# PowerEdge MX7000: How to configure AD and LDAP

Dell EMC Technical White Paper

# Revisions

| Date | Description |
|---|---|
| May 2017 | Initial release |
| | |

# Acknowledgements

This paper was produced by the following members of the Dell EMC storage engineering team:

Author: Nitesh Anand

# Table of contents

# Introduction

PowerEdge MX7000 comes with a **Management Module** that provides chassis management. Management Module supports High Availability with the help of a redundant module. An integral feature of the management firmware is to allow access to the system and its configuration to authorized personnel only.

This technical white paper shows how users can benefit from configuring AD/LDAP.

# Overview

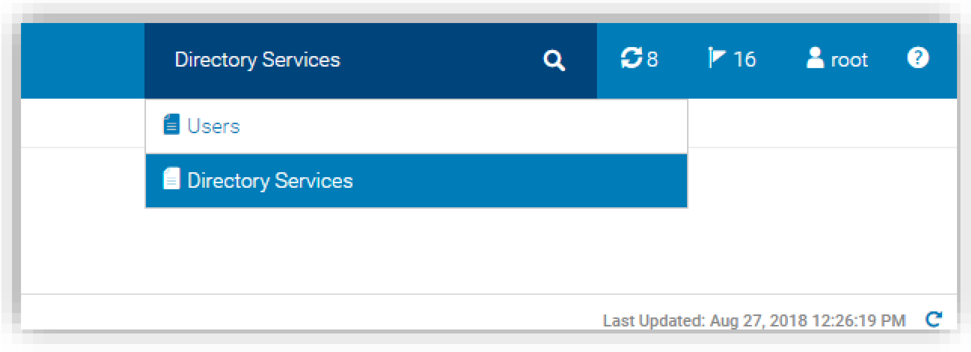
Management Module provides an application interface for configuring itself with an existing AD, LDAP or ADLDS server for authentication and authorization.

# Need for AD/LDAP

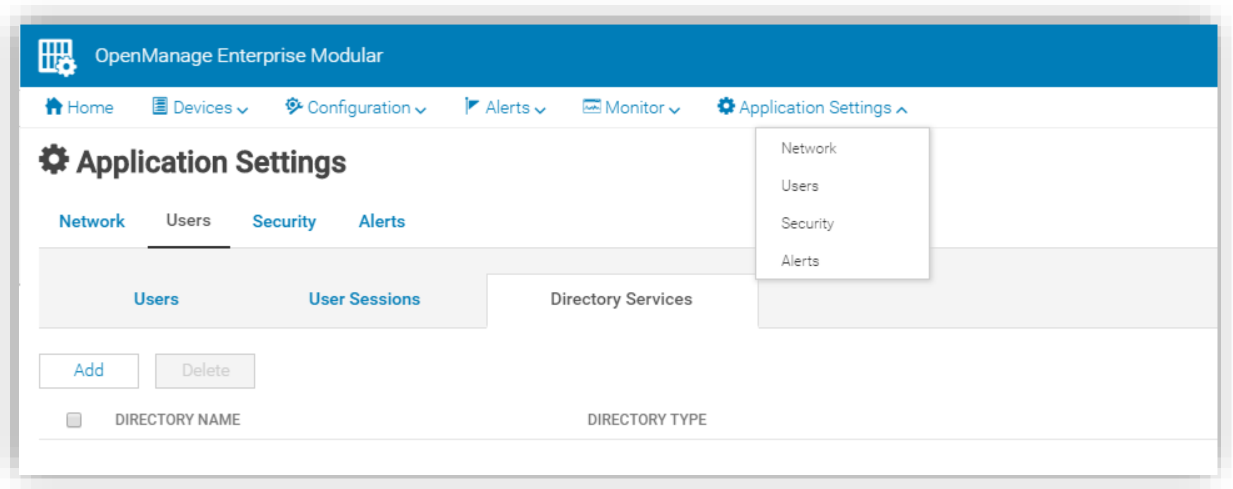
Customers can choose either to create users in the management module for authentication and authorization or can connect to an existing AD or LDAP server and provide different access levels to existing AD/LDAP groups. This drastically brings down the user setup time.

# Configuring AD/LDAP

Management Module provides a user interface to configure AD/LDAP servers. Before importing the groups, customers will need to configure a directory service. They can either search for "Directory Services" in the global search box on the top as shown in the picture below and click on it to be immediately navigated to it

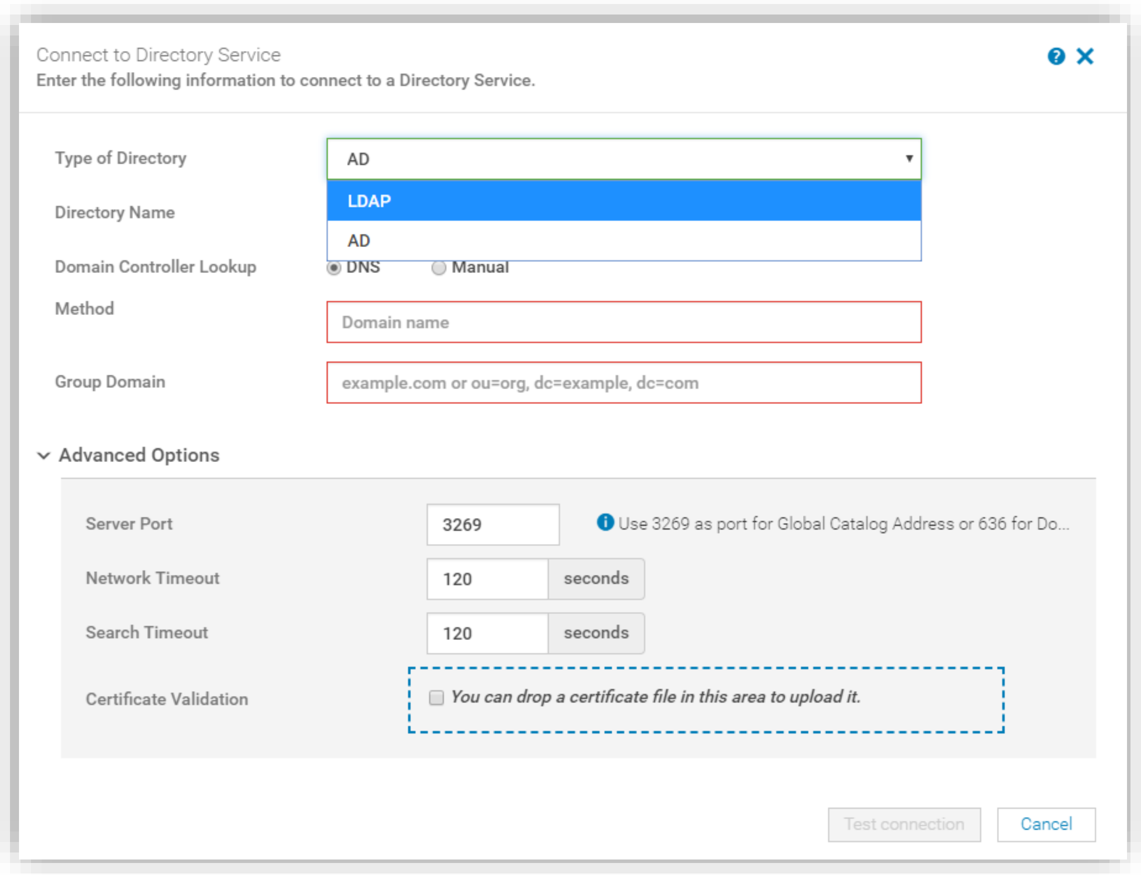


or manually navigate to: Home page → Application Settings → Users. Here on "Users" page, they will notice a tab for "Directory Services".



They can click on the “Add” button on this page to add a new configuration.

Management Module UI interface provides an option to choose between AD and LDAP services.


Connect to Directory Service

Enter the following information to connect to a Directory Service.

Type of Directory: AD (LDAP, AD)

Directory Name

Domain Controller Lookup Method: ● DNS ○ Manual

Domain name

Group Domain: example.com or ou=org, dc=example, dc=com

Advanced Options

Server Port: 3269 — Use 3269 as port for Global Catalog Address or 636 for Do...

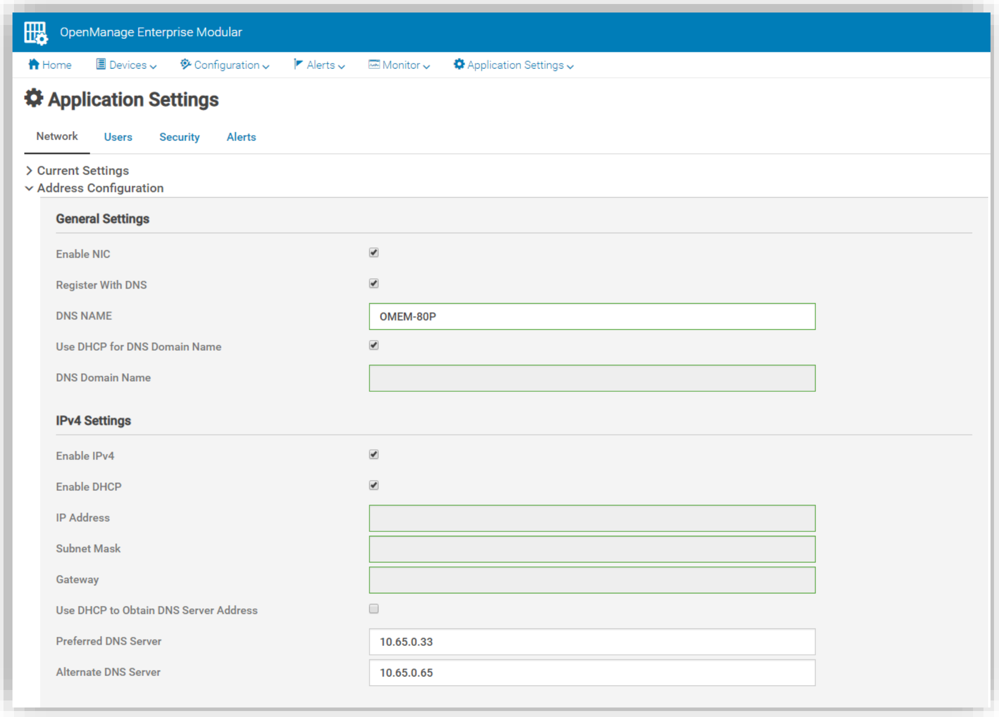
Network Timeout: 120 seconds

Search Timeout: 120 seconds

Certificate Validation: □ You can drop a certificate file in this area to upload it.

- Choose the type of directory service you want to connect to.
- Provide directory name. This name is just a name to relate to the configuration to. Please note that this name is not the name of the group that you want to import.
- Choose between DNS or Manual settings for domain controller lookup.

- If you do not know the details of the domain controllers in the domain from which you are planning to import the group or groups, you may want to choose DNS setting. This setting will discover the domain controllers automatically with provided configuration. For this to work, please ensure that “Register with DNS” has been enabled and the corresponding configuration for Primary/Alternate DNS Servers are provided in the Network Settings.



**Application Settings**

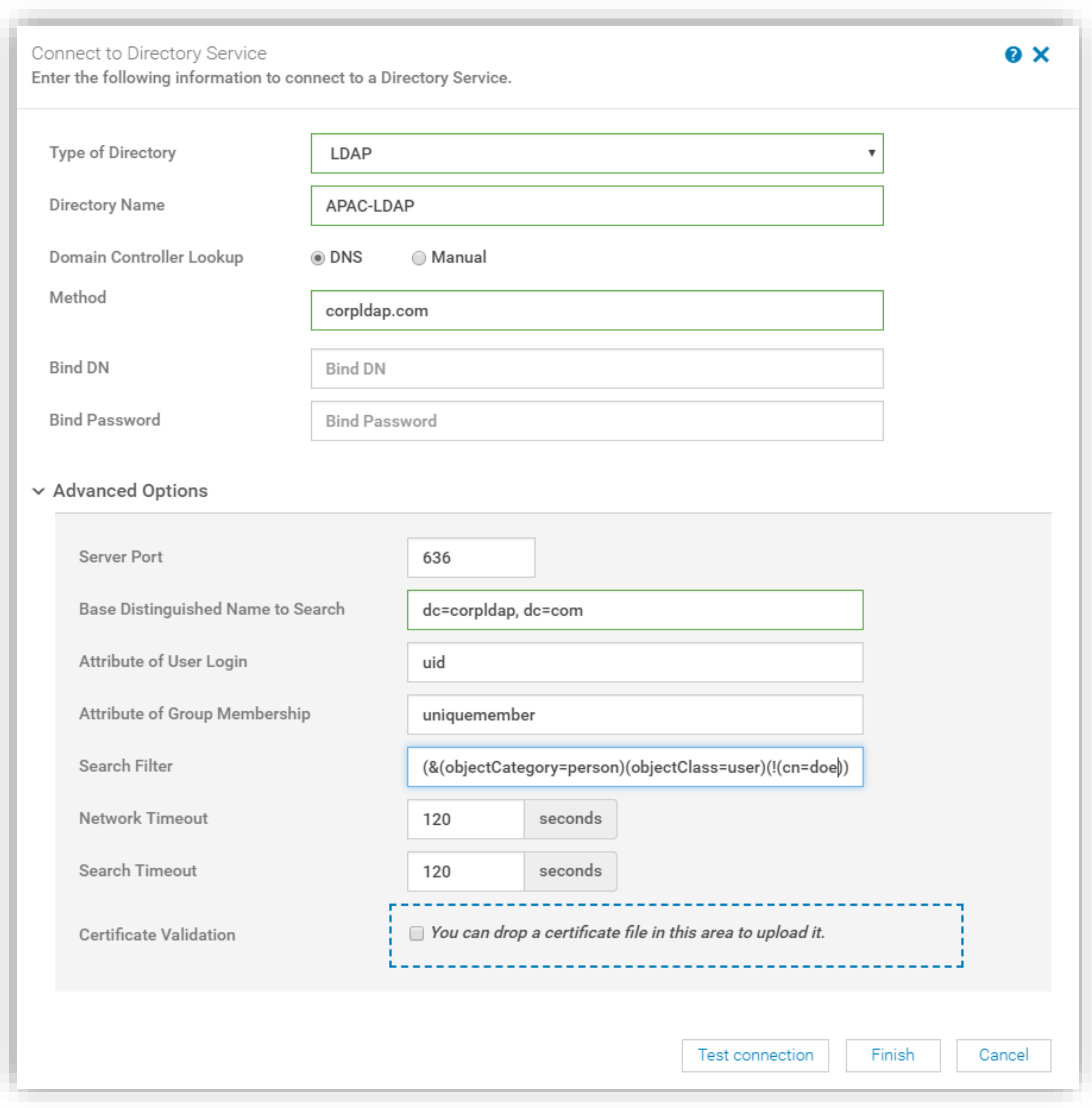
**General Settings**

| | |
|---|---|
| Enable NIC | ☑ |
| Register With DNS | ☑ |
| DNS NAME | OMEM-80P |
| Use DHCP for DNS Domain Name | ☑ |
| DNS Domain Name | |

**IPv4 Settings**

| | |
|---|---|
| Enable IPv4 | ☑ |
| Enable DHCP | ☑ |
| IP Address | |
| Subnet Mask | |
| Gateway | |
| Use DHCP to Obtain DNS Server Address | ☐ |
| Preferred DNS Server | 10.65.0.33 |
| Alternate DNS Server | 10.65.0.65 |

- Now provide the “Domain Name” under which the group(s) intended to be imported belongs. The way application works is that it looks at the SRV record on the DNS servers (*which we configured in the “Network Settings” as shown in picture above*), to get the list and the details of domain controllers in the provided Domain. After that, it makes requests to these domain controllers to get the list of groups.
- If you know IP address or FQDN of the domain controller(s), you can choose the Manual settings and provide the list in a comma separated fashion.
- Provide “Group Domain” string, which generally looks like “CN=Builtin, DC=MyDomain, DC=com”. Customers can contact the network administrator to find out this information. Please note that this configuration is not used by “Test connection” feature.



Connect to Directory Service

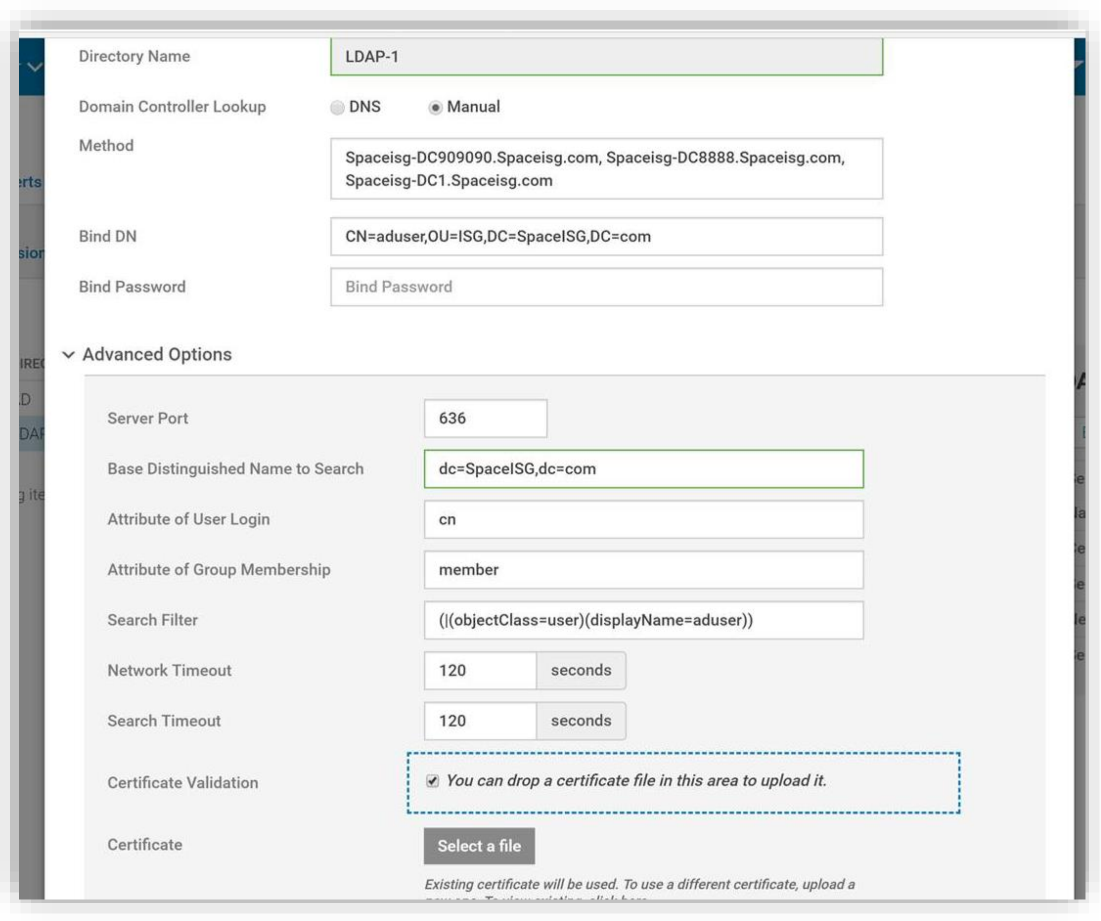
Enter the following information to connect to a Directory Service.

| | |
|---|---|
| Type of Directory | LDAP ▾ |
| Directory Name | APAC-LDAP |
| Domain Controller Lookup | ● DNS ○ Manual |
| Method | corpldap.com |
| Bind DN | Bind DN |
| Bind Password | Bind Password |

Advanced Options

| | |
|---|---|
| Server Port | 636 |
| Base Distinguished Name to Search | dc=corpldap, dc=com |
| Attribute of User Login | uid |
| Attribute of Group Membership | uniquemember |
| Search Filter | (&(objectCategory=person)(objectClass=user)(!(cn=doe)) |
| Network Timeout | 120 seconds |
| Search Timeout | 120 seconds |
| Certificate Validation | □ *You can drop a certificate file in this area to upload it.* |

Figure 1 Picture showing possible values of all different fields with LDAP configuration



Directory Name: LDAP-1

Domain Controller Lookup: ○ DNS ● Manual

Method: Spaceisg-DC909090.Spaceisg.com, Spaceisg-DC8888.Spaceisg.com, Spaceisg-DC1.Spaceisg.com

Bind DN: CN=aduser,OU=ISG,DC=SpaceISG,DC=com

Bind Password: Bind Password

Advanced Options

Server Port: 636

Base Distinguished Name to Search: dc=SpaceISG,dc=com

Attribute of User Login: cn

Attribute of Group Membership: member

Search Filter: (|(objectClass=user)(displayName=aduser))

Network Timeout: 120 seconds

Search Timeout: 120 seconds

Certificate Validation: ☑ *You can drop a certificate file in this area to upload it.*

Certificate: Select a file

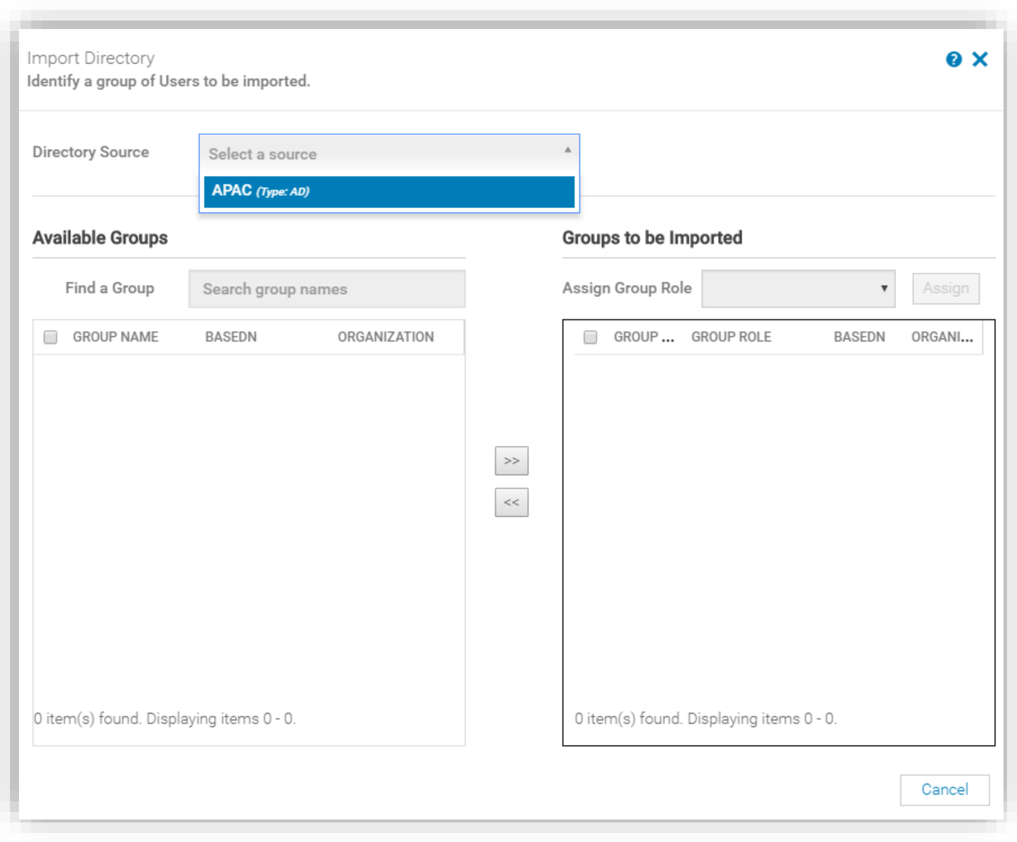
*Existing certificate will be used. To use a different certificate, upload a*

Figure 2 Picture showing possible values of all different fields with ADLDS configuration

- Customers can modify “Network Timeout” and “Search Timeout” settings as per their server and network requirement.
- For additional security, customers can also provide a certificate file that will be used for validation when connecting to AD/LDAP servers.
- Once all these settings are provided, customers can either save this configuration and head over to import or choose to verify if this configuration works fine by clicking on the “Test connection” button on this wizard. Test configuration needs user credentials which will not be stored and is only used for testing the configuration.

# Importing groups AD/LDAP

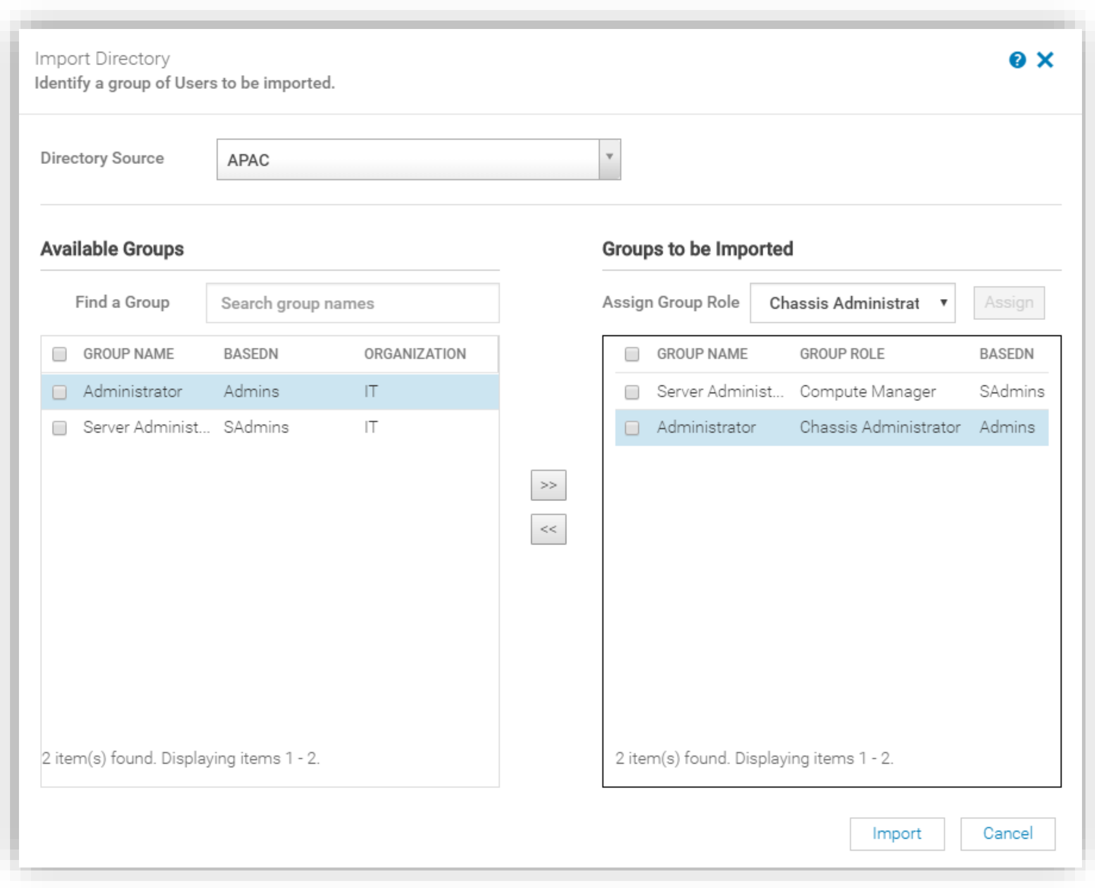
With all AD/LDAP configured and working, customers can head over to “Users” tab to import the directory group(s) that they are interested in.



Import Directory
Identify a group of Users to be imported.

Directory Source: Select a source

- After selecting the directory source, customers will be prompted to enter their credentials, which will allow the application to get the list of groups from the server.
- Provide a few letters of the group name in the "Find a Group" field, and the groups matching the string will be listed in the section on the left below the search box.
- Move one of more of these groups into the right sections. From the selection box, "Assign Group Role", select a group to be assigned to the selected groups on the right section.



Import Directory

Identify a group of Users to be imported.

Directory Source: APAC

**Available Groups**

Find a Group: Search group names

| □ | GROUP NAME | BASEDN | ORGANIZATION |
|---|---|---|---|
| □ | Administrator | Admins | IT |
| □ | Server Administ... | SAdmins | IT |

2 item(s) found. Displaying items 1 - 2.

**Groups to be Imported**

Assign Group Role: Chassis Administrat

| □ | GROUP NAME | GROUP ROLE | BASEDN |
|---|---|---|---|
| □ | Server Administ... | Compute Manager | SAdmins |
| □ | Administrator | Chassis Administrator | Admins |

2 item(s) found. Displaying items 1 - 2.

- Once all the groups are assigned roles, customer can import them. Upon successful import, a message is displayed and all the users under these groups will be able to access the Management Console with specified roles and privileges.
- With all these configuration in place and import completed, users of imported groups will be able to login with their domain credentials. They can provide their domain\username in the username field and the domain password in the password field. Example: americas\john_doe