – Facility WebView group

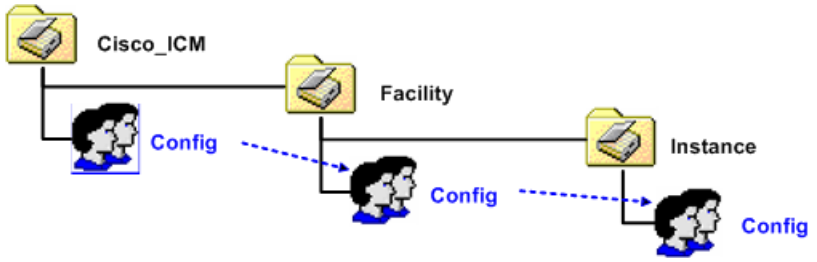
  – Instance WebView group

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



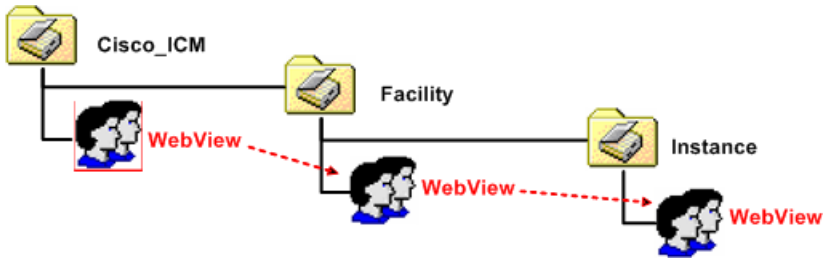
Making a user a member of the Root Config security group grants permissions/access rights in that security group as well as the Facility and the Instance Config security groups.

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



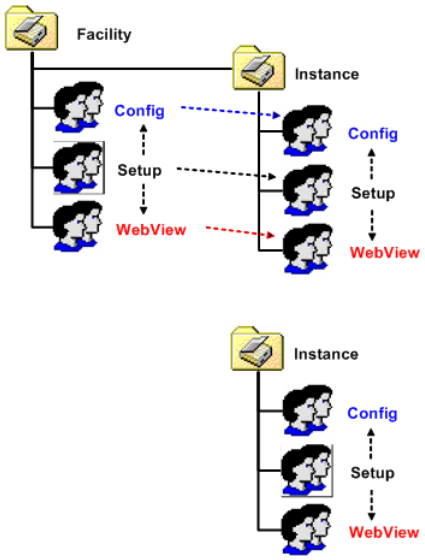
Members of a Facility security group have all the permissions/access rights granted to Instance OUs nested within that Facility. However, members of those Instance OU's security groups do not necessarily have the permissions/access rights granted to their containing Facility OU.

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.

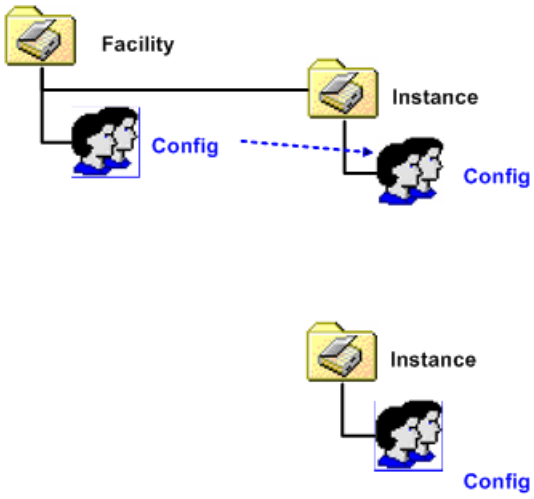
A member of the Instance Setup security group is granted permissions/access rights only to the Instance level security groups (Setup, Config, and WebView).

Figure 16: Faciliy/Instance Setup Security Group Member Permissions/Access Rights



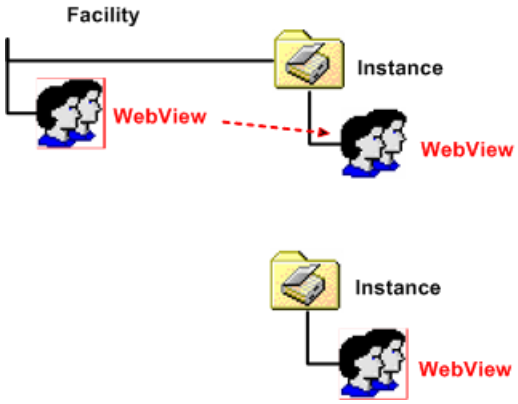
In the following illustrations, a member the Facility Config security group has permissions/access rights to that security group and the Instance Config security group. However, a member of the Instance Config security group only has permissions/access rights to that security group.

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 Organizational Units (page 41). It exists at the Instance level only. The Service Security Group controls access between ICM 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
- AW DB
- HDS
- WebView DB
- Outbound Option DB

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

- Logger
- the Distributor

- WebView (Jaguar)
- Tomcat

  Note: For Web Re-skilling and the System IPCC Web Administration tool.

Service Logon Accounts

- Passwords do not have to be randomly generated, they can be provided and saved in Active Directory, 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 Domain Conversion Tool was used to migrate ICM users from the NT domain architecture to the AD domain architecture and placed the users in the appropriate ICM security groups when migrating from ICM 5.0(0) or ICM 6.0(0) to ICM 7.0(0). Due to the Active Directory design change in later versions of ICM, the Domain Conversion Tool can no longer be used. The User Migration Tool (UMT) replaces the Domain Conversion Tool for ICM versions 7.5(1) and higher.

The User Migration Tool (UMT):

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

  It migrates only ICM Active Directory user accounts (config/setup/webview users and supervisors) and can be used during Technology Refresh (TR) upgrade to a new domain, or if the 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 an ICM Logger system, or on System IPCC Central Controllers.

  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; and, as of Release 7.5, it is installed by ICM Setup.

- Performs migration of ICM users from:
  - One domain to another.
  - One ICM facility to another in the same domain.
  - One ICM facility in one domain to another ICM facility in another domain.
- Serves the following purposes:
  - All ICM users retrieved from the ICM Logger database are migrated from the source to the target Active Directory domain.
  - All AD user accounts that are directly a member of ICM Instance security groups are migrated from the source to the target domain.
  - The user information table in the ICM Logger database in the target server is updated to point to the user accounts created in the target Active Directory domain.
  - in the target domain, ICM security group membership is updated for the users belonging to an external domain.

This chapter contains the following topics:

User Migration Tool Pre-requisites

The following pre-requisites must be met prior to running the User Migration Tool:

- in the target domain, the ICM organizational unit (OU) hierarchy must have been laid out and the ICM security groups created for each ICM instance, prior to running the User Migration Tool. This must be done by running the ICM Domain Manager or the IPCC Machine Initializer tool (as applicable).
- Import the exported ICM registry from the source Logger system to the target Logger system.
- The ICM 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 ICM users from an external domain that are a member of the ICM security groups at the source domain, then the trust relationship(s) need to be established between the target domain and the external domain corresponding to the trust relationship(s) that existed between the source domain and the external domain. This can be done using "Active Directory Domains and Trusts" tool.
- If the 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 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, ICM facility.
- Adds the user account in the corresponding ICM security groups in the target domain.
- Updates the ICM Logger database with the Globally Unique Identifier (GUID) of the user account from the target domain.
- Migrates the ICM security group membership of Foreign Security Principals to the new domain.
- Migrates the 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 ICM Facility OU in a target domain.
- Moving machines with pre-installed ICM components to a target domain.
- Moving machines with pre-installed ICM components to a different ICM Facility OU in the target domain.
- Moving machines with pre-installed ICM components to a target domain and performing a Common Ground upgrade.
- Moving machines with pre-installed ICM components to a different ICM Facility OU in the target domain and performing a Common Ground upgrade.
- Migration of user accounts to a different ICM Facility OU in the same domain.

Internationalization (I18n) and Localization (L10n) Considerations

In the localized version of ICM, you can store ICM user names in non-Western European characters (but not in Unicode) in the 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 ICM systems.

Performance Considerations

The larger the number of users being exported or imported is, 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 ICM 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 ICM 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.

User Migration Steps

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 User Name and UserGroupID) and the security group membership from the source Active Directory 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:

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

Step 2 On the ICM 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 ICM registry.

c. Verify the log file for any errors.

Target Server in the Target Domain

Perform the following:

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

Step 2 If the domain name needs changing when in a Common Ground upgrade scenario, refer to Changing the Domain Name Using ICM Setup (page 56) or Changing the Domain Name Using the System IPCC Machine Initializer (page 57) as applicable.

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 ICM registry exported from the source domain.

Step 4 Run the User Migration Tool in Import mode for each ICM 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 ICM services if they were previously running.

Changing the Domain Name Using ICM Setup

To change the Domain for an ICM system you must run ICM Setup.exe from the media.

Note: You can not perform this procedure from a local copy of ICM Setup.exe.

Perform the following to change the Domain and the Facility for an ICM system:

Step 1 Run ICM Setup.exe from the media.

Step 2 Select the Instance to be modified, then click **Edit**.

Step 3 Select the new Domain name.

Step 4 Select the new Facility name.

The Edit Instance dialog displays the new Domain and the new Facility. The Instance filed automatically displays the correct Instance and the dialog states that a matching Instance was found in the selected Facility.

Step 5 Click **OK**.

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.

Changing the Facility Name Using the System IPCC Machine Initializer

To change the Facility for a System IPCC system you must run the System IPCC Initializer.

Perform the following to change the Facility for a System IPCC system:

Step 1 Run the System IPCC Initializer.

When run, it selects the correct Domain, then displays a dialog allowing you to select an existing, or create a new Facility.

Step 2 Select/create the new Facility.

Once the Facility has been provided, the correct Instance is automatically displayed.

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 ICM instance specific parameters such as the ICM Facility name, ICM Instance name, and ICM 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 Active Directory and the Logger database (if necessary).

  Note: Due to the need to replicate new user accounts and Active Directory 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 arguements or the **/help** arguement. This displays the command line syntax, and all modes and parameters are displayed.

Refer to the following sections for additional information concerning the Export (page 59), Import (page 60), and Verify (page 61) 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 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 that the user account is added to

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 user name 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 log in using the WebView login interface, the log on fails. This is because the Active Directory 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 log-in using the Active Directory account. A prompt appears asking to change the password. Provide a new password, then use the WebView interface to log-in.

Export Mode

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

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

- the ICM Facility and Instance name
- the ICM Logger database name
- the AD user account name and the domain name
- the ICM security group(s) 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, refer to Content Parameter Descriptions (page 62).
- 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(s), to the target domain; and then updates the ICM database.

In the Import mode, the User Migration Tool gets the user name from the input file, and searches for a user account in the Active Directory, and creates one if not found. The user account is created in the Instance Organizational Unit 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.

The User Migration Tool adds the user account to the ICM security group(s) based on the information from the exported file. The ICM Logger database is then updated with the user account's Active Directory Globally Unique Identifier (GUID) and the target domain name.

The following information is imported from the exported file:

- the ICM Logger database name
- the 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 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 Active Directory, and creates one if not found. The user account is created in the Instance Organizational Unit 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, refer to Content Parameter Descriptions (page 62).
- 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 Active Directory and ICM database migration done during Import.

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

- Verifies the existence of the user account in Active Directory.

- Verifies the membership of the user in the ICM security groups.
- Validates the user's Active Directory Globally Unique Identifier (GUID) and the domain name with the information in the ICM Logger database. (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, refer to Content Parameter Descriptions (page 62).
- 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 ICM Logger database name.
/Facility	The ICM Instance facility name. When it is optionally specified during the import or verify mode, the User Migration Tool migrates users to a different ICM facility.
/Instance	The 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 user's are members of ICM security group(s). The User Migration Tool performs migration of 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 ICM security group membership in the current domain

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

1. Enter user name on domain <*DomainName*>.
2. Enter <*password*>.

For users of a trusted domain, the ICM security group membership is migrated if, and only if, the user is a direct member of the 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 ICM security group membership of *ExtUser1* is migrated, only the Cisco_ICM_Setup and the Cisco_ICM_Config security groups are picked. The Cisco_ICM_WebView security group is not picked.

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

In order to migrate 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 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 case, error message, 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 an 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 ICM 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 ICM 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 ICM 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 ICM Organizational Units is missing in the current domain.	Run Domain Manager tool and create ICM security groups, and re-run the User Migration Tool.

Error Message	Solution
One or more of the ICM security groups do(es) not exist in the current domain.	Run the Domain Manager tool and create the ICM security groups, then re-run the User Migration Tool.
The logged-in user has insufficient credentials.	The logged-in user must be a Local Administrator. The logged-in user must be a member of the Domain Users group in the current domain. For import, the logged-in user must be a member of Cisco_ICM_Setup security group.
The Logger database is corrupted.	Fix the Logger database and re-run the User Migration Tool.
The system is either running stand-alone, or in a workgroup.	The User Migration Tool must be run on a system that is in a domain.
Mismatch of version between the User Migration Tool and the exported file.	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 ICM/IPCC 7.5(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 ICM facility and domain that it was exported from. It must be run under a different 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

ICM and Contact Center Enterprise services, such as Logger or Distributor, execute under the context of a domain user account commonly known as a service account. ICM Setup and System IPCC Installer create these service accounts in the Active Directory (AD) domain and associate them with the corresponding service on the ICM server.

The Service Account Manager is invoked by ICM Setup or System IPCC Installer when you choose to manipulate the default service account creation process.

The Service Account Manager decouples the service account management from ICM Setup or System IPCC Installer. This provides you with the needed flexibility to:

- either create a new service account or choose one created prior to ICM Setup or System IPCC Installer.
- enter your own password or let the ICM application generate one for you.

  Note: If passwords are changed using an application other than SAM, SAM cannot detect the changes.

- allow you (when applicable) to choose whether or not to update the account in AD and use existing AD accounts as ICM service accounts.
- allow you to fix service account group membership issues (such as modifying ICM service account passwords) without recreating accounts or without re-running ICM Setup or System IPCC Installer.

The Service Account Manager is called by ICM Setup or System IPCC Installer to when either Creating Service accounts or Use existing accounts checkboxes is selected. When Creating Service Accounts checkbox is selected, the Setup/Installer silently calls SAM to generated Account and password. When the Use existing account checkbox is selected, Setup/Installer calls SAM and the graphical interface.

The Service Account Manager provides an additional functionality via its command line interface to set service account memberships for CICR replication in a NAM/CICM deployment.

You have the option to re-run the Service Account Manager post ICM/System IPCC installion to modify the 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:

- Distributor
- LoggerA
- LoggerB
- Tomcat
- Jaguar

This chapter contains the following topics:

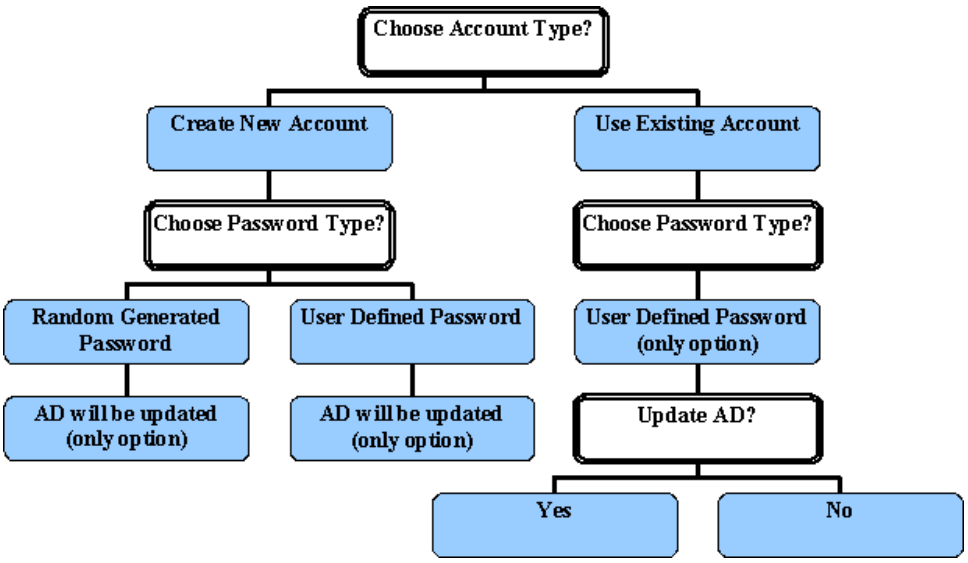
Managing Service Accounts

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

1. create new accounts with random passwords, like the current ICM Setup and System IPCC Installer.
2. use existing AD accounts as ICM service accounts.
3. Provide an interface to modify ICM service account passwords.

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

Figure 19: Service Account Manager Application Workflow



Integration with ICM Setup and System IPCC Installer and Upgrade

Currently ICM Setup and System IPCC Installer create a service account in AD for the following ICM services and then associate these services with their respective service accounts:

- Distributor
- Logger
- Tomcat
- Jaguar

ICM Setup and System IPCC Installer are modified to create the above listed services using the NetworkService account, a Windows predefined local account (other services such as Router and PG are not modified).

Note: You must have Microsoft .NET Framework 3.5 installed on all systems you intend to install the Service Account Manager on. This is automaticallt installed by ICM Setup or the System IPCC Installer.

ICM Setup and System IPCC Installer use the Service Account Manager to create the service accounts. You can choose to either let Setup/Installer manage the service account creation process, or take control over the service account management process.

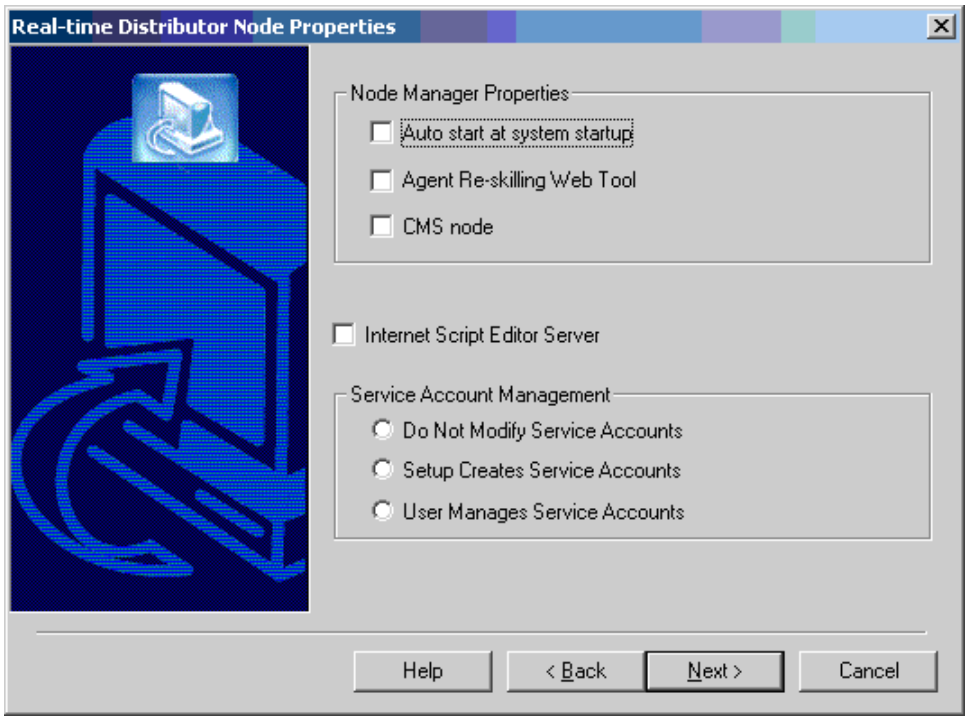
Interaction with ICM Setup

.

The following ICM Setup dialogs have been modified (the **Recreate Service Account** checkbox has been removed and the **Service Account Management** section has been added) to gather service account management input:

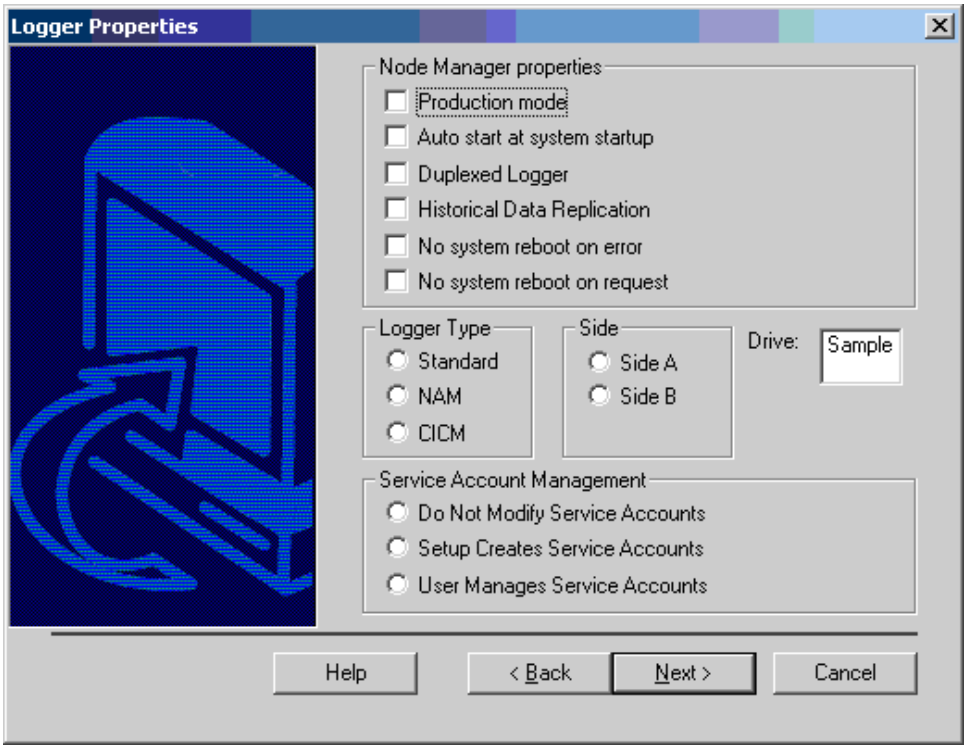
- Distributor

Figure 20: Distibutor Setup Dialog



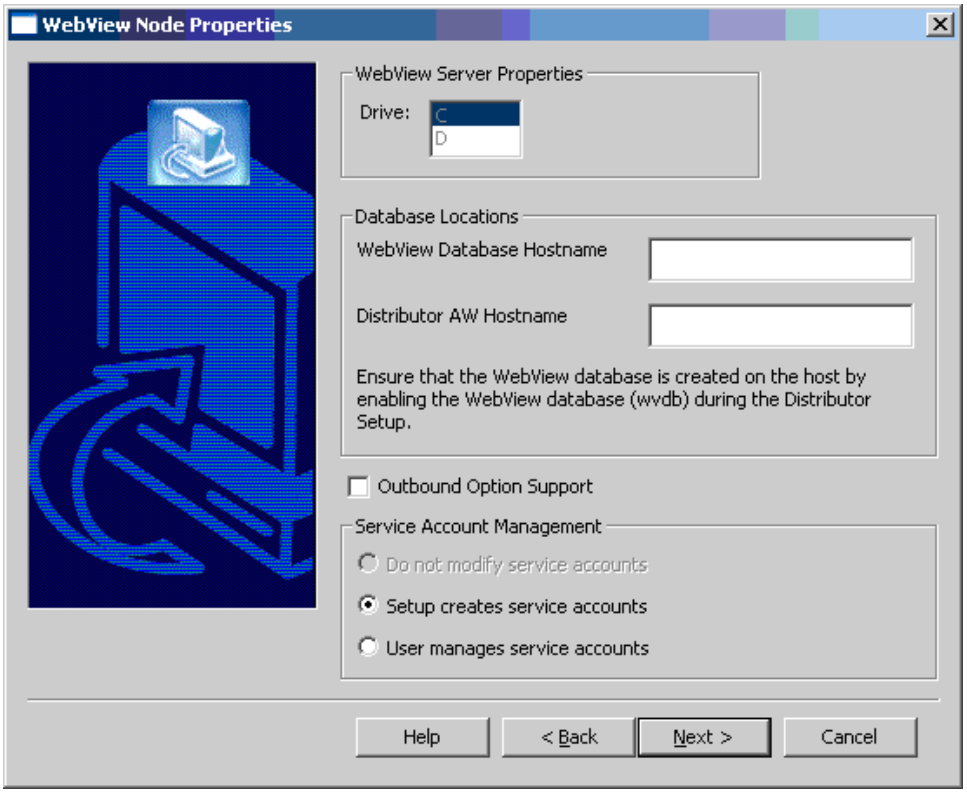
- Logger

Figure 21: Logger Setup Dialog



- WebView

Figure 22: WebView Setup Dialog



The **Service Account Management** section contains three radio buttons:

- Do not modify service accounts
- Setup creates service accounts
- User manages service accounts

Additional information concerning the three new radio buttons can be found in the following sections.

Fresh Installation using ICM Setup

During a fresh installation of the Logger, Distributor, and/or WebView component(s), **Do not modify service accounts** is grayed out and **Setup creates service accounts** is selected by default. You must choose between **Setup creates service accounts** and **User manages service accounts**. When you click **Next**, Setup notes your selection. Setup then creates the service(s) using the NetworkService account. After creating the service(s), Setup invokes the Service Account Manager as follows:

- If you selected **Setup creates service accounts**, Setup invokes the Service Account Manager silently, without bringing up the Service Account Manager user interface.
- If you selected **User manages service accounts**, Setup invokes the Service Account Manager to allow you to take control of setting up the service account name and password.

Editing Component using ICM Setup

If you edit any of the three components listed above, **Do not modify service accounts** is enabled and selected by default.

Upgrade using ICM Setup

During an upgrade, once **Upgrade All** is selected, there is no other user interface. You have no options regarding service account creation. ICM Setup uses the following logic to decide if Service Account Manager needs to be invoked on not:

- *Common Ground*

  If the services already exist, ICM upgrade does not modify the service accounts.

- *Technology Refresh*

  ICM Upgrade invokes Service Account Manager to create the service accounts.

Interaction with the System IPCC Installer

Fresh Installation of System IPCC

Service Account Management has been added to the System IPCC Installer. It has the following two radio buttons:

- Installer Creates Service Accounts
- User manages service accounts

Similar to ICM Setup, the default selection for a new installation is **Installer Creates Service Accounts**. When you choose between the two, the Installer takes note of your selection, then acts on it later. The Installer lays down the files, updates the registries, and creates the Distributor, Logger, WebView, and Tomcat services using the NetworkServices account. The Installer then calls the IPCC Machine Initializer to create the ICM OU, the facility and the instance OU.

The Installer passes a new argument to the IPCC Machine Initializer indicating your choice of service account management. The IPCC Machine Initializer creates the OU and security groups. Then, if you selected **Installer Creates Service Accounts**, after the successful installation, the IPCC Machine Initializer tool invokes the Service Account Manager silently, without bringing up the Service Account Manager UI, and then passes control back to the System IPCC Installer.

If you selected **User manages service accounts**, after the successful installation, the IPCC Machine Initializer tool invokes the Service Account Manager for you to take control of setting up the service account name and password. Once the Service Account Manager is closed, the IPCC Machine Initializer tool passes the control back to the Installer.

If IPCC Machine Initializer tool fails then the Service Account Manager is not invoked, no matter what option is selected by you regarding service account creation. Fix the issue as reported by the IPCC Machine Initializer and then rerun the IPCC Machine Initializer in standalone mode. This, in turn, runs Service Account Manager as explained in the *Standalone Use of the IPCC Machine Initializer* section, following.

Upgrade of System IPCC

A new dialog panel has been added to the System IPCC Upgrade, with the following radio buttons:

- **Do not modify service accounts**
- **Setup creates service accounts**
- **User manages service accounts**

Similar to ICM Upgrade, the default selection is **Do not modify service accounts**.

When performing an System IPCC *Common Ground Upgrade*:

- System IPCC Upgrade does not invoke the IPCC Machine Initializer. Unlike System IPCC Installer, System IPCC Upgrade invokes the Service Account Manager directly when needed.
- If you select **Do not modify service accounts**, the service accounts are not recreated and Service Account Manager is not invoked.
- If you select **Installer Creates Service Accounts**, System IPCC upgrade invokes the Service Account Manager tool silently, without bringing up the Service Account Manager.
- If you select **User manages service accounts**, System IPCC Installer invokes the Service Account Manager tool, allowing you to take control of setting up the service account name and password. Once the tool is closed, System IPCC upgrade takes control and finishes the installation steps.

When performing an System IPCC *Technology Refresh Upgrade*:

- System IPCC Upgrade invokes the IPCC Machine Initializer. This is the only difference from the System IPCC Common Ground Upgrade above.

Standalone Use of the IPCC Machine Initializer

The IPCC Machine Initializer can be run as a standalone application to create or modify the facility OU. When creating/modifying the facility OU, the initializer invokes the Service Account Manager automatically. If the facility OU is changed, the service accounts must be recreated.

WebView configuration

Both ICM Setup and System IPCC Installer configure Jaguar service as a part of the installation. However, Jaguar service cannot be configured unless a service account is associated with it. Since service accounts are no longer created by Setup, Setup cannot configure the Jaguar service. Due to this, the Service Account Manger is responsible for configuring the Jaguar service after associating a service account with it.

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 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. While this functionality was originally taken care of by Setup, this function is now handled by the Service Account Manager.

AD Update Failures

If the Service Account Manager finds that a service is running, it first requests your permission, then 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 Setup/Installer, logs are written to the Setup/Installer log files only.

Set Service Account Memberships for CICR Replication

When upgrading the Cisco Intelligent Contact Manager (ICM) Hosted Edition to ICM 7.0 (or later) the CICR replication process (CRPL) does not have the proper rights and permissions in order to make configuration updates to the customer instances (CICM) and the slave NAM instance without manually configuring Active Directory.

This configuration entails adding the Provisioning NAMÃƒÂ¢Ã¢â€šÂ¬Ã¢â€ Â¢s logger service accounts to the service groups of the CICMs and the slave NAM. This way the Provisioning NAMÃƒÂ¢Ã¢â€šÂ¬Ã¢â€ Â¢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 (described at: 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 ICM Setup is executed, running the batch file follows 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 76) consisting of the following dialogs:
  - Main Dialog (page 76)
  - Edit Service Account Dialog (page 77)
- The Command Line Interface (page 83)

Service Account Manager Graphical User Interface Dialogs

A shortcut to the application can be found in Windows Start > Programs folder.

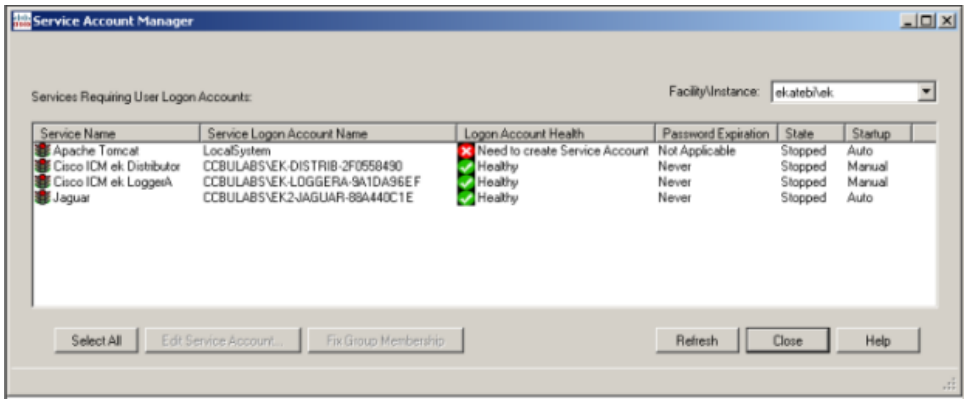
- For ICM, the shortcut is under ICM Administration.
- For System IPCC, the shortcut is under IPCC Administrator.

The Service Account Manager has two dialogs

- The Main dialog

  Lists all services with their account information.

  Figure 23: Main Service Account Manager Dialog

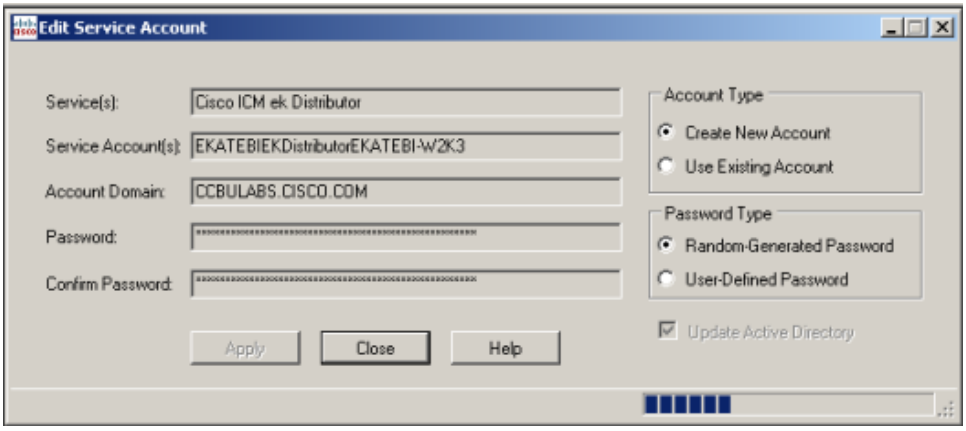


  Note: For additional information on all dialog fields and buttons refer to Service Account Manager - Main Dialog (page 76).

- The Edit Service Account dialog

  Used to edit the service account information.

Figure 24: Service Account Manager - Edit Service Account Dialog



Note: For additional information on all dialog fields and buttons refer to Service Account Manager - Edit Service Account Dialog (page 77).

Service Account Manager - Main Dialog

The Service Account Manager can be used as a standalone application as well as being invoked from ICM Setup and System IPCC Installer.

The Main Service Account Manager dialog 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** dropdown; and the **Select All**, **Edit Service Account**, **Fix Group Membership**, **Refresh**, **Close**, and **Help** buttons.

The following table provides a description for each of the fields and buttons for this dialog.

Field/Button/ Dropdown	Description
Service Name	A list of all relevant services. If there are no relevant services on the server, such as a Distributor, 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 ICM services and flags them as indicated below. • Green – Healthy Account: the service account state is normal. • Yellow

Field/Button/ Dropdown	Description
	– 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 ICM 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 may 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 ICM or System IPCC domain. • Account Disabled

Field/Button/ Dropdown	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 (Distributor only) – Distributors 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 Distributor. • Central Controller (sideA) Domain is not trusted or trust is not two-way (Distributor only) – There must be a two-way trust between the Central Controller and the Disributor. SAM detects the lack of the trust relationship and displays this message. SAM may detect this issue, but is unable to fix it. • Account not a member of LoggerA Domain Service Group (Distributor only) – If the Distributor is on a different domain than the Central Controller, it applies the Distributor's Domain Service Group to both itself and the Central Controller. • Central Controller (sideB) Domain name is unknown (Distributor only) – Distributors 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 Distributor. • Central Controller (sideB) Domain is not trusted or trust is not two-way (Distributor only) – There must be a two-way trust between the Central Controller and the Disributor. SAM detects the lack of the trust relationship and displays this message. SAM may detect this issue, but is unable to fix it.

Field/Button/ Dropdown	Description
	• Account not a member of LoggerB Domain Service Group (Distributor only) – If the Distributor is on a different domain than the Central Controller, it applies the Distributor'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 may 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 may 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** field to determine how long before the password expires. 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 to reattempt placing the account in the relevant local and domain security groups. **Note:** SAM health reporting may be inaccurate for the period of time while AD replication is in progress. The previous health state may be indicated during this time.

Field/Button/ Dropdown	Description
Password Expiration	Service account passwords created by the Service Account Manager are set to not 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 ICM 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	Dropdown displaying the "Facility/Instance" name. In case of multiple instances, the default "Facility/Instance" selected in the dropdown 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 Distributor, 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, the Service Account Manager prompts you to try to use the account recently created, as it keeps a 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.
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.
Close	Closes the Service Account Manager dialog.

Field/Button/ Dropdown	Description
Help	Select to access the online help for the Service Account Manager.

Service Account Manager - Edit Service Account Dialog

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 displays status messages as needed.

The following table provides a description for each of the fields, buttons, and checkboxes for this dialog.

Field/Button/Checkbox	Description
Services	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 there is 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. **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.

Field/Button/Checkbox	Description
Update Active Directory	**Checked** is the default, and only, option if you are creating a new account. **Note:** By checking this checkbox, you are actually making changes to the Active Directory domain and any changes to passwords will effect the password of the existing user. **Unchecked** is the default if using an existing account.
Apply	Click to apply any changes on this dialog.
Close	Click to close this dialog. Whenever this dialog is closed, the Service Account Manager determines if a valid domain account is associated with the service(s) 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 ICM or System IPCC Setup to silently create service accounts.

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

/Instance <InstanceName>

- The InstanceName argument specifies the 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

– Tomcat

– Jaguar

/Log <Path\LogFileName>

- The Log argument specifies the log file name and the path where the log is appended. Typically, ICM Setup and System IPCC 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.

Step 2 Click **Edit Service Account**.

The Edit Service Account dialog 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.

Step 2 Click **Edit Service Account**.

The Edit Service Account dialog 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 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 chooses to enter 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.

Step 2 Click **Edit Service Account**.

The Edit Service Account dialog 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 account(s) in the "Group Membership Missing" health state is (are) selected.

Step 1 Select the unhealthy account(s) displaying the "Group Membership Missing" state.

Step 2 Click **Fix Group Membership**.

If any of the selected account(s) is/are 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 account(s) in the groups, it provides the appropriate error.

Service Account Manager - How to ...

Chapter 6

About ICM Software Setup and Active Directory

How to Prepare to Work with Active Directory

Follow the steps below before beginning to work with Active Directory through the ICM Setup program.

Warning: The Domain Administrator must begin the ICM installation by creating the Root Organizational Unit (page 99) "Cisco_ICM". You need not be a Domain Administrator to create the Cisco Root OU if that OU is going to be created in a nested OU (for example, Applications |_ Voice Applications ..), the Domain Administrator can create a parent OU with delegated rights to create Cisco_ICM Root OU.

Step 1 Review the ICM software staging guidelines (page 115).

Step 2 Ensure that you have Microsoft Windows installed.

Step 3 If you are installing a Logger or Distributor/HDS Admin Workstations, ensure that you have Microsoft SQL Server with the required service pack installed.

See Also

See the **Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html) for information on supported Windows and SQL Server versions.

Setup, Domain Manager, and the OU Hierarchy

- The Instance is no longer 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.
- Integrated use of the Domain Manager

When Instance Organizational Units are created by the ICM Domain Manager, user accounts in old ICM/IPCC security groups are automatically copied to new security groups in the ICM/IPCC 7.0 instance OU. The old groups are not modified.

If you create new user accounts in the old ICM/IPCC 5.0 or ICM/IPCC 6.0 system after the new ICM/IPCC 7.0 instance OUs were created, these accounts will not be valid in the new ICM/IPCC 7.0 system.

Domain Manager Functions

Refer to "About the Cisco ICM Domain Manager" for the detailed steps for each of the following:

- Open the Domain Manager (page 92).
- View Domains (page 98)
- Add a Domain to a View (page 98)
- Remove a Domain from a View (page 98)
- Create (Add) the Cisco Root Organizational Unit (page 99)
- Remove the Cisco Root Organizational Unit (page 100)
- Create (Add) a Facility Organizational Unit (page 101)
- Remove a Facility Organizational Unit (page 102)
- Create (Add) an Instance Organizational Unit (page 103)
- Remove an Instance Organizational Unit (page 103)
- Add members to a Security Group (page 106)
- Remove members from a Security Group (page 107)

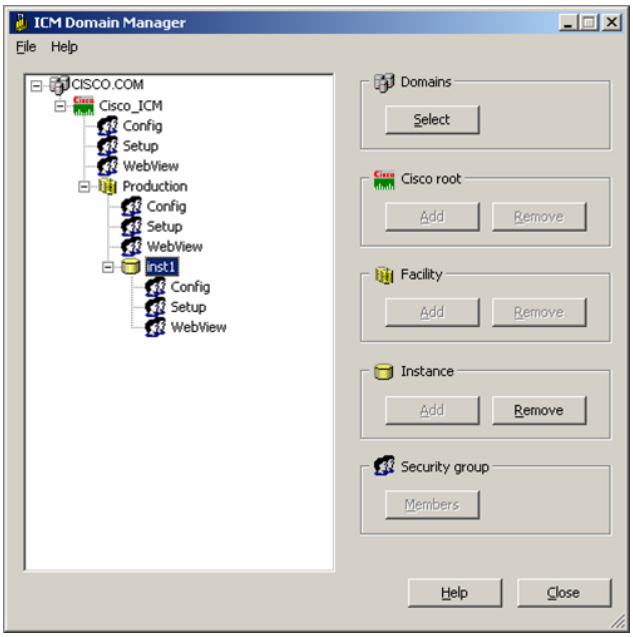
Chapter 7

About the Cisco ICM Domain Manager

The Cisco ICM 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 ICM related tasks.

The Domain Manager provides the means for you to select a domain then add/remove the Cisco Root, Facilities, and Instances.

Figure 25: 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 AWs

This chapter contains the following topics:

How to Open the Domain Manager

You can open the Domain Manager:

- Directly from the Cisco ICM Software CD.
- From Setup, including the main Cisco ICM Setup dialog (page 93), and when adding or editing an instance.
- From the ICM/bin shortcut in the Program Group on the AWs after a component has been installed.

For example, to open the Domain Manager from the Cisco ICM Software CD:

Step 1 Open the Cisco ICM software CD.

Step 2 Run the ICM Setup program, **setup.exe**, which you can find on the Cisco ICM Software CD or run the Domain Manager application **DomainManager.exe**.

The Cisco ICM Setup dialog (page 93) or the ICM Domain Manager dialog (page 94) opens, respectively.

Note: Refer to the **Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html) for information concerning hardening.

Step 3 If you ran **setup.exe**, in the Cisco ICM Setup dialog (page 93), click **Domain Manager**. Alternately, in the Cisco ICM Setup dialog (page 93), click **Add** in the ICM Instances list.

The Domain Manager dialog (page 94) or the Add Instance dialog (page 94) opens.

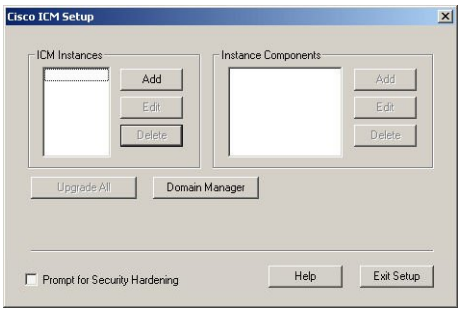
Step 4 If you opened the Add Instance dialog (page 94), click **Domain Manager**.

The ICM Domain Manager dialog (page 94) opens.

The default domain displayed is the domain the current user is logged into. You may display multiple domains in the domain tree in the left pane of the dialog.

ICM Setup Dialog

Figure 26: ICM Setup Dialog Box



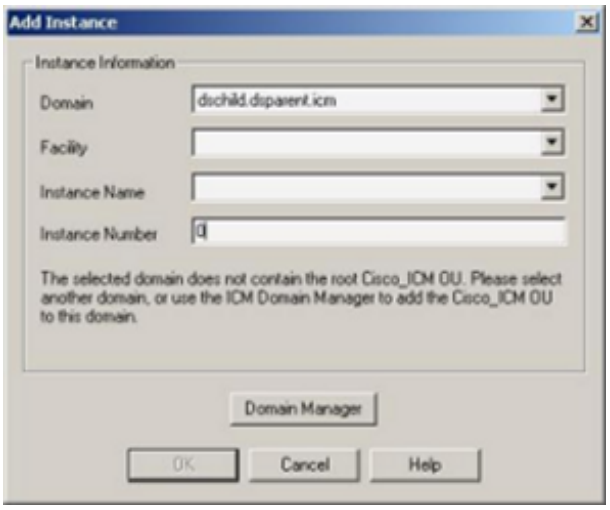
Note: Refer to the **Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html) for information concerning hardening.

In the ICM Setup dialog, click **Domain Manager** to open the Domain Manager (page 92) dialog.

You can also click **Add** under ICM Instances to open the Add Instance dialog, from which you can access the Domain Manager.

Add Instance Dialog

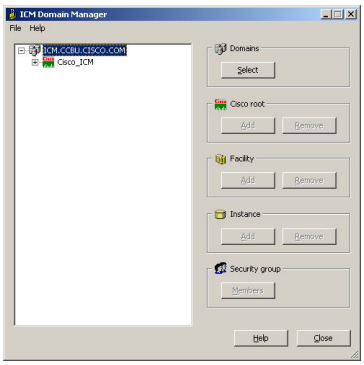
Figure 27: Add (ICM) Instance Dialog Box



In the Add Instance dialog, click **Domain Manager** to open the Domain Manager (page 92) dialog.

Domain Manager Dialog

Figure 28: Domain Manager Dialog Box



The Domain Manager dialog displays the current domain and the Cisco ICM related Organizational units contained in the domain.

Table 8: Domain Manager Dialog Properties

Property	Description
Domain Manager tree	Provides a view of the Cisco ICM created organizational units (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, the Domain Manager loads the Cisco OU

Property	Description
	hierarchy, which is then validated. The Organizational Unit Validation Errors dialog appears only if the error is due to missing or incorrect OU hierarchy information. Right-clicking any object in the tree presents a context menu. These menus provide additional functionality specific to the selected level: Domain • 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
Domains	To add or remove a domain from the Domain Manager tree, click **Select**. The Select Domains dialog (page 97) appears.

Property	Description
Cisco Root	To add the Cisco Root when a domain is selected that does not already have the Cisco Root, click **Add**. The Select Organizational Unit dialog (page 102) appears. To remove the selected Cisco Root and all of its facilities and instances, click **Remove**. **Warning: All ICM instances in this domain will no longer work properly if the organizational unit is removed. All users, groups, and other objects in this organizational unit will also be deleted.**
Facility	To add a new facility, select the Cisco Root OU then click **Add**. The Enter Facility Name dialog (page 101) appears. To remove the selected facility and all of its instances, click **Remove**. **Warning: All ICM instances in this facility will no longer work properly if the organizational unit is removed. All users, groups, and other objects in this organizational unit will also be deleted.**
Instance	To add an instance, select a facility in the Domain tree display, then click **Add**. The Add Instance dialog (page 94) appears. To remove the selected instance, click **Remove**. **Warning: This ICM instance will no longer work properly if the organizational unit is removed. All users, groups, and other objects in this organizational unit will also be deleted.**
Security group	Click Members to display the Security Group Members dialog (page 104) where you assign users to security groups.

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

- View Domains (page 97)
- Add a Domain to a View (page 98)
- Remove a Domain from a View (page 98)
- Create (Add) the Cisco Root Organizational Unit (page 99)
- Add a Facility Organizational Unit (page 101)
- Remove a Facility Organizational Unit (page 102)
- Add an Instance Organizational Unit (page 103)
- Remove an Instance Organizational Unit (page 103)
- Add members to a Security Group (page 106)
- Remove members from a Security Group (page 107)

How to View Domains

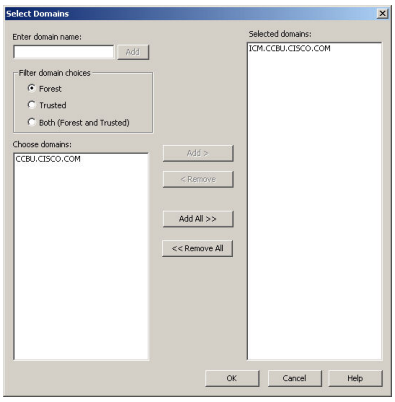
Step 1 Open the Domain Manager (page 92).

Step 2 In the right top pane of the ICM Domain Manager dialog (page 94), click **Select**.

The Select Domains dialog (page 97) opens. You can now add (page 98) or remove (page 98) domains for use with ICM software.

Select Domains Dialog

Figure 29: Select Domains Dialog Box



The Select Domains dialog offers a listing of domains for you to choose from. From the Select Domains dialog, you can add (page 98) or remove (page 98) domains that are displayed in the Domain Manager dialog.

Table 9: Select Domain Dialog 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:	Displays a list of domains you can choose from to add to the Selected domains list. **Add** > - Adds domains selected in the Choose domains list to the Selected domains list. < **Remove** - Removes selected domains from the Selected domains list.

Property	Description
	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. After clicking **OK**, these domains appear in the Domain Manager dialog.

How to Add a Domain to a View

Step 1 Run the Domain Manager, then click **Select**.

Step 2 Add domains to the view by using the controls in the Select Domains dialog (page 97):

a. In the left pane under **Choose domains:**, select one or more domains.

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

Step 3 You can also manually type in a domain to add to a view instead of clicking.

a. In the field under **Enter domain name:**, enter the fully qualified domain name to add.

b. Click **Add**.

Step 4 Click **OK**.

The selected domains now appear in the ICM Domain Manager dialog. You can then add the Cisco Root organizational unit (page 99).

How to Remove a Domain from a View

Step 1 Run the Domain Manager, then click **Select**.

Step 2 In the Select Domains dialog (page 97), in right pane under **Selected domains:**, select one or more domains.

Step 3 Click <**Remove** to remove the selected domains, or click <<**Remove All** to remove all the domains.

Step 4 Click **OK**.

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

How to Create (Add) the Cisco Root Organizational Unit

Create the Cisco Root Organizational Unit (page 40) either in the domain root, or beneath another organizational unit in the domain.

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

Before you can create the Cisco Root Organizational Unit, you must add the domain (page 98) that is to contain it.

Step 1 Add a domain (page 98). The default list contains the current domain.

Step 2 Click **Add** to add the Root.

The Select Organizational Unit dialog opens.

Figure 30: Select OU Dialog Box

Step 3 Select the Organizational Unit under which to create the Cisco Root OU, then click **OK**.

When you return to the ICM Domain Manager dialog, the "Cisco_ICM" OU appears at the domain Root. You can now add facilities (page 101) and configure security groups (page 106).

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 and select **Properties**. **Add** is disabled if the Root already exists.

Figure 31: Select OU Dialog Box After Creating the Cisco Root OU

See Also

What is the Cisco Root Organizational Unit? on page 40

How to Remove the Cisco Root Organizational Unit

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

Step 1 Open the Domain Manager (page 92).

Step 2 Select the Cisco 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 Organizational Unit.

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

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

Enter Facility Name Dialog

Figure 32: Enter Facility Name Dialog Box

You use the Enter Facility Name dialog to add a new Facility Organizational Unit (page 101) to the OU tree.

Enter the name of the new facility and click **OK** to return to the ICM Domain Manager dialog. The new facility OU is created and is displayed as a new node in the Domain tree display.

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

How to Create (Add) a Facility Organizational Unit

You create a Facility Organizational Unit (page 41) to group one or more Instance Organizational Units (page 41).

Note: You must create at least one Facility Organizational Unit before you can create an ICM instance.

Before you can create a Facility Organizational Unit, you must havecreated the Cisco Root Organizational Unit (page 99) for the domain.

Step 1 Open the Domain Manager (page 92).

Step 2 In the tree view in the left pane, select the Cisco Root Organizational Unit under which to create the Facility Organizational Unit.

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

The Enter Facility Name dialog (page 101) opens.

Step 4 Type the name for the facility.

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

Step 5 Click **OK**.

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

How to Remove a Facility Organizational Unit

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

Step 1 Open the Domain Manager (page 92).

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

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

You are prompted to confirm the removal.

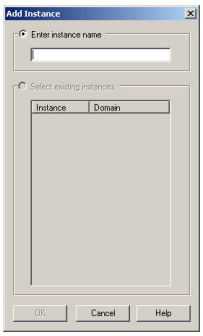
Warning: All ICM instances in this facility will no longer work properly if the organizational unit is removed. All users, groups, and other objects in this organizational unit will also be deleted.

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

The Facility Organizational Unit is removed from the tree.

Add Instance (Organizational Unit) Dialog

Figure 33: Add Instance (Organizational Unit) Dialog Box



You can use the Add Instance dialog (page 94) to add a new instance organizational unit (page 41) corresponding to an ICM instance, or create OUs based on existing registry information from previous ICM instance installations.

If you are creating the ICM instance for the first time, click **Enter instance name** and enter the name for the Instance OU corresponding to that ICM instance. After entering the new instance name, click **OK** to return to the ICM Domain Manager dialog. The new OU is created and displayed in the Domain Manager tree.

Note: The Instance Organizational Unit name must be five alpha-numeric characters or less, and cannot begin with a numeric character.

If, during an upgrade, you want to choose from existing instances (from older versions of the ICM software) to add to the new domain structure, click **Select existing instances** and make your choice.

Note: Select existing instances only appears if the Domain Manager is run on a machine where that instance was previously installed.

Click **OK** to return to the ICM Domain Manager dialog.

How to Create (Add) an Instance Organizational Unit

Create an Instance Organizational Unit (page 41) before, or while, creating an ICM instance.

You must create at least one Facility Organizational Unit (page 101) before you can create an Instance Organizational Unit.

Step 1 Open the Domain Manager. (page 92)

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

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

The Add Instance dialog (page 94) opens.

Step 4 If you are installing ICM software on the current computer for the first time, under the Enter instance name radio button, enter the instance name.

Note: The Instance Organizational Unit name must be five alpha-numeric characters or less, and cannot begin with a numeric character.

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

Step 5 Click **OK**.

The Instance Organizational Unit is added below the selected Facility Organizational Unit.

How to Remove an Instance Organizational Unit

Step 1 Open the Domain Manager (page 92).

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

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

You are prompted to confirm the removal.

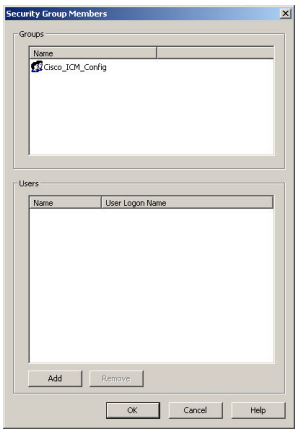
Warning: This ICM instance will no longer work properly if the organizational unit is removed. All users, groups, and other objects in this organizational unit will also be deleted.

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

The Instance Organizational Unit is removed from the tree.

Security Group Members Dialog

Figure 34: Security Group Members Dialog Box



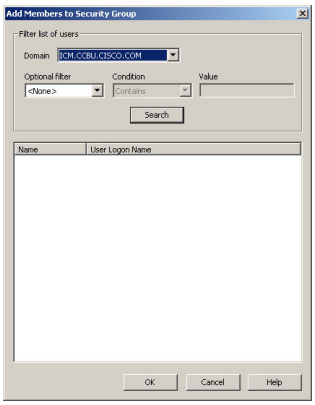
This dialog shows you the users and groups that are members of the group selected in the Domain Manager dialog. It allows you to add and remove users from the selected group.

Table 10: Security Group Members Dialog Properties

Property	Description
Groups	Displays the name of groups.
Users	Displays the name and user logon name of the user(s).
Add	Click to display the Add Members to Security Group dialog (page 105).
Remove	Click to remove the selected users from the Users list.
OK	Click to save changes and return to the ICM Domain Manager dialog (page 94).

Add Members to Security Group Dialog

Figure 35: Add Members to Security Group Dialog Box



This dialog is used to select members to add to a security group. When you click **OK**, the users selected are added to the Users list on the Security Group Members dialog (page 104). Double-clicking on a single user adds that user to the Users list as well.

Table 11: Add Members to Security Group Dialog Properties

Property	Description
Domain	Select the domain the users are in.
Optional Filter	There are three Optional Filter options: • <None> • Name • User Logon Name
Condition	There are three Condition options: • Contains • Ends with • Starts with
Value	Enter your own search criteria.
Search	Click to search for users based on the filter settings.
Member list	Displays a list of the user name(s) and user logon name(s) resulting from the search.

How to Add Users to a Security Group

Step 1 Select the Security Group you want to add a user to.

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

The Security Group dialog appears.

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

The Add Members to Security Group dialog appears.

Step 4 Select the filters to use to create a list of users to select from.

- **Domain** - Select the domain the user(s) you want to add to the Security Group is/are in.
- **Optional filter**

  Select the appropriate optional filter(s) to use to search for and list the member(s) you want to select from to add to the Security Group.

  – **<None>** - No additional filter selections applied, Condition and Value inaccessible.

  – **Name** - Continue and select the appropriate Condition and Value. This filter is based on the name of the user.

  – **User Login Name** - Continue and select the appropriate Condition and Value. This filter is based on the User Login Name of the user.

- **Condition**

  Select the condition to facilitate your search for the member(s) you want to list and select from to add to the Security Group.

  – **Contains** - find and list user(s) containing the entered Value.

  – **Starts with** - find and list user(s) whose name or user login name starts with the entered Value.

  – **Ends with** - find and list user(s) 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(s) you want to add to the Security Group from the displayed list.

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

How to Remove Members from a Security Group

Step 1 Select the Security Group you want to remove members from.

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

The Security Group dialog appears.

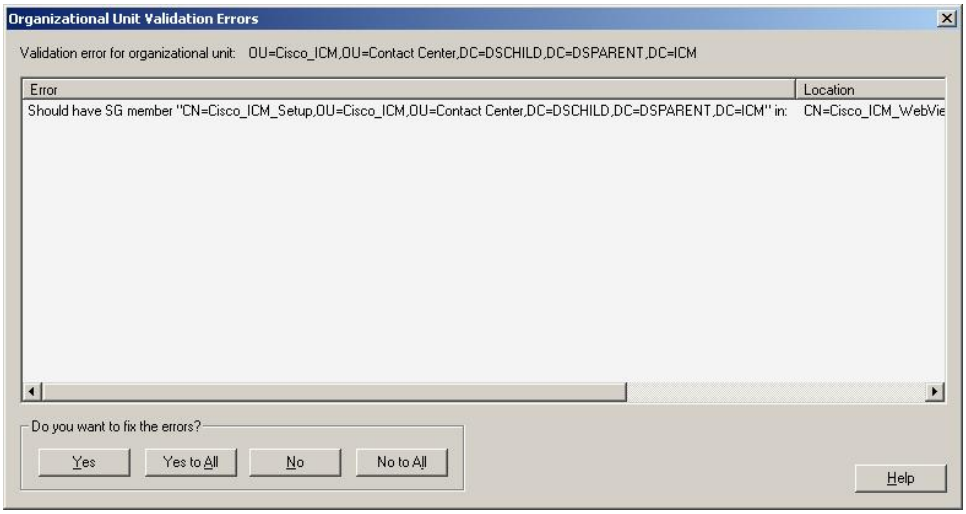
Step 3 In the Users pane, select the member(s) you want to remove from the Security Group, from the displayed list.

Step 4 Click **Remove**.

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

Organizational Unit Validation Errors Dialog

Figure 36: Organizational Unit Validation Errors Dialog Box



This dialog appears if errors are found during OU validation.

Table 12: Organizational Unit Validation Errors Dialog Properties

Property	Description
Validation error for organizational unit:	Displays the OU containing the error(s) found during OU validation.
Error	Displays description(s) of errors found during OU validation.
Location	Displays the location of each error found during OU validation.

Property	Description
Do you want to fix the errors?	Four possible responses: • **Yes** - Fixes the displayed error(s) then attempts to sequentially validate the next OU. If additional errors are found, you are returned to this dialog. • **Yes to All** - Recursively fixes the displayed error(s) and any errors found during sequential validation attempts for other ICM OUs without returning to this dialog. • **No** - Does not fix the displayed error(s) but attempts to sequentially validate the next OU. If additional errors are found, you are returned to this dialog. • **No to All** - Does not fix the displayed error(s) but recursively validates the OUs and logs any additional errors without returning you to this dialog.

Chapter 8

About the IPCC Machine Initializer Utility

The IPCC Machine Initializer is used in System IPCC to create the Root OU in the AD domain in which your deployment runs. These specifications are a required part of System IPCC configuration.

This chapter contains the following topics:

Who can use the IPCC Machine Initializer?

Any user with network access that can login to the machine on which it is installed can access IPCC Machine Initializer. However, only users with the appropriate Active Directory permissions can create the IPCC Root and Facility. To allow this, your Active Directory domain administrator must delegate full control of the parent of the Cisco Root OU needed to create the Cisco Root OU to the individual who performs your initial System IPCC installation.

How to Create the IPCC Root and Facility

Use the main window in the IPCC Machine Initializer to create the IPCC Root, and to create or select an IPCC Facility.

How to Create the IPCC Root

You can add the IPCC Root Organizational Unit (OU) either to the domain root, or beneath another organizational unit in the domain.

Step 1 Under IPCC Root, click **Create Root**. The Create Root dialog opens.

Step 2 To create the IPCC Root at the top level of the domain, click **OK**. The IPCC Root (automatically named "Cisco_ICM") is created.

Step 3 To create the IPCC Root within another OU in the domain, expand the desired OU to the location you want to create the IPCC Root. Click **OK**. The IPCC Root (automatically named "Cisco_ICM") is created.

Note:

- Once the IPCC Root is created on your domain, the Create Root button becomes permanently unavailable.
- The user who creates the Cisco Root Organizational Unit automatically becomes a member of the Setup Security Group for the Cisco Root OU. In effect, this user is granted privileges to all IPCC tasks in the domain.

How to Create the IPCC Facility

Note: Before you can add a facility, you must create the IPCC Root for the domain.

Step 1 To create a new facility, under *Create or Select New Facility* click **Create**.

Step 2 Enter a facility name up to 32 characters. Click **OK**.

How to Select an Existing IPCC Facility

Step 1 Under *Create or Select New Facility* select an existing IPCC facility from the list.

Note: All IPCC machines in your deployment must use the same facility.

Using the Machine Initializer Before and After IPCC Installation

Using the IPCC Machine Initializer during IPCC Installation

The IPCC Machine Initializer runs automatically as part of the System IPCC installation process.

The first time the IPCC Machine Initializer runs on the current Active Directory Domain on which you are installing System IPCC, it prompts you to create the IPCC Root.

Once you have created the IPCC Root, the IPCC Machine Initializer allows you to create an IPCC OU Facility. Once the facility has been created, use the same facility during the installation of subsequent IPCC machines. If the facility does not appear in the list, use the Refresh button to update the list. All machines in your IPCC deployment must reference the same facility.

Using the IPCC Machine Initializer Post IPCC Installation

The IPCC Machine Initializer is installed on every machine in your System IPCC deployment and can be accessed on any of these machines after installation. Under typical circumstances, it is not necessary to run the IPCC Machine Initializer after IPCC install. However, as desired, it can be used post-install to create a new IPCC OU Facility and to assign your IPCC machines to that facility.

IPCC Machine Initializer Requirements

- The machine must be in the domain.
- Must be run as a Domain user with administrative privileges.
- SQL Server must be running on machines requiring the database
  - Administration & WebView Reporting
  - Central Controller

System IPCC to ICM Component Mapping

The table below maps System IPCC machine types to their equivalent ICM components.

System IPCC Machine Type	Corresponding ICM Component
Central Controller	CallRouter, Logger
Agent/IVR Controller	System PG, CTI Server, CTI OS Server **Note:** If CVP is deployed, this also includes the VRU PG.
Administration & WebView Reporting	Distributor Admin Workstation, Historical Data Server (HDS), WebView
Multichannel Controller	Media Routing Peripheral Gateway (MR PG)
Outbound Controller	Outbound Dialer, MR PG

Chapter 9

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

LimitUserAssociationByInstance

As of 7.5(1), the feature to restrict associating or adding a duplicate user to multiple instances has been implemented. To activate/deactivate this feature, you must change the registry value of *LimitUserAssociationByInstance*. This registry key is added when User List tool, Agent Explorer, or ICM local Setup is run.

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

When *LimitUserAssociationByInstance* is set to 1, the feature is activated 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 <*user name*>, 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 ICM instance than the instance you are in. When the error message is displayed, you can enter the user name as JohnMSmith to make it unique.

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

LimitUserAssociationByInstance

Part 2: Staging Guidelines

Chapter 10

About Staging Prerequisites

System Design Specification

Before beginning the ICM software staging process, ensure that an ICM/IPCC System Design Specification is created and approved.

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

- Familiar with Windows Operating System
  - Active Directory
  - Security concepts
  - Network configuration and operation
- Familiar with SQL Server
  - Enterprise Manager
  - Query Analyzer
  - SQL scripting
- ICM/IPCC Knowledge
  - ICM/IPCC Nodes (Router, Logger, AW, PGs)
  - HDS Schema knowledge
  - Deployment models (including WebView)

  - Have read the Cisco ICM/IPCC Enterprise & Hosted Rel. 7.0(0), 7.1(1), & 7.1(2) Hardware & System Software Specification (Bill of Materials) [Cisco Unified Intelligent Contact Management Enterprise] and the SRND

The System Design Specification must contain the following:

- Description of ICM Sites and Nodes
- Data Communications Infrastructure
- Event Notification and Remote Access Points
- Naming Conventions
- IP Addressing Scheme
- Active Directory Plan

  Including:

  - Active Directory 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 ICM software deployment, you define the hardware specifications and third-party software requirements. You can find the Cisco guidelines for hardware and software requirements for ICM software in the **Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

In addition, for additional information refer to the **IPCC Enterprise Software Compatibility Guide** (http://www.cisco.com/univercd/cc/td/doc/product/icm/ipccente/index.htm)

How to Set the Staging Environment

Follow the steps below to set the staging environment:

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

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

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

Step 4 Ensure you have all software license numbers available.

Step 5 Ensure that the 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 can follow the System Design Specification and are available on site.

See Also

System Design Specification templates on the Cisco Web site (www.cisco.com/partner/WWChannels/technologies/IPCC/design2.html) **Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)

Chapter 11

About Windows Server 2003 Staging

Note: This section does not provide step-by-step instructions for tasks related to Microsoft Windows. For such information, see Microsoft documentation or the Windows online help.

This chapter contains the following topics:

Drive Partitioning Guidelines

Create drive partitions for the servers being built according to settings in the ICM/IPCC System Design Specification.

Format C drive as NTFS.

Note:

- You may need to use the manufacturer's drive partitioning/RAID array software to set up the partition.
- Because of its automated installation and configuration, System IPCC does not allow the partitioning described below. For System IPCC, you must not partition the server.

Logger and Admin Workstation Historical Data Server Partitioning Guidelines

For servers hosting an ICM Logger or Admin Workstation Historical Data Server, use the following guidelines for partitioning.

- Use the C drive for the operating system, virtual memory paging file space, core ICM software, 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, Admin Workstation, CTI Server, and CTI OS Server Partitioning Guidelines

For servers hosting an ICM Router, Peripheral Gateway, Admin Workstation (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 ICM software, the Admin Workstation 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 Setup Guidelines

Note: For additional information on installing Microsoft Windows Server 2003, refer to the **Windows Server 2003 homepage** (http://www.microsoft.com/windowsserver2003/default.mspx)

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

Use the following guidelines when setting up a Windows 2003 Server for ICM software:

- Select the necessary Management and Monitoring Tools.

  Check the following items on the list:

  – **Network Monitor Tools**

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

- Do not install Internet Information Services unless the server will host WebView or the ICM multichannel options.
- Install the WMI Windows Installer Provider.

  Note: Refer to SNMP Management (page 126) for additional information.
- Install SNMP support.

  Note: Refer to SNMP Management (page 126) for additional information.
- 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, do the following:
  - 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, do the following:
  - 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: Refer to Persistent Static Routes (page 125) for information on configuring a default gateway for the private network.
  - In the DNS tab, leave the address space empty and uncheck **Register**.

How to Join Standalone Servers to the Domain

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

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

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

- Logger
- CallRouter
- AWs
- WebView Server

Note: WebView must be installed on the same domain as the AW/HDS.

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

Step 4 Reboot the server and login to the domain.

How to Customize Your Desktop

Customize your desktop on all ICM components.

Step 1 Create shortcuts on desktop, as detailed in the ICM/IPCC System Design Specification.

Step 2 Configure the command prompt:

a. Open the command prompt from the desktop shortcut.

b. Right-click in the title bar and select **Defaults**.

c. On the Options tab, uncheck **Insert Mode**.

d. Select the Font tab. Set the command prompt font size to **7x12**.

e. Select the Layout tab. Set the Command Prompt screen buffer to **200x9999**.

Step 3 Set the Folder Options:

a. Open the **Control Panel**, then open **Folder Options**.

b. On the General tab, select **Use Windows classic folders**.

c. On the View tab, select **Display the full path** for the address bar and title bar. Select **Show hidden files and folders** and uncheck **Hide extensions for known file types**.

Network Card Settings

To setup the network card settings, select **Start > Control Panel > Network Connections** then, in the menu bar, click **Advanced > Advanced Settings**, the Advanced Settings dialog 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**
  - **100Mb 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, do the following:
  - 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.

Persistent Static Routes

For geographically distributed ICM software 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 ICM/IPCC Enterprise and Hosted Edition servers. However, to ensure seamless integration with the Microsoft native SNMP components, installation of the Microsoft Management and Monitoring Tools subcomponents is required.

To install these required subcomponents, from Control Panel:

1. Select **Start > Settings > Control Panel > Add/Remove Programs > Add/Remove Windows Components**
2. Select **Management and Monitoring Tools**.
3. Click **Details**.
4. Select **Simple Network Management Protocol** and **WMI Windows Installer Provider**.
5. Click **OK** then click **Next** to continue with the wizard to install these subcomponents.

   Note: You may need to have your Microsoft Windows 2003 Server CD handy to complete the installation.
6. When the installation is complete, click **Finish**.

If SNMP management support has already been installed and configured for this server, the existing configuration parameters should be collected so they can be used to configure the components installed by ICM 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-

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

2. Click **Properties** (or select the Properties context menu).
3. On the SNMP Service Properties dialog, select the **Security tab**.

   Note the following settings and configuration data:

   – The state of the **Send authentication trap** checkbox.

   – 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.

   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, 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 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(s).
- 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:
  – User names

- Authentication protocol used (if authentication is required)
- Privacy protocol used (if privacy is required)
- Trap destinations and the user name expected by each management station

The installed Microsoft Management Console Snap-In (Cisco SNMP Agent Management) is used to configure the SNMP properties. Please consult the ICM/IPCC SNMP User Guide for details.

Installing the Windows Firewall

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, refer to the

Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0) (http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/coreicm7/config7/index.htm)

For detailed information on supported platforms for ICM software, see the **Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)

For additional information on the Windows Firewall see the:

Windows Server 2003 Windows Firewall (WF) (http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/wf.mspx) **Help: Windows Firewall How To...** (http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/005d7651-fefa-4e00-8f55-714fc0175fe1.mspx)

Configuring Windows Server 2003 Firewall to Communicate With Active Directory

You need to open up the ports used by domain controllers (DCs) for communication via LDAP and other protocols to ensure Active Directory 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 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 Active Directory 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 Active Directory 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 2000 and 2003 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
636	TCP	UDP	LDAP SSL
3268			LDAP GC
3269			LDAP GC SSL
42			Wins Replication
53	TCP	UDP	DNS

Server Port	Protocol	Protocol	Service
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 Active Directory, 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 Active Directory.

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 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.

Remote Monitoring System Requirements

Follow the instructions below if you plan to use the Phone Home capabilities of Cisco Remote Monitoring System (RMS) software. The RMS software sends events to the Cisco Technical Assistance Center.

Note: Enable the Phone Home system on servers running the Logger component

Drive Shares

You must configure a hidden share folder on the C drive of servers running the Logger component in order for RMS Listeners to access Phone Home events.

See Also

Routing and Remote Access Configuration on page 132
Cisco Remote Monitoring System Administration Guide
Cisco AlarmTracker Client User Guide

Routing and Remote Access Configuration

If the Logger is utilizing Phone Home functionality using a modem, you must configure a Listener server for Routing and Remote Access. This provides dial-up access to the Listener for the Remote Monitoring System (page 131) and Phone Home functionality.

Typically a deployment also has one Peripheral Gateway that the Cisco Technical Assistance Center can access.

Note:

- When monitoring pre-ICM 5.0(0) systems, you must use Windows 2000 as your operating system due to the NET BEUI requirements for RMS.
- When Monitoring ICM 5.0(0) and ICM 6.0(0) systems using NET BEUI, you must have Windows 2000 as your operating system until you reconfigure the Logger to use TCP/IP. At this point, you can upgrade to Windows 2003.

Refer to the *Remote Monitoring Suite Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Cisco Remote Monitoring Suite Release 2.1(0)* for information concerning how to configure routing and remote access using the Routing and Remote Access Server Setup Wizard.

Automatic Updates

Refer to the **Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0)** (http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/coreicm7/config7/index.htm) for information on this setting.

Display Settings

Through the Windows Control Panel Display dialog:

- Ensure that no Screen Saver is selected.
- Set the AW 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 Advanced tab:

- When setting virtual memory, set the initial and maximum total paging file sizes to the values recommended 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, 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. Refer to the **Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0)** (http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/coreicm7/config7/index.htm) for additional information.

Remote Control Options

Refer to the following documents for information on remote control options:

- **Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)
- **Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0)** (http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/coreicm7/config7/index.htm)

Connectivity Validation

Before you begin the ICM software installation process, you should validate network connectivity for all servers that are part of the ICM software 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: Refer to the System Design Specification (page 117) to confirm that the system topology is correct.

Chapter 12

About Microsoft SQL Server Staging

ICM software requires that you install Microsoft SQL Server on each server that hosts a Logger or Admin Workstation (Real Time Distributor and HDS only) component.

This section contains guidelines for setting up Microsoft SQL Server for use with ICM software's Logger and Admin Workstation components.

For information about specific versions and patches of Microsoft SQL Server supported by ICM software, see the **Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) Hardware and System Software Specifications (Bill of Materials)** (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 installing Microsoft SQL Server. For that information, refer to Installing Microsoft SQL Server 2000 (page 139) or Installing Microsoft SQL Server 2005 (page 143) as applicable.

- 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

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, accept the defaults.
- For SQL Server Service Account, select the following:
  - **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, please use it to customize the installation of SQL Server.

Please note that this user account (e.g. 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)
- Increase quotas (Windows 2000 Server)

- 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. Refer to Q283811 at http://support.microsoft.com/default.aspx?scid=kb;en-us;283811 for more details on "How to change the SQL Server or SQL Server Agent Service account without using SQL Enterprise Manager in SQL Server 2000".

Please refer to the **Security Best Practices Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.0(0)** (http://www.cisco.com/univercd/cc/td/doc/product/icm/icmentpr/icm70doc/coreicm7/config7/index.htm) 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 2000 Component Installation Options

This section provides an overview of the basic SQL Server component installation options. For a detailed step-by-step instructions, refer to How to Install Microsoft SQL Server 2000 (page 140) or How to Install Microsoft SQL Server 2005 (page 143) as applicable.

Do the following when starting the SQL Server setup program:

1. In the first dialog of the setup wizard, select **SQL Server 2000 Components**.
2. In the second dialog of the setup wizard, select **Install Database Server**.
3. In the Computer Name dialog, use the default, **Local Computer**.
4. In the Installation Selection dialog, use the default, **Create a new instance of SQL Server, or install Client Tools**.
5. When given the option to chose between the setup types **Typical** or **Custom**, choose **Custom**.
6. When setting the Network Library, ensure **Named Pipes** and **TCP/IP** are enabled. Once SQL is installed you must ensure the order is Named Pipes, then TCP/IP.
7. In the Installation Definition dialog, use the default, **Server and Client Tools**.

Basic SQL Server 2005 Component Installation Options

This section provides an overview of the basic SQL Server component installation options. For a detailed step-by-step instructions, refer to How to Install Microsoft SQL Server 2000 (page 140) or How to Install Microsoft SQL Server 2005 (page 143) as applicable.

Do the following when starting the SQL Server setup program:

1. On the Start screen, 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 is displayed.

   The correct order and states are:

   – **Shared Memory** - Enabled
   – **Named Pipes** - Enabled
   – **TCP/IP** - Enabled
   – **VIA** - Disabled

Authentication Mode

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

Note: Environments integrated with CIM require selecting **Mixed Authentication Mode** as the CIM application does not support Windows authentication mode. In addition, some environments have custom applications that access the ICM Logger and/or Distributor databases

and may 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 Microsoft SQL Server 2000

SQL Server 2000 is only installed on Loggers, HDS, or AWs. ICM/IPCC 7.5(1) supports MS SQL Server 2000 or 2005 Standard and Enterprise Editions.

Note: When performing a Technology Refresh upgrade on an AW, SQL Server must be installed on the same drive on the new server. For example: If SQL Server was installed on the C: drive of the source server, it must be on the C: drive of the destination server.

The following is an overview of the SQL Server 2000 installation:

1. Copy all of the files on the SQL Server 2000 CD to a directory on your drive.
2. Install SQL Server 2000.
3. Install the SQL Server service pack(s).

How to Install Microsoft SQL Server 2000

SQL Server 2000 is only installed on Loggers, HDS, or AWs.

Step 1 Run **autorun.exe**.

Step 2 Select **SQL Server 2000 Standard Edition** to start SQL Server setup.

Step 3 On the first screen:

a. Select **Install SQL 2000 Server Components**.

b. Select **Install Database Server**.

c. Read the Welcome screen.

d. Click **Next**.

Step 4 On the Computer Name screen:

a. Choose the default, **Local Computer**.

b. Click **Next**.

Step 5 On the Installation Selection screen:

a. Choose the default, **Create a new instance of SQL Server**.

b. Click **Next**.

Step 6 On the User Information screen:

a. Enter the **user name** and **company name**.

b. Click **Next**.

Step 7 On the Software License Agreement screen:

a. Read the terms of the license agreement, then click **Yes**.

Step 8 On the Installation Definition screen:

a. Choose the default **Server and Client Tools**.

b. Click **Next**.

Step 9 On the next screen:

a. For Instance Name, check **Default**.

b. Click **Next**.

Step 10 On the Setup Type screen:

a. Select **Custom** for the setup type.

b. Install the program files to any disk with space available (default is C:).

Note: MS SQL disk space requirements: 270 MB (full installation), 250 MB (typical), 95 MB (minimum), 44 MB (Desktop Engine) plus Analysis Services: 50 MB minimum and 130 MB typical and 80 MB for the English Query. Check your MS SQL documentation for additional information.

Step 11 On the Select Components screen:

a. Uncheck **Install Books Online**.

b. Leave all other fields set to their default values.

c. Click **Next**.

Step 12 Under Services Accounts select items in exactly this order:

a. Select **SQL Server**.

b. Select **Customize settings for each service**.

c. Select **Use domain account**.

d. Check **Auto-start service**.

e. Select **SQL Server Agent**.

f. Select **Customize settings for each service**.

g. Check **Auto-start service**.

h. Click **Next**.

i. A pop-up dialog explaining a dependency appears, click **OK**.

Step 13 Under Authentication Mode:

a. Select the **Windows Authentication** or the **SQL Authentication** mode.

If you select the Windows Authentication mode enter the:

1. ICM instance name

2. Login ID
3. User password

Note: User must be able to log into the ICM Logger with read privileges.

If you select the SQL Authentication mode enter the:

1. ICM instance name
2. Login ID
3. User password

Note: User must have read access to the ICM Logger database.

b. Press **Enter**.

c. Click **Next**.

Step 14 On the Collation Settings screen:

a. Click **Collation Designer**.

b. Be sure that **Latin1_General** is selected.

c. Set the Sort Order to **Binary**.

d. Leave other files set to their default values.

e. Click **Next**.

Step 15 Under Network Libraries:

a. Uncheck all choices except for **Named Pipes** and **TCP/IP Sockets** unless instructed otherwise.

For **Named Pipes**, the pipe reads **\\.\pipe\sql\query**.

For **TCP/IP Sockets**, the Port number is **1433**.

b. Click **Next**.

Step 16 On the Start Copying Files screen:

a. Read and click **Next**.

Note: Prior to completing the Licensing dialog box, refer to the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html) "SQL Server 2000 Licensing" section. In addition, ensure you meet all the terms of the licensing agreement between you and your software OEM.

Step 17 In the Licensing dialog box, select the Licensing method and the number of devices or connections, as appropriate. Click **Continue**.

Note: If you choose **Processor License**, make sure there are sufficient concurrent connection licenses so that the system does not run into licensing problems. A minimum of 40 concurrent connections is required, though the precise number depends on the accessing need.

Step 18 A dialog box with the message "Setup is installing Microsoft Data Accessing Components (MDAC) ..." appears.

Note:

- Occasionally, MDAC installation fails. The remedy is to download MDAC 2.7, or later, from a Microsoft web site and install it. Once MDAC has been installed, run SQL Server setup again.
- If a message box for Configure SQL Server Agent pops up, click **OK**.

The SQL 2000 installation is now complete.

Step 19 Install the appropriate SQL Server Service Pack.

Note: For additional information on the applicable Microsoft SQL Server Service Pack, refer to the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

a. Download the appropriate SQL Server service pack from the Microsoft web site.

b. Following the instructions provided with the service pack, install it.

c. Verify the Network Library protocol order (Named Pipes first, then TCP/IP) using the SQL Client Network Utility.

Installing Microsoft SQL Server 2005

SQL Server 2005 is supported with the 7.5(1) release.

Note: When performing a Technology Refresh upgrade on an AW, SQL Server must be installed on the same drive on the new server. For example: If SQL Server was installed on the C: drive of the source server, it must be on the C: drive of the destination server.

The following is an overview of the SQL Server 2005 installation:

1. Copy all of the files on the SQL Server 2005 CD to a directory on your drive.
2. Install SQL Server 2005.
3. Run the SQL Server Configuration Manager to configure the Client Protocols.

4. Install the SQL Server service pack(s).

How to Install Microsoft SQL Server 2005

In ICM/IPCC 7.5(1), SQL Server 2005 is only installed on Loggers, HDS, or AWs.

Note: In System IPCC 7.5(1), these core components are referred to as the Central Controller and Administration and WebView Reporting machine.

Step 1 Run **autorun.exe**.

Step 2 On the Start screen, select **Server components, tools, Books Online, and samples** to start SQL Server setup.

The Software License Agreement screen appears.

Step 3 Read the terms of the license agreement.

a. Check **I accept the licensing terms and conditions**.

b. Click **Next**.

The Installing Prerequisites screen appears.

Step 4 Click **Install**.

The Welcome to the Microsoft SQL Server Installation Wizard screen appears.

Step 5 Click **Next**.

The System Configuration Check screen appears.

Step 6 When the system configuration check completes successfully, click **Next**.

The Microsoft SQL Server Installation screen appears.

Step 7 When the installation has completed, click **Next**.

The Registration Information screen appears.

Step 8 Complete the Name, Company, and Product Key fields, then click **Next**.

The Components to Install screen appears.

Step 9 Select **SQL Server Database Services** and **Workstation components, Books Online and development tools**, then click **Next**.

The Instance Name screen appears.

Step 10 Select **Default instance**, then click **Next**.

The Service Account screen appears.

Step 11 Select **Use a domain user_account**, then complete the Username, Password, and Domain fields.

Step 12 In the Start services at the end of setup section select **SQL Server** and **SQL Server Agent**, then click **Next**.

The Authentication Mode screen appears.

Step 13 Select **Windows Authentication Mode** or **Mixed Mode (Windows Authentication and SQL Server Authentication)** as appropriate.

If **Mixed Mode (Windows Authentication and SQL Server Authentication)** is selected, you must provide the sa logon password and confirm it.

Note: The sa user must have read access to the ICM Logger database.

Step 14 Click **Next**.

The Collation Settings screen appears.

Step 15 Select **Collation designer and sort order**, then select **Latin 1_General** from the drop-down list.

Step 16 Select **Binary**, then click **Next**.

The Error and Usage Report Settings screen appears. You have the option of selecting either error and reporting selection, or neither.

Step 17 After making your choice, click **Next**.

The Ready to Install screen appears.

Step 18 After reviewing the components to be installed, click **Install**.

The Setup Progress screen appears and the installation begins.

Step 19 When the installation has completed, click **Next**.

The Completing Microsoft SQL Server 2005 Setup screen appears.

Step 20 After reviewing the provided information, click **Finish**.

The SQL Server 2005 installation is complete.

Step 21 Select **Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager**.

The SQL Server Configuration Manager appears.

Step 22 Expand **SQL Native Client Configuration** and select **Client Protocols**.

A list of the client protocols appears to the right.

The correct order and states are:

1. **Shared Memory** - Enabled
2. **Named Pipes** - Enabled
3. **TCP/IP** - Enabled
4. **VIA** - Disabled

Step 23 If the order/state is 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.

Step 24 Click **OK**.

The Client Protocol Properties dialog closes.

Step 25 Expand the SQL Server Network Configuration and select **Protocols for MS SQL Server**.

Step 26 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.

Step 27 On the Menu bar select **File > Exit**.

The SQL Server Configuration Manager closes.

Step 28 Install the appropriate SQL Server Service Pack.

Note:

- In "Services", the Distributed Transaction Coordinator must be set to **Automatic** and running prior to applying the service Pack.
- For additional information on the applicable Microsoft SQL Server Service Pack, refer to the **Cisco ICM/IPCC Enterprise and Hosted Edition Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html).

a. Download the appropriate SQL Server service pack from the Microsoft web site.

b. Following the instructions provided with the service pack, install it.

Installing SQL Service Packs

Install the latest supported SQL service pack as indicated by the **Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.0(0) 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 > Programs > MS SQL Server > Client Network Utility**).

Chapter 13

Active Directory and Domain Security Troubleshooting

It is important that Active Directory be fully functional so that the Organizational Unit Hierarchy can be created and ICM components installed. This section describes basic Active Directory troubleshooting and the tools you can use to detect common problems.

Warning: This section is not a substitute for more in-depth Microsoft Active Directory training.

Refer to the following troubleshooting hints prior to contacting Cisco TAC.

This chapter contains the following topics:

Cisco ICM Frequently Asked Questions (F.A.Q.)

Prior to contacting support services, refer to the following frequently asked questions:

Question: After all installation has been completed, can I remove "Create account Objects" and "Delete account Objects" delegation from the Cisco_Root OU? (When you uncheck these two, it also removes "Create All Child Objects" and "Delete All Child Objects"as well.) Will this break anything? Will Cisco still provide support if I change these properties?

Answer: Technically, yes, you can do it. However, there is a caveat. If you need to run Setup to alter configuration, ICM will not function correctly. Every time you run Setup, service

accounts are recreated. If you run Setup again with those rights removed, the account creation fails and you can not create user accounts. There is currently no rollback for this scenario. Do not remove the delegated rights.

Question: If the users in the local administrator group or Domain Admin group are changed, would it have any affect on ICM?

Answer: No the user added or removed from the group does not affect the handling of ICM. ICM only adds the ICM Security Service and Config groups to local administrator group. Presently it also adds the Service Account to the local administrator group. ICM considers Domain Admin group another group that can be added to ICM Security groups. Local Admin and Domain Admin group names can be changed because it is the token ID of the group that determines if the group being looked for is either of these groups.

Question: If there are mixed mode domains (having NT domain controllers) in the forest, will this affect ICM in any way?

Answer: As long as the domain functional level where ICM is located is Windows 2000 Native or higher, there will be no issues. Forest functional level has a minimal impact. However, from a network health perspective it is strongly suggested that you eliminate the remaining NT boxes in the short term, as network requirements will only become more stringent with time, and NT4 is a very unsecure platform.

Question:ICM 5.0(0) is not supported on Windows 2003 and no longer runs once the OS upgrade has taken place. Understanding this, could you save a considerable amount of time by moving the domain structure to a single forest and upgrading to Windows 2003 at the same time? Is this a feasible solution?

Answer: It is OK to upgrade the domain controllers to Windows 2003 as long as none of the domain controllers is co-located with an ICM component.

Question: Can Cisco further quantify the problems with running ICM 5.0(0) on Windows 2003 - is it just that this hasn't been tested? Would it be possible for Cisco to look at an amendment to the ICM 5.0(0) installer so that it would operate with Windows 2003?

Answer: ICM 5.0(0) has been end-of-lifed and is no longer supported. ICM 5.0(0) functionality fails on a Windows 2003 server partially, but not entirely, because the installer will not run.

Question: Can you put ICM on the domain controller?

Answer: Absolutely not. Co-locating ICM on the domain controller is not supported (see Domain Requirements (page 17) for additional information.)

Question: The implementation of multiple trees does not provide any level of access control. From any tree you can see all users and computers in all domains in the forest. Can you prevent users from browsing the forest?

Answer: There are other steps and settings that must be implemented to facilitate the isolation (such as disabling the computer browsing service). It is entirely possible to do the same things in a Grandfather, Father, Son (GFS) domain tree as well.

Question: In a situation where all DCs in the Forest Root fail, or the Schema becomes corrupt, it was our understanding that all domains in the forest would need to be rebuilt if no backup of the forest root is available. Please point to documentation that provides details on how to recover from this scenario without rebuilding the entire forest and all child domains.

Answer: The following websites document the proper recovery of Active Directory:

- *Best Practices: Active Directory Forest Recovery* - This paper is a best practice recommendation for recovering an Active Directory® forest after forest-wide failure has rendered all domain controllers (DCs) in the forest incapable of functioning normally. One section of the paper describes how you can reset trust passwords on one side of the trust.

  Best Practices: Active Directory Forest Recovery (http://www.microsoft.com/windows2000/downloads/tools/redir-netdom.asp)

- *Windows Server 2003 Active Directory Fast Recovery with Volume Shadow Copy Service and Virtual Disk Service* - Recovery with Volume Shadow Copy Service and Virtual Disk Service.

  Published: August 14, 2003; Download 173 KB; Microsoft Word file.

  Recovery with Volume Shadow Copy Service and Virtual Disk Service (http://www.microsoft.com/windowsserver2003/technologies/activedirectory/W2K3ActDirFastRec.mspx)

  Restoring a domain controller - Describes how to restore Active Directory data on a domain controller.

  Restoring a domain controller (http://www.microsoft.com/WINDOWSXP/home/using/productdoc/en/sag_restore_DC_overview.asp)

- *Windows 2000 Active Directory Diagnostics, Troubleshooting and Recovery* - This article covers: verifying Active Directory functionality; diagnosing and troubleshooting replication; locating Active Directory database files; backing up and recovering system state data; seizing FSMO roles; and session slides and demos.

  Windows 2000 Active Directory Diagnostics, Troubleshooting and Recovery (http://www.microsoft.com/technet/community/events/windows2000srv/tnt1-76.mspx)

- *How to perform a disaster recovery restoration of Active Directory* - on a computer with a different hardware configuration. This article describes how to perform a disaster recovery restoration of the Microsoft Windows 2000 Active Directory domain controller on a computer that has a different hardware configuration from that of the computer where you performed the Active Directory install.

  How to perform a disaster recovery restoration of Active Directory (http://support.microsoft.com/default.aspx?scid=kb;en-us;263532)

- *Microsoft Active Directory Disaster Recovery* - Recover a domain controller running Active Directory from a disaster such as a database malfunction caused by hardware or software failure.

  Microsoft Active Directory Disaster Recovery (http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/support/adrecov.mspx)

- *Active Directory Disaster Recovery in Branch Office Environments* - Chapter 10 of the Active Directory Deployment Guide outlines the steps necessary to backup and restore Active Directory and discusses the process of staging and shipping replacement domain controllers from a staging site.

  Active Directory Disaster Recovery in Branch Office Environments (http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/deploy/adguide/addeploy/addch10.mspx)

- *Support Webcast: Microsoft Active Directory Disaster Recovery* - Session Summary During this session, we will discuss the different types of Active Directory disaster recovery, and explain the steps needed to perform both authoritative and non-authoritative restores.

  Support Webcast: Microsoft Active Directory Disaster Recovery (http://support.microsoft.com/default.aspx?scid=kb;en-us;325560)

Question: The ICM servers must be placed into the existing corp.com\server OUs so that existing GPOs can be leveraged rather than having to create and administer GPOs and GPO links on separate server OU containers. Is this feasable?

Answer: If it is required that you put the ICM servers container in the corp.com\server OU, create a sub OU (ICM servers) then see About Security Groups (page 42). Remember to block corporate policies and use only ICM policies.

Question: Can the User accounts needed for IPCC, be located outside the OU structure created for IPCC?

Answer: User accounts can be located anywhere in the forest and will not negatively affect ICM. However, the ICM Service Accounts are created by the application and must exist in the instance OU. They cannot be changed.

Question: Do ICM administrators have to perform any AD functions that are currently only permitted to authorized groups currently handled by a third party service desk today? Can you use 3rd party tools to create/manage users and ICM OUs?

Answer: Administrators require the delegations specified in Chapter 3 (page 39) of the Staging Guide to ensure operation of ICM in a given environment. Administrators need general read access to the user containers and must be members of the Setup group in the ICM root container. For AD administration, only the use of ICM or Microsoft tools is supported by Cisco.

Question: Placing ICM objects elsewhere in Active Directory requires a change in processes and subsequent training to the Service Desk staff. Would these functions be better handled by the ICM Administrators within the recommended Cisco AD structure?

Answer: Yes, the only alteration that may be needed to your current design is the exclusion of ICM containers from GPO propagation. The actual location of the ICM Root OU tree is not relevant. As long as the OUs contain the appropriate groups, delegations, and the tree remains intact. The administration of the OU tree is delegated to the setup group as per the staging guide.

Question: Does placing ICM Security Groups outside the established corporate groups create the following issues?

- Additional delegations must be created for ICM Administrators to view/administer the Groups in that OU.
- Additional training for ICM Administrators must be provided for this.

Answer: Yes, ICM Administrators must be administering this OU tree to prevent accidents by lack of knowledge that may result in downtime.

Question: Are there risks involved when you allow ICM Administrators to administer/populate group objects within the Cisco OU heirarchy?

Answer: There are no inherent risks as ICM Administrators only have access to ICM information, for which they are responsible.

Question: Do the IPCC CallRouter servers have to reside in the Cisco OU heirarchy?

Answer: No, they cannot. See ICM Server Requirements (page 19) for additional information.

Question: Do unqualified security hardening settings across the enterprise present a risk to the IPCC System?

Answer: Yes, unqualified hardening may cause ICM to fail. That is why it is imperative that the ICM server OU containers have the Group Policy Object (GPO) settings “No Override” and “Block Policy Inheritance” checked.

Question: Must service accounts be created in the Instance OU. Can you move them to conform with internal policies?

Answer: No, the location of service accounts cannot be changed. These accounts are created by ICM setup and given the appropriate permissions.

Question: ICM 7.0 SR3 ES 29 is applied on the real time distributor and the central controller which are in different domains but have an external trust between them. When running AW setup on the distributor machine and trying to add the Distributor Service account in the Service Security group of CC domain, Setup throws an error saying that current setup user needs to be added in the Setup Security group of CC domain. Why does this error occur?

Answer: This behavior is expected. You must add the user to the same instance setup security group as the central controller domain.

Question: What do you do in the following situation?

When performing

- an Upgrade All
- editing an ICM component using the Installer Update C media
- after applying ICM 7.0 SR3, ES24, ES29, ES 35, ES 36, or ES 37 and performing a local edit

After clicking **Exit Setup** on the Instance dialog, Setup displays an error message saying "An installation support file could not be removed. The interface is unknown."

Answer: Click **OK** on the error message window. Setup will complete. There is no side effect to this bug.

Troubleshooting Tools

This section describes the tools you can use to detect common problems. Not all tools mentioned here are installed with the operating system. Some tools need to be installed from the **Server CD** > **Support Tools** folder.

What are the Troubleshooting Tools?

This section provides pointers to tools that you may find useful in troubleshooting Active Directory for ICM setup. It does not provide detailed or complete instructions on using Windows support tools. For more information, see the Microsoft documentation.

Table 13: Tools for Troubleshoot Active Directory and Other Windows Networking Problems

Tool	Description
Event Viewer (page 156)	Used to identify networking problems, name resolution, directory service and other types of problems. It categorizes error codes and makes it easier to identify a problem, and then analyze the cause of it.
IP Config (page 156)	Ensures the IP address, subnet mask, Default Gateway (DG), and DNS are set correctly. Also ensures the ethernet cable is connected.
Ping (page 156)	Tests the connectivity of machines.
Netdiag (page 156)	Network Connectivity Tester
Dcdiag (page 157)	Domain Controller Diagnostic Tool **Note:** Netdiag and Dcdiag are typically the best starting points to troubleshoot Active Directory problems.
Nslookup (page 157)	DNS queries and examining the contents of zone files.
Nbtstat (page 157)	Displays protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP.
Dnscmd (page 157)	Checks DNS Zone Types.
Ntdsutil (page 157)	Directory service management.
Netdom (page 158)	Locates Active Directory FSMO role holders and verifies trusts.
Dsacls (page 158)	Displays the security descriptor of an Active Directory object.
Sdcheck (page 158)	Verifies that ACL entries are correctly propagated through parent-child relationships.
Nltest (page 158)	Locates a Global Catalog and queries trusts.
Dsrevoke (page 158)	Reports the existence of all permissions for a specific user, or group, on a set of OUs in a domain and optionally, to remove from the DACLs of a set of OUs all permissions specified for a particular user or group.
Dsastat (page 159)	Checks domain replication.
Dsquery (page 159)	Checks for Object Name conflicts.

Install the Microsoft Windows Support Tools installer for Windows Server 2000 located on the Windows Server installation CD at \support\tools\setup.exe.

Install the Microsoft Windows Support Tools installer for Windows Server 2003 located on the Windows Server installation CD at \support\tools\suptools.msi.

Note: For additional information, refer to the **Microsoft Windows Server 2003 Tech Center** (http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/86ac50f1-0fbb-42c4-ba68-727efb24136f.mspx)

Event Viewer

Problems with Active Directory or DNS are reported in the Event Viewer.

The Event Viewer provides access to the:

- Active Directory log
- the DNS Server log (only on DNS Servers)

IP Config

Use the Windows Ipconfig utility to examine the computer's IP address, subnet mask, default gateway, and DNS servers and to ensure that these networking values are set correctly.

At a command prompt, simply enter **`ipconfig /all`**.

Pinging Other Machines

Test the computer's network connections to other computers using the *ping* command.

Ensure you can ping the Domain Controller(s) and the default gateway.

Netdiag

Network Connectivity Tester

Use the Netdiag utility to check that the client computer and domain controller(s) are functioning properly. Also determines if DNS is working properly. This tool helps isolate networking and connectivity problems.

Domain Controller service records must be in the DNS path.

At a command prompt, simply enter **`Netdiag`** or use **`netdiag /fix`**.

Dcdiag

Checks all the Domain Controllers in the domain and determines if they are working. Use the Domain Controller Diagnostic utility (Dcdiag) to analyze the state of a domain controller in a forest or enterprise and to report any problems. This tool analyzes the domain controller's functions and interactions across an entire enterprise.

To use the Dcdiag utility, at a command prompt on a domain controller, enter **`dcdiag /e`**. For information on the options and parameters available for the Dcdiag tool, enter **`dcdiag /h`**.

Nslookup

Use the Nslookup utility to perform DNS queries and to examine the contents of zone files on local and remote servers.

At a command prompt, enter **`nslookup`**.

Nbtstat

Use the Nbtstat utility to display protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP.

Note: The NBTStat utility has several other options in addition to viewing the name table of a remote server. For a list of options, enter **`nbtstat -help`**.

Dnscmd

You can use the Dnscmd utility to view properties of DNS servers, zones, and resource records.

For a complete list of Dnscmd commands and parameter options, at the command prompt, enter **`DnsCmd -help`**.

For example, to check DNS zone types:

- Use **`dnscmd /EnumZones /Primary`**.
- Use **`dnscmd /EnumZones /Secondary`**.

Ntdsutil

Use the Ntdsutil utility for directory service management.

For information on the options and parameters available for the Ntdsutil utility, at a command prompt on a domain controller, enter **`ntdsutil /?`**.

Netdom

Use the Netdom utility to manage computer accounts for member workstations and member servers. Also use netdom to find ADFSMO role holders by entering **`netdom query fsmo`**.

Note: Follow Microsoft recommendations for FSMO Role placement.

For information on the options and parameters available for the NETDOM utility, at a command prompt on a domain controller, enter **`netdom -help`**.

To verify a trust use **`netdom query /domain:<domain> trust /verify`**.

Dsacls

Use the Dsacls utility to view the security descriptor of an Active Directory object. The security descriptor for an object includes the Access Control List (ACL). The ACL contains the discretionary access control list (DACL) and the system access control list (SACL).

For information on the options and parameters available for the Dsacls utility, at a command prompt, enter **`dsacls`**.

Sdcheck

Use the Security Descriptor Check (Sdcheck) utility to verify that ACL entries are correctly propagated through parent-child relationships. The Sdcheck utility allows you to determine if ACLs are inherited correctly and replicated from one domain controller to another.

For information on the options and parameters available for the Sdcheck utility, at a command prompt, enter **`sdcheck`**.

NLTest

This command-line tool helps perform network administrative tasks. This also applies to service logon accounts.

A Global Catalog (GC) is needed during user creation, otherwise users are not able to login. If the Global Catalog is not available when you create the user, it must be online before the service is started for the first time. Each Active Directory site must have a Global Catalog server.

Use **`nltest /dsgetdc:<domain> /GC`** to find a Global Catalog.

To query trusts use **`nltest /domain_trusts`**.

Dsrevoke

Dsrevoke is a command-line tool that can be used on domain controllers that are running Windows Server 2003 or Windows 2000 Server to report the existence of all permissions for a

specific user or group on a set of OUs in a domain and optionally remove from the DACLs of a set of OUs all permissions specified for a particular user or group.

Dsrevoke complements the functionality provided by the Delegation of Control Wizard, which is used to delegate administrative authority, by providing the ability to revoke delegated administrative authority.

Dsastat

Use the Dsastat utility to compare and detect differences between directory partitions on domain controllers. The Dsastat tool monitors replication status at a higher level than monitoring detailed transactions.

Use **`dsastat –s:<server1>;<server2>`**.

For information on the options and parameters available for the Dsastat utility, at a command prompt on a domain controller, enter **`dsastat /?`**.

Dsquery

Queries Active Directory according to specified criteria. Each of the following dsquery commands finds objects of a specific object type. If the predefined search criteria in these commands is insufficient, use the more general version of the query command, **`dsquery *`**.

Dsquery commands::

- **`dsquery computer`**

  Finds computers in the directory that match specified search criteria.

- **`dsquery contact`**

  Finds contacts in the directory that match specified search criteria.

- **`dsquery group`**

  Finds groups in the directory that match the specified search criteria.

- **`dsquery ou`**

  Finds organizational units in the directory that match the specified search criteria. If the predefined search criteria in this command is insufficient, use the more general version of the query command, **`dsquery *`**.

- **`dsquery site`**

  Finds sites in the directory that match the specified search criteria.

- **`dsquery server`**

  Finds domain controllers according to specified search criteria.

- **dsquery user**

  Finds users in the directory that match the specified search criteria.

  Example: **dsquery user -name *CNF:***.

- **dsquery quota**

  Finds quota specifications in the directory that match the specified search criteria. A quota specification determines the maximum number of directory objects a given security principal can own in a given directory partition.

- **dsquery partition**

  Finds partition objects in the directory that match the specified search criteria.

Conflicts can happen after a failed domain replication.

Troubleshooting Reference

This section provides a reference and helps troubleshoot some basic AD issues.

The most common issues can be categorized as follows:

- Network Connectivity
- Name Resolution
- Domain Controller Issues
- Join and Authentication Issues
- Access Control
- AD Installation and Removal Issues[1]
- Database Issues[1]
- Schema Issues[1]
- Flexible single-master operations (FSMO)[1]
- Replication Issues[1]

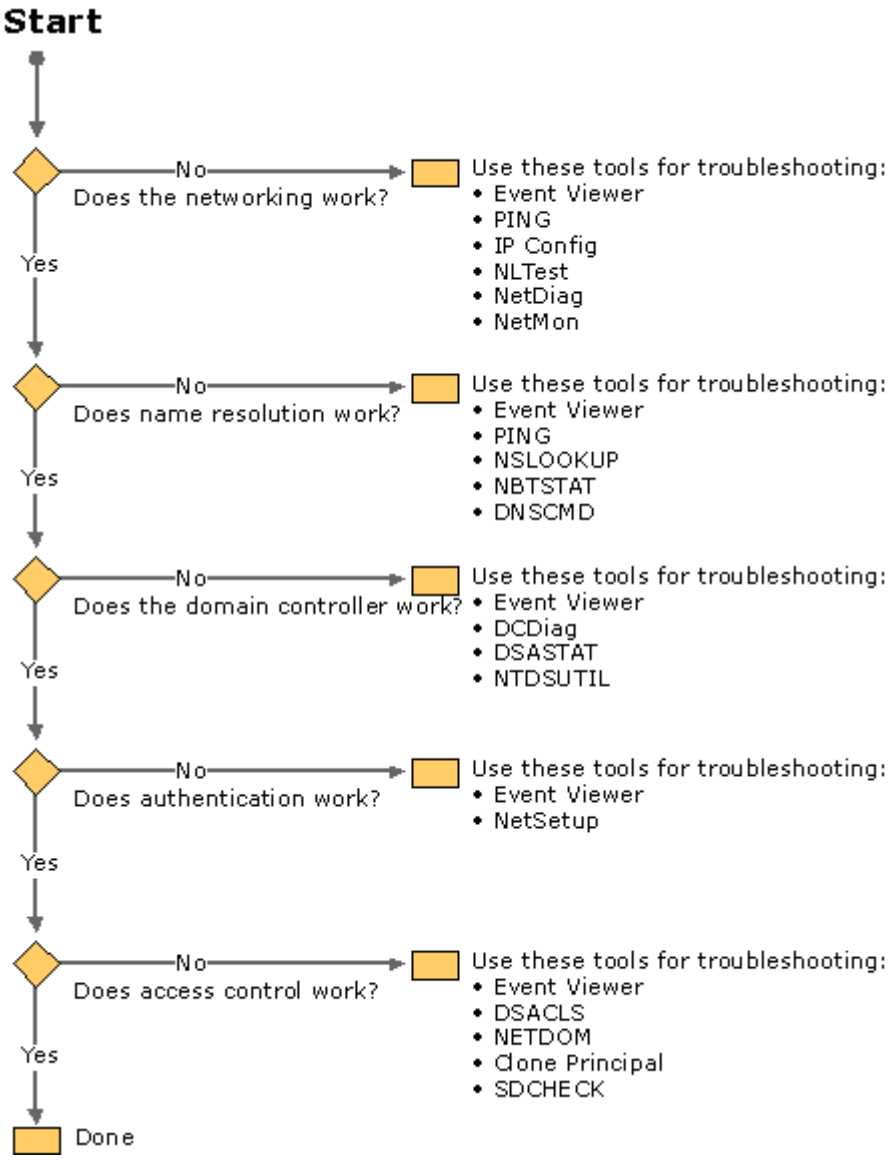
[1]These issues are not covered in this document. Refer to Microsoft documentation for additional information.

The following flowchart shows the sequence of events that must be followed to identify, analyze the cause of, and repair AD problems. This sequence serves as a roadmap to help accurately identify a situation, diagnose it, and then resolve it. In each step, a few tools are recommended that can be used to further help to nail down the problem.

Active Directory Troubleshooting Prerequisites

To troubleshoot Active Directory and Domain Security issues follow the following Microsoft provided troubleshooting sequence:

Figure 37: Troubleshooting Flowchart



If you have an Active Directory issue, consult your local AD administrator to perform the following prior to contacting Cisco TAC:

Step 1 Follow the steps indicated in the flowchart above.

Step 2 Check the results for errors.

Note: Save the results in the TAC case.

Step 3 Ensure you have the following information on hand:

- Domain topology (number of domains and their relationships)
- Sites per domain
- Domain Controllers per site
- Role of each Domain Controller (placement of Global Catalogs in particular)

This preliminary information provides Cisco TAC with better insight into your system and potential causes of the problem. The log from the dcdiag is a useful tool in identifying the cause. Dcdiag is part of the Microsoft Support Tools suite and is usually found on the Windows Server media under the *support* folder and must be installed.

Cisco recommends you have knowledge of the following topics prior to troubleshooting Active Directory issues on your ICM system:

- Active Directory
- ICM Active Directory setup

Note: The information in this document is based on ICM 7.0(0), or later, running on a Windows 2003 Server.

Troubleshooting Hints

The following troubleshooting situations are provided to assist in resolving commonly occurring issues.

Setup impacted by domain problems

Symptom:

Setup takes a long time to complete and appears not to be making any progress. Avoid exiting prematurely and wait for setup to complete.

Message:

None.

Cause:

If setup is run on a component requiring a service account, setup can take around 30 minutes to create the account if the domain is not properly configured, or the domain is not functioning properly.

Action:

Let setup complete and do not cancel the operation. Fix any domain problems so that subsequent attempts to run setup will not take as long.

User login before replication can result in service install failure #1

Symptom:

If a user is given setup permissions on a Domain where there are Domain Controllers in different sites, and the user logs onto a machine before replication of user permissions has completed, setup may experience errors.

Message:

None.

Cause:

The user does not have setup permissions for a specific instance.

Action:

Check the setup group in the instance OU on all of the Domain Controllers and wait until the user has been replicated to all of them. After the user has been replicated, logout of the machine and then log back in. This resets the user permissions. Now you are able to run setup with no issues.

User login before replication can result in service install failure #2

Symptom:

If a user is given setup permissions on a Domain where there are Domain Controllers in different sites, and the user logs onto a machine before replication of user permissions has completed, setup may experience errors.

Message:

Setup failed to add the Distributor, Logger, Jaguar, and/or Tomcat service accounts for the instance [*InstanceName*]

Cause:

This error is only be seen when installing a Distributor or Logger.

Action:

Check the setup group in the instance OU on all of the Domain Controllers and wait until the user has been replicated to all of them. After the user has been replicated, reset user permissions by logging out and then logging back in.

Domain Controller not supported

Symptom:

Unable to collocate the Domain Controller and ICM 7.0(0).

Message:

None.

Cause:

Collocating ICM 7.0(0), or later, on a Domain Controller is not supported.

Action:

The Domain Controller must be on a dedicated server with no additional applications collocated on it.

Reasons to isolate the Domain Controller function include

- Security

  This is the most important reason.

  Running SQL Server on a Domain Controller puts the entire Active Directory infrastructure at risk, thus placing the entire deployment at risk. Microsoft, as well as others in the industry, strongly recommend against installing SQL Server on a Domain Controller. Most require isolation of services as a method of secure server deployments.

- Performance

  While negligible for small deployments with few servers, the demands placed on the Domain Controller when the number of domain member services and users grows, can have a negative impact on the core functions of these systems.

- Automated Security Hardening is not applied to a server that is found to be a Domain Controller.

Cisco ICM services intermittently fail to start when set to Automatic

Symptom:

The system is in an Active Directory domain and was just rebooted. Some Cisco ICM services do not start correctly.

Message:

None.

Cause:

Cisco ICM services do not start correctly due to login failure.

Action:

There are two possible workarounds for this problem:

1. Open the ICM Service Control or the Windows Services Control and manually start the services that failed to start.
2. Remove the system from the domain, then re-add the system from the domain. All ICM services should start correctly.

Setup appears to hang while upgrading database if Domain Controller down

Symptom:

ICM/IPCC Setup appears to hang while upgrading the database on the Logger or AW components .

Message:

None.

Cause:

This may occur while installing or upgrading to ICM/IPCC 7.0(0), or while running local setup. Only occurs when a Domain Controller is down or has been removed.

Action:

Perform the following workaround:

1. Use diagnostics supplied by Microsoft (see Troubleshooting Tools (page 155)) to find problems with DNS.
2. Check the DNS Forward zones and Reverse Zones for all Domain Controllers in the domain (Root and Child Domain Controllers) for any reference(s) to Domain Controllers that no longer exist.
3. If a Domain Controller is down, attempt to bring it up (if possible).
4. If a Domain Controller can not be brought up, try to remove the Domain Controller from any domain controller DNS Forward zones and Reverse Zones.

5. Rerun Setup.

ICM Setup executes a routine to verify each ICM user exists in the domain when doing an Upgrade All or editing a ICM component such as the AW or Logger. This problem can also occur when installing ICM 7.0 or later. The routine executes a Microsoft Active Directory call to determine if the Domain Controller is active. If the Domain Controller is down or no longer exists, the MS Active Directory call waits until the call times out. This increases the time needed to verify a user exists, so ICM Setup appears to be hanging.

User List tool permissions checkboxes not checked in multiple domain scenarios

Symptom:

Permissions checkboxes not checked.

Message:

None.

Cause:

In a multiple domain scenario, the User List tool permissions checkboxes (Setup, Config and WebView) may not be checked.

This is not a caveat if all of the following are true:

- The deployment is split between two or more domains, such as the CICM and the Customer domain for Hosted customers.
- The User List tool is used from two or more AWs that are in different domains.
- The user is added via the User List tool on domain 1 and the retrieved via user list tool on domain 2.

This is because the User List tool only scans the local domain (D1, the domain on which the tool is invoked) for ICM permissions. Since the ICM database is common to all AWs for an instance, if the User List tool is invoked from an AW in a different domain (D2), all users are displayed, but only permissions from the local domain (D1) are displayed. No permissions for the second domain (D2) are displayed because the users do not have permission(s) in that domain.

Action:

None, as this is normal operation in this case.

Appendix A

Installing the Domain Controller on Windows 2003

How to Install the Domain Controller on Windows 2003

Prior to 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 Select **Start** > **Run** > **`dcpromo.exe`** > **OK**.

Step 2 Click **Next** through the Active Directory Wizard screens until you reach the *Domain Controller Type* screen.

Step 3

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 4 Click **Next**.

The *Create New Domain* screen appears.

Step 5

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: Refer to Supported Domain Models (page 21).

Step 6 Click **Next**.

The *New Domain Name* screen appears.

Step 7 Enter the DNS name. The DNS name must have a suffix. You may use whatever you want for a suffix (examples, .com, .icm, .ipcc, .lab - if this is a corporate domain installation, follow these guidelines).

Step 8 Click **Next**.

The *NetBIOS Domain Name* screen appears.

Step 9 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 10 Click **Next** until the *DNS Registration Diagnostics* screen appears.

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

Step 11 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: Active Directory DNS servers must be in the DNS path for each server. This is accomplished by pointing directly to the Active Directory servers or by having other DNS servers forward to the DNS servers.

Step 12 Click **Next** through the end of the wizard, then click **Finish**.

Step 13 When prompted, restart Windows.

Appendix B

Moving the Cisco Root OU

Introduction

This document describes the instructions to safely move the Cisco Root Organizational Unit (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 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 7.0(0) of ICM software.

Definitions

Cisco Root OU

The OU containing all ICM created domain resources. It defines the permissions for all 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 ICM related tasks.

Requirements and Prerequisites

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

- The OU may only be transferred to a new location within the same domain.
- All 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 ICM Instance on the system.

Best Practices to Avoid Problems

Perform the following to avoid problems:

1. Stop all ICM services before removing the OU.
2. Reset the permissions for the users, using the User List tool.
   - Rerun Local Setup (**ICMSetup.exe** from the icm\bin directory) or Media Setup.

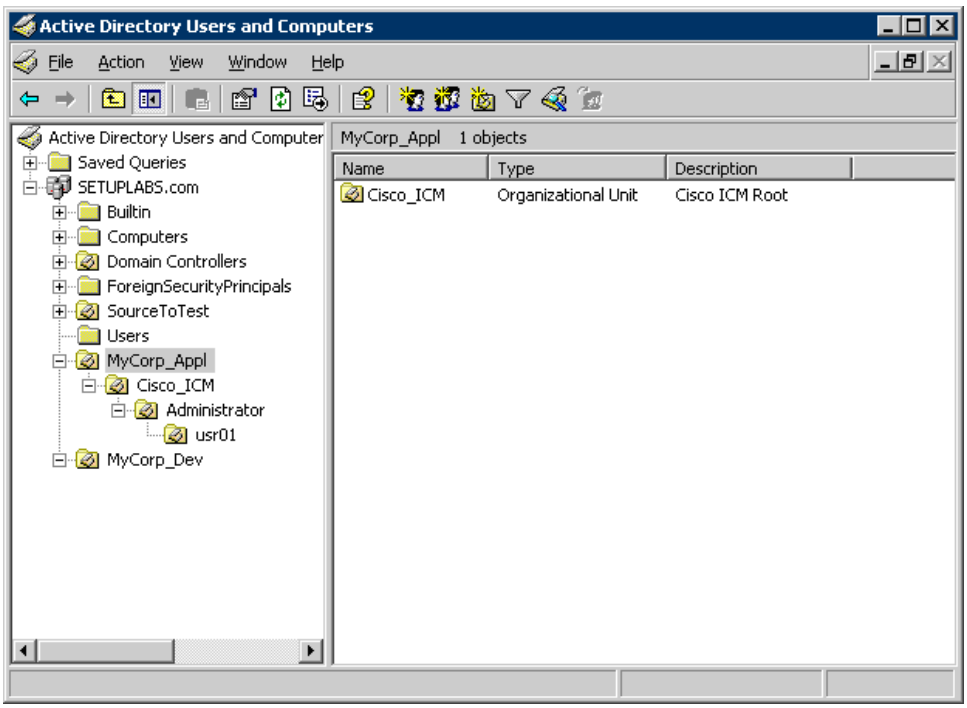
     If Local Setup is run, edit each component of each instance to reset the service account to this new OU.

     If Media Setup is run, run **Upgrade All**.
   - Start all ICM services.
   - Run the **Configuration Manager** tool.
   - 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.

How to transfer the Cisco Root OU to another OU

As an example, refer to 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 38: SETUPLABS Domain



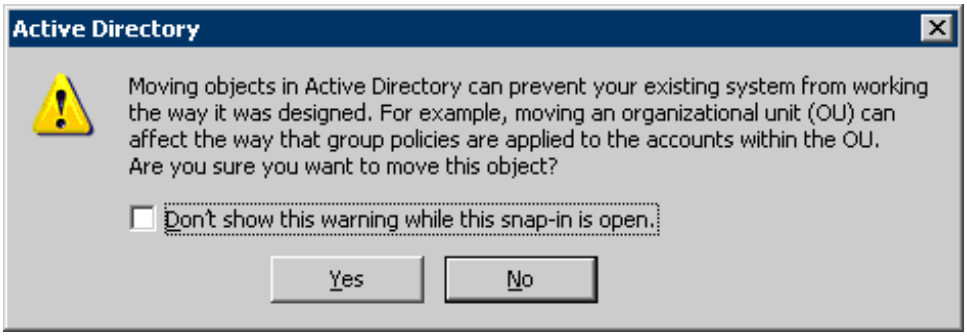
Step 1 On the Domain, find the OU in which the Cisco Root OU is contained.

Step 2 Stop All ICM Services and Applications on the 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.

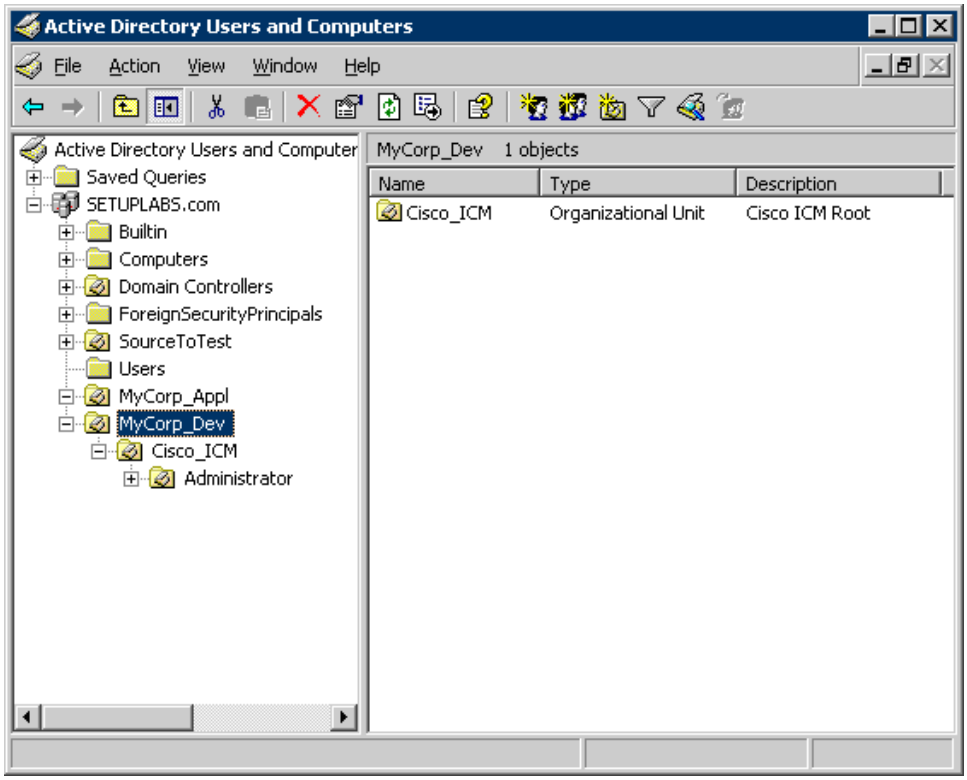
Figure 39: AD Moving Objects Error Message



Step 4 Click **Yes** to continue.

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

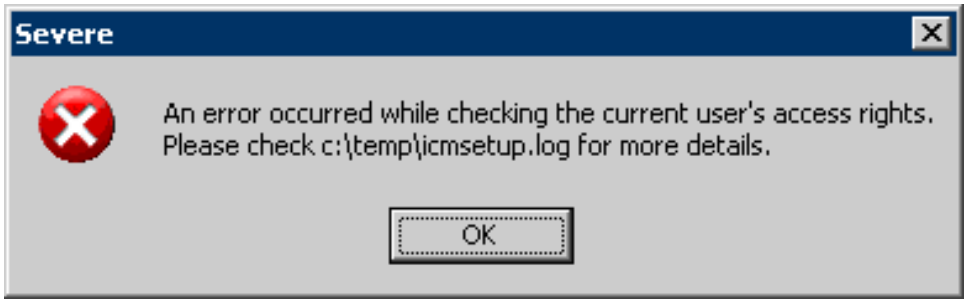
Figure 40: Cisco Root OU Location



Step 5 On the ICM System, run Local Setup (**ICMSetup.exe** from the icm\bin directory).

Setup displays the following message box.

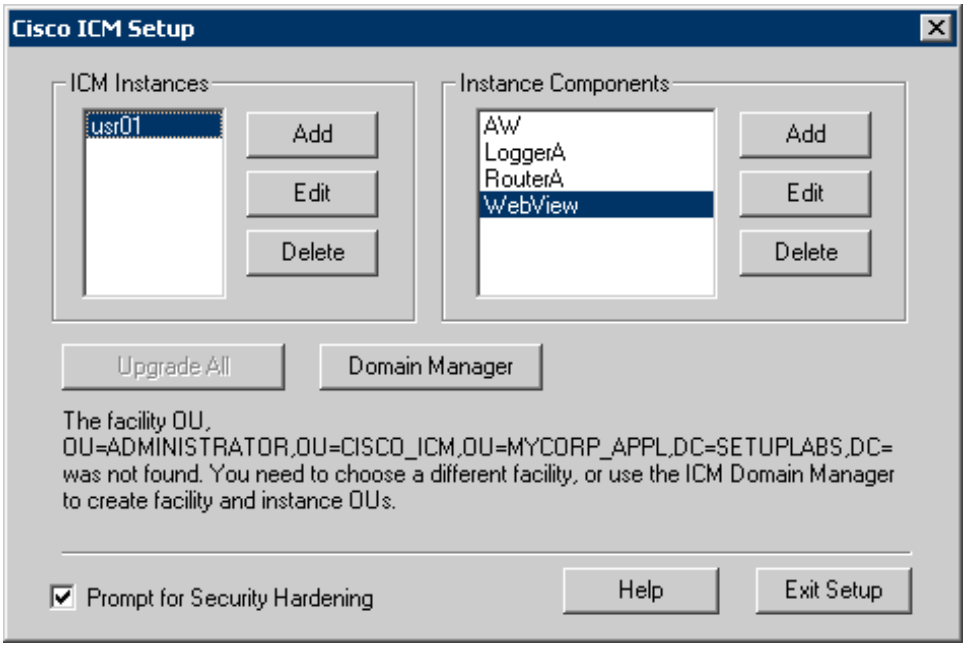
Figure 41: Setup Error Message



Step 6 Click **OK**.

The ICM Setup dialog is displayed.

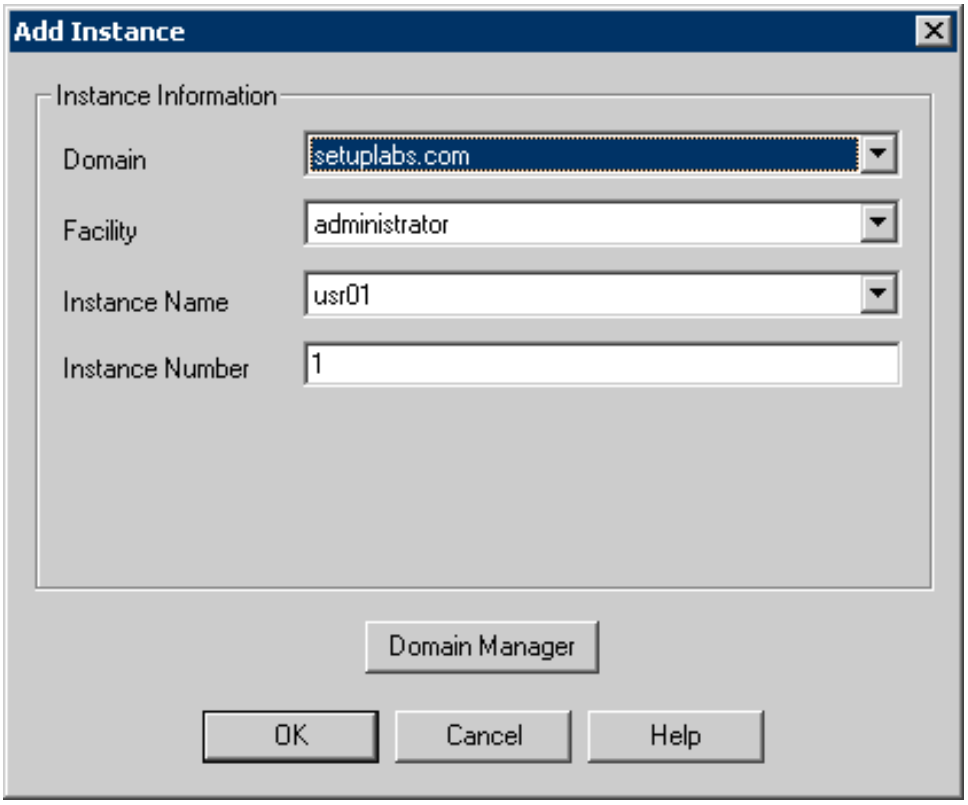
Figure 42: ICM Setup Dialog Box



Step 7 Click **Add** on the ICM Instances group box.

The Add Instance dialog is displayed.

Figure 43: Add Instance Dialog Box



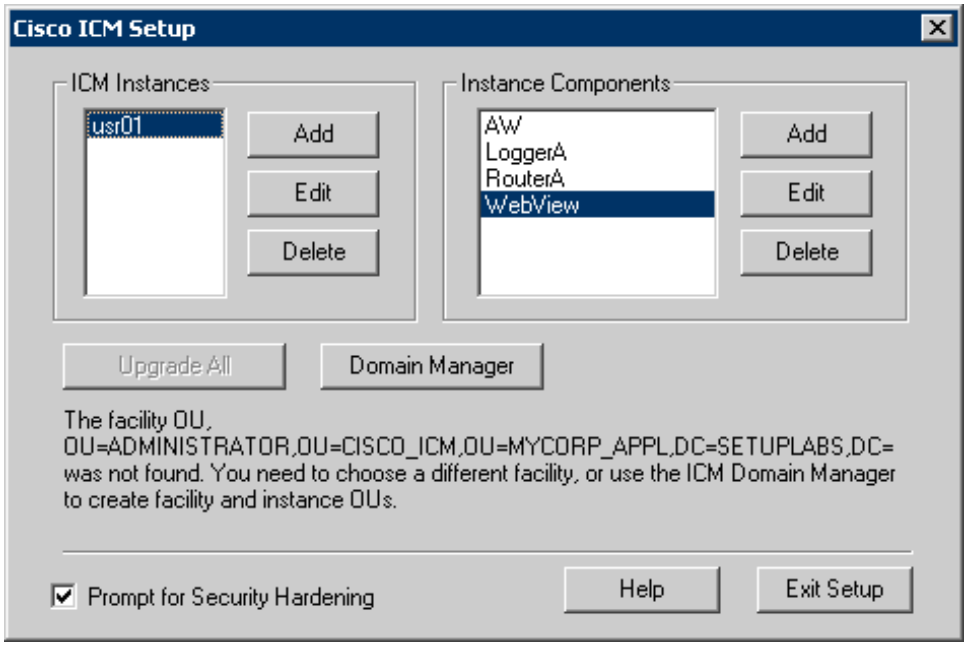
Step 8 Click **OK** to accept the default Instance Number.

Step 9 Exit Setup.

Step 10 Rerun Local Setup (**ICMSetup.exe** from the icm\bin directory) .

The ICM Setup dialog appears.

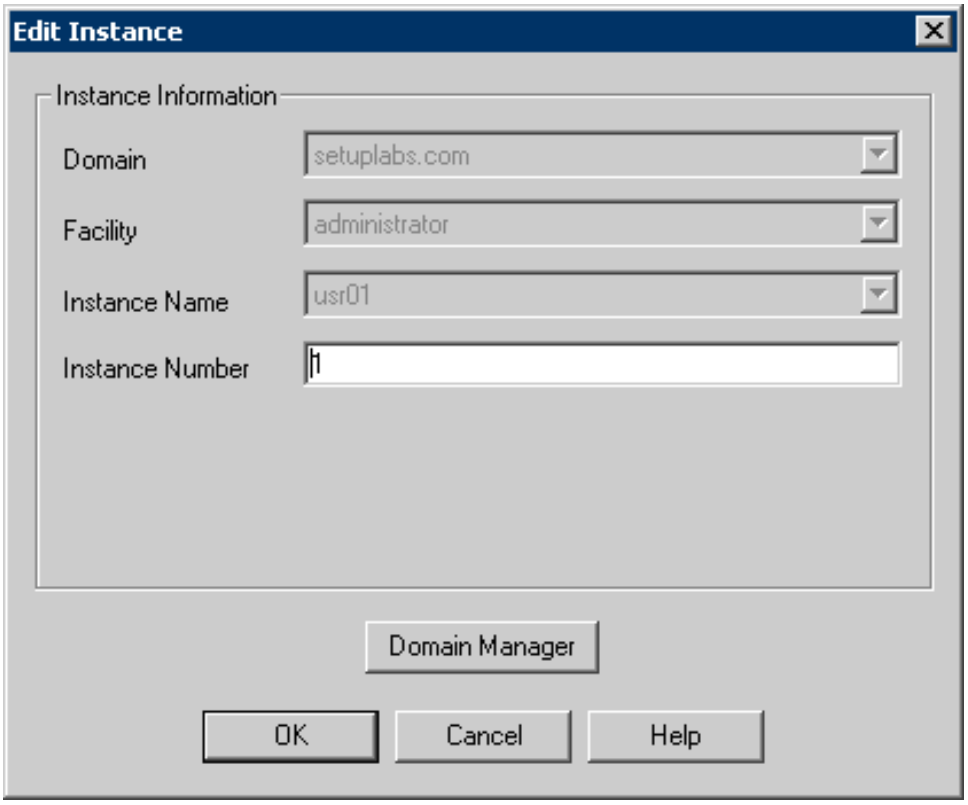
Figure 44: ICM Setup Dialog Box



Step 11 Click **Edit** on the ICM Instances group box.

The Edit Instance dialog is displayed.

Figure 45: Edit Instance Dialog Box



Step 12 Change the **Instance Number** to whatever number existed before, then click **OK**.

Step 13 Start all 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.

Appendix C

Migrating ICM Servers from Multiple Forest to Single Forest for ICM/IPCC 5.0(0) Hosted

Synopsis

Cisco ICM, IPCC Enterprise and Hosted solution utilizes Microsoft Active Directory for ICM user authentication and resource access control. Active Directory can be deployed in various topologies such as single or multiple trees, and single or multiple forests. Cisco requires that ICM must be deployed in a single forest Active Directory topology, simplifying to single domain or tree whenever possible. This document iterates the steps required to move ICM components between domains.

Note: Before starting the migration from separate forest to single forest or single domains, **Cisco supports Central Controllers only in a single domain configuration**. Do not bring up the CICM SideA while the CICM SideB is in another domain. Cisco recommends moving CICM SideA first, then SideB and then starting the ICM components.

Migration Process Overview

Perform the upgrade in the following order:

- Stop all ICM services on SideA.
- Migrate the SideA CallRouter/Logger to the new Domain as described in the following sections.
- Stop all ICM services on SideB.
- Start all ICM services on SideA.

- Run Setup and edit the AW/Distributor instance to select the new domain for the Central Controller.
- Migrate the SideB CallRouter/Logger to the new domain as described in the following sections.
- Start all ICM services on SideB.

Common Steps Required before Migrating any ICM Component

On the Domain Controllers:

Step 1 Confirm that Domain Controllers have been upgraded from NT Domain to Windows 2000 Active Directory

On the CallRouter Server:

Step 2 \RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance.

Note: If moving a CICM with SideA and SideB disable the Configuration changes on both sides.

On the Logger server:

Step 3 Copy the Domain Conversion Tool (DomCvt.exe) from the ICM 5.0(0) or ICM 6.0(0) Third-Party Tools CD as applicable (Domain Conversion Utility folder) onto the Logger server.

Step 4 Export the ICM user list using the DomCvt tool using the following command: **domcvt /DB:** <*instancename*>**_sideA /F:c:\DomConvert\userlist.txt /M:E**.

ICM 5.0(0) Hosted to 7.0 (0) Hosted Upgrade SQL Permissions Issue

When an upgrade from ICM 5.0(0) Hosted to 7.0 (0) Hosted environment is planned, Cisco requires that ICM must be deployed in a single forest Active Directory topology, simplifying to single domain (or tree) whenever possible. In order to meet this requirement, you must move the ICM 5.0 systems to a single forest before upgrading to ICM 7.0(0).

By running the Domain Conversion tool on the Logger system, the attributes of the users added through the User List tool are retained after the users are migrated to the new domain. However, while the users were successfully migrated to the new domain, Configuration Manager tool users are unable to open the Configuration Manager in the new domain, and therefore are unable to make any configuration changes.

When a newly migrated user tries to open the Configuration Manager tool, an error stating "(-9986) Session to local database could not be opened" is displayed. This occurs because the user logged on to the AW system does not have SQL DB access on the ICM 5.0 AW system. While this can be resolved by manually providing SQL permission to the user, it can be a tedious process if it needs to be done for all Configuration Manager users.

How to Grant SQL Permissions

A new tool to be run on the AW system resolves this issue. This tool must be run before upgrading to ICM 7.0 system in order to grant the correct SQL permission to all the migrated Configation Manager tool users.

Step 1 Run the DomCvt Tool on the Logger Server using the command: **domcvt /DB:**<*instancename*>**_sideA /F:c:\DomConvert\Userlist.txt /M:E**

The output file (Userlist.txt) is created in the c:\DomConvert folder. This file has all the information of the migrated users.

Step 2 Create the folder **C:\DomConvert**.

Step 3 Copy the Userlist.txt file from the c:\DomConvert folder on the Logger system, to the C:\DomConvert folder on the AW system.

Step 4 Run the new tool by entering the following command: **SetSQLAccess /f:c:\DomConvert**

All the Configuration Manager tool users listed in the userlist.txt file are granted appropriate SQL permissions.

Logger (Common Ground)

Prerequisite:

Step 1 Ensure the Common Steps Required before Migrating any ICM Component (page 178) were followed before proceeding further.

On the Logger Server:

Step 2 Shutdown the ICM Logger service.

Step 3 Set the ICM Logger service to **Manual**. This ensures the Logger service is not started when moving the server from the old domain to the new domain.

Step 4 Remove all installed ICM service releases and engineering specials.

Note: Make a note of all the installed service releases and engineering specials, as these need to be reinstalled later.

Step 5 Backup the ICM sideA (or sideB) database and the Outbound database.

Step 6 Backup the ICM registry (HKLM\Software\Cisco System, Inc. registry hive).

Step 7 If not at MS SQL 2000 or SQL 2005 as applicable, upgrade to it.

Step 8 Backup the upgraded MS SQL version of the ICM sideA (or sideB) database and the Outbound database.

Step 9 Detach the ICM sideA (or sideB) database and the Outbound database.

Step 10 Uninstall MS SQL.

Step 11 Take the server out of the domain.

Step 12 Check the TCP/IP properties of the server to ensure the DNS server is pointing to the new domain.

a. Select **Advanced** to bring up the Advanced TCP/IP Settings.

b. On the Advanced TCP/IP Settings dialog, select the **DNS** tab.

c. On the DNS Tab, check **Append these DNS suffixes** and enter the new and old DNS suffixes.

Note: The new domain must be first followed by the old domain.

Step 13 Put the server into the new domain.

The new domain can be configured as a:

- Single Domain: The NAM domain.
- Single Tree: A child domain of the NAM domain.
- Single Forest: Any domain in the same forest as the NAM domain, such as a new tree root.

Step 14 Reinstall MS SQL and the supported SQL service pack.

Step 15 Reattach the ICM sideA (or B) database and the Outbound database.

Step 16 Rerun ICM Setup from the media, then:

- Edit the instance to correct the domain name.
- Edit through the ICM components.

Step 17 Install all the ICM service releases and engineering specials installed prior to the domain migration.

Step 18 Set the Logger service back to **Automatic**.

The ICM services are now installed and ready to be started.

Step 19 Continue to migrate the other components and wait for the cut over before starting the ICM services.

CallRouter (Common Ground)

Prerequisite:

Step 1 Ensure the Common Steps Required before Migrating any ICM Component (page 178) were followed before proceeding further.

On the CallRouter Server:

Step 2 Shutdown the ICM Router service.

Step 3 Set the ICM Router service to **Manual**. This ensures the Router service is not started when moving the server from old domain to the new domain.

Step 4 Backup the ICM registry (HKLM\Software\Cisco System, Inc. registry hive).

Step 5 Remove all installed ICM service releases and engineering specials.

Note: Make a note of all the installed service releases and engineering specials, as these need to be reinstalled later.

Step 6 Take the server out of the domain.

Step 7 Check the TCP/IP properties of the server to ensure the DNS server is pointing to the new domain.

a. Select **Advanced** to bring up the Advanced TCP/IP Settings.

b. On the Advanced TCP/IP Settings dialog, select the **DNS** tab.

c. On the DNS Tab, check **Append these DNS suffixes** and enter the new and old DNS suffixes.

Note: The new domain must be first followed by the old domain.

Step 8 Put the server into new domain (the same domain as the Logger).

Step 9 Rerun ICM Setup from the media, then edit through the ICM components.

Step 10 Install all the ICM service releases and engineering specials installed prior to the domain migration.

Step 11 Set the Router service back to **Automatic**.

The ICM services are now installed and ready to be started.

Step 12 Continue to migrate the other components and wait for the cut over before starting the ICM services.

AW without WebView (Common Ground)

Prerequisite:

Step 1 Ensure the Common Steps Required before Migrating any ICM Component (page 178) were followed before proceeding further.

On the AW Distributor Server:

Step 2 Shutdown the ICM Distributor service.

Step 3 Set the ICM Distributor service to **Manual**. This ensures the Distributor service is not started when moving the server from old domain to the new domain.

Step 4 Remove all installed ICM service releases and engineering specials.

Note: Make a note of all the installed service releases and engineering specials, as these need to be reinstalled later.

Step 5 Backup the ICM database (AW DB).

Step 6 Backup the ICM registry (HKLM\Software\Cisco System, Inc. registry hive).

Step 7 If not at MS SQL 2000 or SQL 2005, upgrade to it.

Step 8 Backup the upgraded MS SQL version of the ICM database (AW DB).

Step 9 Uninstall MS SQL.

Step 10 Take the server out of the domain.

Step 11 Check the TCP/IP properties of the server to ensure the DNS server is pointing to the new domain.

a. Select **Advanced** to bring up the Advanced TCP/IP Settings.

b. On the Advanced TCP/IP Settings dialog, select the **DNS** tab.

c. On the DNS Tab, check **Append these DNS suffixes** and enter the new and old DNS suffixes.

Note: The new domain must be first followed by the old domain.

Step 12 If the AW is collocated with the domain controller, demote the domain controller using the dcpromo tool.

Step 13 Put the server into the new domain.

The new domain can be configured as a:

- **Single Domain**: The Central Controller domain.
- **Single Tree**: A child domain of the Central Controller domain.
- **Single Forest**: Any domain in the same forest as the Central Controller domain, such as a new tree root.

Step 14 Reinstall MS SQL and the supported SQL service pack.

Step 15 Rerun ICM Setup from the media.

a. Edit the instance and change the domain to point to the Central Controller domain.

Note: Required only if Central Controller Domain has changed.

b. Edit through the ICM components.

Step 16 Set the ICM Distributor service to **Automatic**.

Step 17 Install all the ICM service releases and engineering specials installed prior to the domain migration.

On the Logger server:

Step 18 Run the Domain Conversion Tool to convert the ICM users exported earlier, using the following command: **domcvt /DB:** <*instance_name*>**_sideA /F:c:\DomConvert\userlist.txt /M:C /OD:** <*old_domain_netbios_name*> **/ND:** <*new_domain_netbios_name*>

Note: You can use the /p option to create a global password. If you do not use the /p option, the password is reset to null.

On the Distributor server:

Step 19 Start the ICM Distributor service.

Step 20 Initialize the ICM database (AW DB).

AW with WebView (Common Ground)

Prerequisite:

Step 1 Ensure the Common Steps Required before Migrating any ICM Component (page 178) were followed before proceeding further.

On the AW Distributor Server:

Step 2 Shutdown the ICM Distributor service, IIS and the Jaguar service.

Step 3 Set the ICM Distributor service to **Manual**. This ensures the Distributor service is not started when moving the server from old domain to the new domain.

Step 4 Remove all installed ICM service releases and engineering specials.

Note: Make a note of all the installed service releases and engineering specials, as these need to be reinstalled later.

Step 5 Backup the ICM database (AW/HDS/WV DB).

Note: If HDS backup is not required then just back up and start with a fresh HDS.

Step 6 Backup the ICM registry (HKLM\Software\Cisco System, Inc. registry hive).

Step 7 If you have custom Webview templates, backup the \icm\<instances>\aw folder.

Step 8 If not at MS SQL 2000 or SQL 2005, upgrade to it.

Step 9 Backup the upgraded MS SQL version of the ICM databases (AW/HDS/WV DB).

Step 10 Detach the ICM AW/HDS/WV Databases.

Step 11 Uninstall MS SQL.

Step 12 Uninstall ICM 3rd party software.

Note: If there are problems with uninstalling the 3rd party software, follow the Technology Refresh procedure following.

Step 13 Take the server out of the domain.

Step 14 Check the TCP/IP properties of the server to ensure the DNS server is pointing to the new domain.

a. Select **Advanced** to bring up the Advanced TCP/IP Settings.

b. On the Advanced TCP/IP Settings dialog, select the **DNS** tab.

c. On the DNS Tab, check **Append these DNS suffixes** and enter the new and old DNS suffixes.

Note: The new domain must be first followed by the old domain.

Step 15 If the AW is collocated with the domain controller, demote the domain controller using the dcpromo tool.

Step 16 Put the server into the new domain.

The new domain can be configured as a:

- **Single Domain**: The Central Controller domain.
- **Single Tree**: A child domain of the Central Controller domain.

- **Single Forest**: Any domain in the same forest as the Central Controller domain, such as a new tree root.

Step 17 Reinstall MS SQL 2000 or SQL 2005 and the supported SQL service pack.

Step 18 Reattach the HDS and WVDB databases.

Step 19 Reinstall the ICM 3rd Party software.

Step 20 Rerun ICM Setup from the media.

a. Edit the instance and change the domain to point to the Central Controller domain.

Note: Required only if Central Controller Domain has changed.

b. Edit through the ICM components.

Step 21 Set the ICM Distributor service to **Automatic**.

Step 22 Install all the ICM service releases and engineering specials installed prior to the domain migration.

On the Logger server:

Step 23 Run the Domain Conversion Tool to convert the ICM users exported earlier, using the following command: **domcvt /DB:** <*instance_name*>**_sideA /F:c:\DomConvert\userlist.txt /M:C /OD:** <*old_domain_netbios_name*> **/ND:** <*new_domain_netbios_name*>

Step 24 Start IIS, the Jaguar service and ICM Distributor service. Check for error messages. If Jaguar/Webview does not work properly, follow the following Technology Refresh procedure.

Note: You can use the /p option to create a global password. If you do not use the /p option, the password is reset to null.

On the Distributor server:

Step 25 Initialize the database.

AW with WebView (Technology Refresh, on New or Existing Hardware)

Prerequisite:

Step 1 Ensure the Common Steps Required before Migrating any ICM Component (page 178) were followed before proceeding further.

On the AW Distributor Server:

Step 2 Shutdown the ICM Distributor service, IIS and the Jaguar service.

Step 3 Set the ICM Distributor service to **Manual**. This ensures the Distributor service is not started when moving the server from old domain to the new domain.

Step 4 Remove all installed ICM service releases and engineering specials.

Note: Make a note of all the installed service releases and engineering specials, as these need to be reinstalled later.

Step 5 Backup the ICM database (AW/HDS/WV DB).

Note: If HDS backup is not required then just back up and start with a fresh HDS.

Step 6 Backup the ICM registry (HKLM\Software\Cisco System, Inc. registry hive).

Step 7 If you have custom Webview templates, backup the \icm\<instances>\aw folder.

Step 8 If not at MS SQL 2000 or SQL 2005, upgrade to it.

Step 9 Backup the upgraded MS SQL version of the ICM database (AW DB).

Step 10 Begin a fresh installation.

Step 11 Put the server into the new domain.

The new domain can be configured as a:

- **Single Domain**: The Central Controller domain.
- **Single Tree**: A child domain of the Central Controller domain.
- **Single Forest**: Any domain in the same forest as the Central Controller domain, such as a new tree root.

Step 12 Install MS SQL 2000 or SQL 2005 and the supported SQL service pack.

Step 13 Install the ICM 3rd Party software.

Step 14 Copy the backed up ICM registry, database and custom template folder.

Step 15 Restore the HDS and WV databases (not the AW DB) on the same drive.

Step 16 Rerun ICM Setup from the media.

a. Edit the instance and change the domain to point to the Central Controller domain.

Note: Required only if Central Controller Domain has changed.

b. Edit through the ICM components.

Step 17 Set the ICM Distributor service to **Automatic**.

Step 18 Install all the ICM service releases and engineering specials installed prior to the domain migration.

On the Logger server:

Step 19 Run the Domain Conversion Tool to convert the ICM users exported earlier, using the following command: **domcvt /DB:** <*instance_name*>**_sideA /F:c:\DomConvert\userlist.txt /M:C /OD:** <old_domain_netbios_name> **/ND:** <*new_domain_netbios_name*>

Note: You can use the /p option to create a global password. If you do not use the /p option, the password is reset to null.

On the Distributor server:

Step 20 Start IIS, Jaguar and the ICM Distributor service.

Step 21 Initialize the database.

Migrating AWs in Different Domains

Step 1

Step 2

Step 3

Common Steps after Migrating All ICM Components

On the Router server:

Step 1 Re-enable configuration changes by changing the following registry key from 1 to 0: **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM**<*instance_name*>**\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance**.

Step 2 Using the ICM User List tool, ensure all users were migrated correctly.

Synopsis

Glossary

Active Directory

A Microsoft service that provides a central repository for managing network resources. ICM software uses Active Directory to control users' access rights to perform setup, configuration, and reporting tasks.

Config Security Group

The Security Group that controls access privileges to the common ICM software configuration tasks.

DCDiag

The Microsoft tool used to analyze the state of a domain controller in a forest or enterprise and to report any problems. This tool analyzes the domain controller's functions and interactions across an entire enterprise.

DNSCMD

The Microsoft tool used to view properties of DNS servers, zones, and resource records.

DSACLS

The Microsoft tool used to view the security descriptor of an Active Directory object. The security descriptor for an object includes the Access Control List (ACL).

DSASTAT

The Microsoft tool used to compare and detect differences between directory partitions on domain controllers. The DSASTAT tool monitors replication status at a higher level than monitoring detailed transactions.

Event Viewer

The Microsoft tool that provides access to Application, Security, System, and DNS Server logs for the computer.

Facility Organizational Unit

A group of Instance OUs 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.

Instance Organizational Unit

The Active Directory representation of an ICM instance. You define permissions for that instance as part of that Instance OU. Each ICM instance has an associated Instance OU.

IPCONFIG

The Microsoft tool used to examine the computer's IP address, subnet mask, default gateway, and DNS servers and to ensure that these networking values are set correctly.

NBTStat

The Microsoft tool used to display protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP.

NetDiag

The Microsoft tool used to check that the client computer is functioning properly. This tool helps isolate networking and connectivity problems.

NETDOM

The Microsoft tool used to manage computer accounts for member workstations and member servers.

NSLookup

The Microsoft tool used to perform DNS queries and to examine the contents of zone files on local and remote servers.

NTDSUTIL

The Microsoft tool used for directory service management.

Organizational Unit

A container in the Active Directory domain that can contain other OUs, as well as users.

Ping

The Microsoft DOS command used to check the computer's network connections to other computers.

Root Organizational Unit

The Organizational Unit that contains all ICM-related organizational units in the domain.

SDCheck

The Microsoft tool used to verify that ACL entries are correctly propagated through parent-child relationships. The SDCheck utility allows you to determine if ACLs are inherited correctly and replicated from one domain controller to another.

Security Group

A collection of domain users to whom you grant a set of permissions to perform tasks with ICM software.

Services Security Group

A Security Group that is generated automatically for Instance Organizational Units. The Services Security Group controls access between ICM software components.

Setup Security Group

The Security Group that controls access to the ICM software Setup program as well as the Active Directory Domain Manager.

System Design Specification

A staging document based on a template that defines the intended ICM software deployment.

WebView Security Group

The Security Group that controls access to the WebView reporting application. Users who are members of the WebView Security Group can access WebView and generate reports at the current level of the OU hierarchy and below.

Index