Application Note - AN17026

MT App Note 17026 (AN 17026)
October, 2017

Active Directory Integration and Interaction with Connect ONSITE

Description: This Application Note describes how Microsoft Active Directory is integrated into Mitel Connect ONSITE and what features are available when AD integration is enabled.

Environment:
Mitel Connect ONSITE
Mitel Connect desktop application (for Windows and Mac)
Microsoft Exchange, Office 365, Outlook

Target Audience:
Mitel Partners
Mitel Partner Sales Engineers
Mitel Solution Architects

When Connect ONSITE is integrated with Microsoft Active Directory (AD), several features are enabled which provides easier user and administrator access, Connect account synchronization, and easier creation of user accounts. Connect AD Integration is configured in Director 2.

This document describes how to configure and test Connect AD Integration, what features are provided when Connect AD Integration is enabled, and how the Connect user experience is enhanced.

Contents

Introduction

Normally, when users access the Connect desktop client and when and administrators access Connect ONSITE Director 2, they must enter the individual credentials that were configured for the user in Director 2. If the user's domain credentials are changed, such as the user's password, the Connect credentials remain the same unless they are changed in Director 2 by an administrator.

Likewise, if the user's extension, name, or email address is changed in Active Directory, that information must be updated in Director 2. Also, individual user accounts must be configured in Director 2 one at a time.

When Connect Active Directory (AD) Integration is configured, several features are enabled which make all these functions easier for the Connect user and the Connect administrator. These features include:

- Automatic login authentication of Connect users when they launch the Connect desktop client and when Connect administrators access the Direct 2 administration page.
- Synchronization of Connect Director 2 user and administrator records from the information in Active Directory.
- Bulk provisioning of Connect user records from Active Directory accounts.

Note that AD Integration is not supported for Connect CLOUD.

CLOUD users can save their Connect client credentials. Those credentials are automatically verified on subsequent launches. Credentials are initially created by the administrator on the BOSS Portal and periodically changed by the user.

CLOUD administrators (Decision Makers) use the BOSS Portal to administer accounts (not Director 2). CLOUD administrators login to the BOSS Portal with separate credentials.

Global Address List (GAL) information for CLOUD accounts comes from the CLOUD user records in BOSS for the particular tenant (not the user's Active Directory).

Understanding Active Directory access with LDAP

In order for Connect ONSITE to find the Active Directory database, the standardized access location of Active Directory must be configured into Director 2. Microsoft provides a service which is used to connect to, search, and modify Internet directories such as the Active Directory. This service is called Lightweight Directory Access Protocol or LDAP.

Using LDAP can be very complicated, because this service is quite flexible and provides many functions. For Connect AD Integration, all that is needed is the path to find and connect to Active Directory. This “path” is expressed by the LDAP “ADsPath” statement. This statement is entered into the “AD Path” parameter of Director 2.

The ADsPath statement has the following format:

LDAP://HostName[:PortNumber][/DistinguishedName]

The “HostName” can be a computer or server name, an IP address, or a domain name. Typically, a server name is specified. For Connect, the Active Directory server is usually specified.

The “PortNumber” is the port to be used for the connection to the directory. If no port number is specified, LDAP uses the default port number (636 if using an SSL connection or 389 if not using an SSL connection).

The "DistinguishedName" is a unique name for an entry in a directory search. The attributes for the "DistinguishedName" describe the desired directory object and the directory hierarchy above it. For accessing an Active Directory, the following attributes are typical:

Attribute Display Name	LDAP Attribute
Common-Name	cn
Organizational-Unit-Name	ou
Domain-Component	dc

LDAP attributes

To assist in determining the correct Active Directory structure, the “dsquery” command can use used. From a Command Prompt on the server where Active Directory is deployed, enter the command “dsquery ou”. The command returns the LDAP Organizational Unit information for the domain. For example:

```
>C:\Users\Administrator>dsquery ou
>"OU=Domain Controllers,DC=anycompany,DC=com"
>"OU=Microsoft Exchange Security Groups,DC=anycompany,DC=com"
```

This information can be used to form the LDAP statement for Connect. In the example above, the “dsquery” command reports that the Organizational Unit (OU) is composed of the Domain Component (DC) “anycompany” and “com”. So the DistinguishedName attributes would be “/dc=anycompany,dc=com”. This is used for the "DistinguishedName" component of the LDAP statement.

For example, for an Active Directory server called “domain1” in the domain “anycompany.com”, and using the information from the “dsquery” command above, a typical LDAP statement would be:

LDAP://domain1.anycompany.com/dc=anycompany,dc=com

This is the simplest example, but the required syntax could be considerably more complex depending on how the specific company’s Active Directory structure has been configured.

This full LDAP statement is entered into the “AD Path” parameter of Director 2. Connect only needs to find the location of the Active Directory. With that information, Connect can then find specific users in Active Directory and link them to the users in Connect.

Important Note: The LDAP statement and the concepts for forming the correct parameters and attributes are often complex and not always obvious. It is recommended that the Connect administrator consult with their I.T. department for assistance in forming the correct LDAP statement.

To verify that the LDAP statement is correct, the administrator must turn on AD Integration for the Connect system, enable a user for AD Integration, and test the Active Director access by retrieving the user’s information. This process is described below in the section Enabling Active Directory Integration in Connect.

For further information on LDAP and its attributes, see the following:

Microsoft Developer Network - Lightweight Directory Access Protocol:
https://msdn.microsoft.com/en-us/library/aa367008(v=vs.85).aspx

Microsoft Developer Network - LDAP ADsPath:
https://msdn.microsoft.com/en-us/library/aa746384(v=vs.85).aspx

Microsoft TechNet - Object Naming:
https://technet.microsoft.com/en-us/library/cc977992.aspx

Enabling Active Directory Integration in Connect

There are two steps to enable and utilize AD Integration in Connect. The first is to turn on AD Integration and specify the Active Directory path. The second is to enable specific users to be enabled and synchronized with Active Directory.

The *Connect System Administration Guide* warns that “At least one user account must have administrative rights before Active Directory is enabled. AD does not allow a user to log in through the default admin account.” Be sure there is at least one Active Directory / Connect user with the Connect “System Administrator” role before enabling Connect AD Integration. Enable this user as the first user with AD Integration. See the *Connect System Administration Guide* for more information.

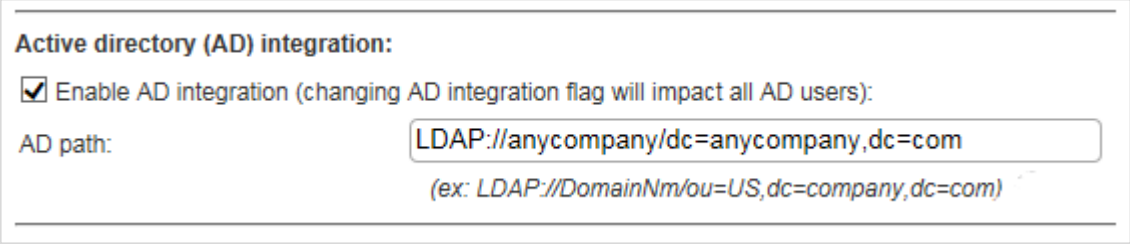
To enable AD Integration for the Connect ONSITE system:

- Access Director 2.
- Navigate to Administration > System > Additional Parameters > Active directory (AD) integration.
- Check “Enable AD integration”.
- Enter the proper LDAP ADsPath statement into the “AD path” text box.

  Note that example under the text box in Director 2 implies to enter the domain name (“DomainNm”). This may not apply to all configurations and greatly depends on the specific Active Directory path. See Understanding Active Directory access with LDAP above.

  There is no direct test to verify if the LDAP statement is correct. The LDAP statement can be tested when a user is enabled for AD Integration (see below).

- Save changes.



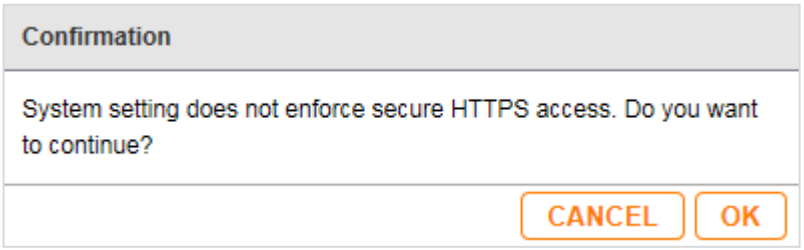
Enabling AD Integration in Director 2

To enable individual users for AD Integration:

- Access Director 2.
- Navigate to Administration > Users > Users.
- Select the desired user.
- On the “General” tab, check “Active Directory user”.
- Enter the full domain username of the user (domain\username) in the “Account” text box.
- Save changes.

Enabling Active Directory integration for a user account

To test the Active Directory integration, click on the “SHOW FROM AD” button. A confirmation window is displayed. This is a cautionary message only and does not represent an error or problem.

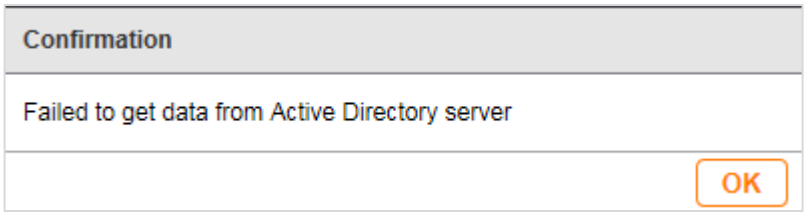


An authentication window is displayed. Enter the Connect administrator password.

If the LDAP path statement is correct and the user exists in Active Directory, the “AD Data” window is displayed. This window verifies that AD Integration is working correctly.

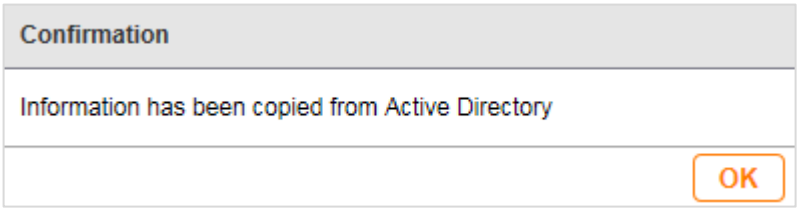
AD Data window from the “Show From AD” button

If the LDAP path statement is incorrect or if the user does not exist in Active Directory, the “Failed to get data from Active Directory server” message is displayed. Confirm that the Active Directory user’s account credentials have been entered correctly into the Connect user record and that the LDAP path statement is correct. The “AD Data” window must be displayed when the “SHOW FROM AD” button is clicked in order for AD Integration to be correctly configured.



“Failed” window from the “Show From AD” button. AD Integration is not correct.

Once AD Integration has been successfully enabled, the user’s name, email address, phone numbers, etc. are copied from Active Directory. If any of these items change in Active Directory, the Connect administrator can synchronize the user’s data by clicking on the “SYNC FROM AD” button. The following confirmation is displayed.



“Sync from AD” confirmation window

Using AD Integration

Once enabled, Connect AD Integration can be used for automatic authentication into the Connect desktop client and for Connect administrators to access Connect Director 2. Whenever the user's domain password changes, the users are not required to update their Connect credentials.

There are several variations for logging into the Connect client and into Director 2 if the user does not have an Active Directory account or is not logged into the domain. Consult the *Connect System Administration Guide* for more information.

AD Authentication for the Connect Client

When the Connect client is initially installed, users who have been preconfigured for AD Integration are not prompted for their credentials. Instead, they are prompted for the Connect server name and are then guided through the rest of the setup process.

When the Connect client is launched for a user enabled with AD Integration, the user is automatically authenticated and the main Connect client screen is displayed. This process continues even if the user changes their domain password.

For Exchange authentication, to create and display meeting information in Connect, the user still needs to update their Exchange credentials (Settings / Preferences > Account > AD Credentials), even if they match the domain credentials.

AD Authentication for Connect Director 2.

Connect administrators can automatically authenticate to the Director 2 web page, when AD Integration has been enabled and configured. Connect administrators must have an Active Directory account, a Connect user account with AD Integration enabled, and are configured for the Connect System Administrator role.

If the administrator is logged into another domain account, such as their own domain user account, and the Connect administrator account credentials are different than the user's account, the user may be prompted for the network credentials for the administrator account. In this case, the user enters the administrator AD credentials, and the user will be authenticated into Director 2.

Bulk Provisioning of Active Directory User Accounts

When Connect is enabled for AD Integration, the administrator can export Active Directory records and use the Connect User Import Tool to create multiple Connect user records. See the *Connect System Administration Guide* for a complete description of this procedure.

Additional Resources

- Mitel Connect Client User Guide
- Mitel Connect System Administration Guide
- Microsoft Developer Network - Lightweight Directory Access Protocol web site

Version	Date	Contributor	Content
1.0	October, 2017	W. Toigo	Original App Note