Active Directory and ICM/CCE

- Active Directory for Unified ICM/CCE, page 1
- Active Directory Support by Unified CCE, page 2
- Benefits of Active Directory, page 2
- Active Directory and Microsoft Windows Server, page 3

Active Directory for Unified ICM/CCE

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

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

Note

This document does not provide detailed information on AD. Unified ICM administrators must be familiar with the Microsoft AD documentation on the Microsoft Windows Server website.

Note

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

Single Sign On (SSO) Support

SSO allows users to sign in to one application and then securely access other authorized applications without a prompt to resupply user credentials. As an agent or supervisor, when you login to a Unified CCE solution web component using a username and password, SSO provides a security token that allows you to securely
access all other web based application and services need not provide your login credentials repeatedly from the same web browser instance. If you move to a different browser you need to re-authenticate the SSO.

Unified CCE Solution requires an Identity Provider (IdP) to interface with Microsoft Active Directory (AD). Irrespective of the IdP used to interface with the identity source, the Active Directory infrastructure is a mandatory component for SSO. In an SSO deployment, AD is still required to support Unified CCE administrator sign-ins.

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

Single sign-on (SSO) is an authentication and authorization process. (Authentication proves that you are the user you say that you are, and authorization verifies that you are allowed to do what you are trying to do.) SSO allows users to sign in to one application and then securely access other authorized applications without a prompt to resupply user credentials. SSO permits Cisco supervisors or agents to sign on only once with a username and password to gain access to all of their Cisco browser-based applications and services within a single browser instance. By using SSO, Cisco administrators can manage all users from a common user directory and enforce password policies for all users consistently.

To enable SSO, the Unified CCE solution requires an Identity Provider (IdP) in addition to Active Directory (AD). The IdP stores user profiles and provides authentication services to support SSO sign-ins to the contact center solution. However, the IdP does not replace AD. In an SSO deployment, AD is still required to support Unified CCE administrator sign-ins.

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

**Active Directory Support by Unified CCE**

Unified CCE to facilitate the upgrade from the release earlier than 11.x, Unified ICM/CCE supports active directory on Windows Server 2008 R2 and 20012 R2.

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


**Benefits of Active Directory**

**Support for Corporate Domain Installations**

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

**Related Topics**

- What Is an OU?
No Domain Administrator Requirement

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

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

For more information, see the chapter Domain Manager.

Flexible and Consistent Permissions

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

You can grant these privileges to any trusted AD user.

Streamlined Administration

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

Standard Windows Naming Conventions

AD supports standard Windows naming conventions.

By default, there are no specific naming requirements for the Unified ICM usernames or the domain name. Certain features, like SSO, can impose requirements. Check the feature documentation for details.

Active Directory and Microsoft Windows Server

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

See Microsoft's documentation at https://docs.microsoft.com/en-us/windows-server/windows-server-versions for details on setting up Windows Server.

Active Directory Domain Services

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

RWDC Authentication

The Unified ICM/CCE application user must be authenticated if the client machines are connected to RWDC.
RWDC LDAP Read

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

RWDC LDAP Write

Unified ICM/CCE must perform the LDAP Write operation successfully when the client is connected to a RWDC. LDAP Write operations occur when Unified ICM/CCE Configuration applications issue LDAP ADSI calls to write the data to the Active Directory.

RWDC Password Change

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

Restartable Active Directory Domain Services

Previously, there was no provision to restart Active Directory separately. As a part of this new enhancement, you can stop and restart the Active Directory Domain Services without restarting the domain controller. Currently, appropriate error messages are not shown because we do not check the running of Active Directory Domain Services and its dependent services before performing the Active Directory related operations. Because Unified ICM/CCE does not use the Microsoft Windows Server LDAP library, no error displays when you restart Active Directory Domain Services.