# Table of Contents

1 **Introduction** .................................................................................................................................... 2
    1.1 Communication between EWS Controller and LDAP Server................................................... 2

2 **Steps to Setup LDAP Server Integration with Controller** .......................................................... 3
    2.1 Windows Active Directory (AD) Configuration ................................................................. 3
    2.2 LDAP Browser Configuration for Querying Data from LDAP Server .................................. 4
    2.3 LDAP Server Configuration on EWS Controller ............................................................... 6
    2.4 Attribute Group Mapping Configuration.......................................................................... 10

3 **Conclusion** .................................................................................................................................... 12

4 **Remarks** ........................................................................................................................................ 12
1 Introduction

This technical guide is aimed at explaining the practical setup flow of LDAP server integration with Edgecore EWS Controller. The EWS Controller offers simple LDAP server integration with a straightforward login flow where users can use web-based login (or universal access method, UAM) to be granted network access. With built-in AAA functionality, the EWS Controller offers various authentication methods using different internal and external servers, and LDAP is one of the protocols supported for communicating with external servers, besides RADIUS, POP3 and SIP.

From the web management interface of the EWS Controller, network administrators can configure settings for the LDAP server to be integrated, which can be a Windows server that supports Windows Active Directory or an OpenLDAP server, for example.

Once integrated, network users will be able to use web-based login to be authenticated to access the network. Users authenticated through the LDAP server configured can be assigned to a particular Group for Policy enforcement. Furthermore, these authenticated users can also be assigned to different groups based on different LDAP attributes using the Attribute-Group Mapping function to provide flexible user management.

1.1 Communication between EWS Controller and LDAP Server

Diagram below illustrates the communication between the EWS Controller and the configured LDAP server in user authentication process. First, user can login by submitting their credentials on the login page. Next, the controller would send the credentials to the external LDAP server configured. Then, the LDAP server would send an authentication reply (allow or deny) to the controller, which would redirect the user to the login success/fail page and grant network access if the login were successful.
2 Steps to Setup LDAP Server Integration with Controller

As an example, the following network topology is used with a Windows server supporting Windows Active Directory being the LDAP server.

2.1 Windows Active Directory (AD) Configuration

a. Create an Organizational Unit.
2.2 LDAP Browser Configuration for Querying Data from LDAP Server

An LDAP browser can be used to query data from the LDAP server and check whether the LDAP server is working properly. Softerra is used as an example of LDAP browsers here.

a. Create a new profile

b. Create a user
Integration with Windows Active Directory (LDAP)

Profile Creation Wizard - Step 1

Server Profile Name
Please enter a name for the profile.

Profile Name: TIR

Profile Creation Wizard - Step 2

Profile General Information
Please provide general information.

Specified server host information & adjust general security options.

Host: 10.2.20.12
Port: 380

Directory:
DC=Configuration,DC=domain,DC=local

Security:
DC=Domain,DC=local

LDAP URL:
ldap://10.2.20.12:389/??ronl?objectClass=*
After the new profile has been setup, the LDAP Browser will query the information on Windows AD and display the information.

2.3 LDAP Server Configuration on EWS Controller

a. Go to Users > External Authentication > LDAP, fill in the necessary information and choose Windows AD as the Binding Type.
Below are explanations of terms on this page.

- **Service Protocol**
  - **LDAP** – The original LDAP service protocol that uses TCP/UDP as the transport protocol and typically uses port 389 for connections. LDAP connections are not encrypted and passwords are sent and stored in clear text.
  - **LDAPS** – Entire LDAPS connections are encrypted using SSL and traffic is handled on a separate port, typically port 636.
  - **LDAP+StartTLS** – This protocol allows connections to be encrypted using SSL or TLS while using the same port 389 as LDAP.

- **Base DN**: Base Distinguished Name for LDAP search. This information can be found using the LDAP browser.
Binding Type: Binding refers to the authentication of EWS Controller by the LDAP server. The controller has to be authenticated for access to the LDAP server.

- **User Account** – A legacy binding type that binds to a certain DN. The Controller can only query user information in this DN but not in its sub directories.
- **Anonymous** – Allows the Controller to query user information without authentication.
- **Specified DN** – An account for the Controller has to be setup before the Controller can use this account to query user information.
- **Windows AD** – Domain names have to be setup in the Windows AD before the Controller can search the logon name in Windows AD based on credentials submitted by the users.
Account Attribute: Account Attribute provides options for using UID, CN or sAMAccountName as login credentials and which one to use depends on the external server and its configurations.

- UID – User ID, usually used for OpenLDAP.
- CN – Common name which usually be someone’s full name and supports the use of space.
- sAMAccountName – The logon name in windows AD and does not support use of space.

Note: For failover, a secondary LDAP server can be configured so that when the controller cannot reach the primary LDAP server, the controller will send authentication requests to the secondary LDAP server.
2.4 Attribute Group Mapping Configuration

By default, the Controller can assign users to one particular Group on the Controller for Policy enforcement. However, with Attribute-Group Mapping function, the Controller can assign users to different Groups based on different LDAP attributes for flexible user management. In this example, a group is created in Windows AD as an example of possible LDAP attributes, and a user with this attribute will sign in to the Controller and be assigned to a particular Group on the Controller based on different LDAP attributes after authentication.

a. Create a user group and assign the group to a user account in Windows AD

![Creating a user group in Windows AD]

b. Use an LDAP browser to query account information to verify if the account has the correct attribute

![Querying account information with an LDAP browser]
c. Go to Users > External Authentication > LDAP > LDAP Attribute Mapping, enable the function, fill in LDAP Attribute Name and Value and choose the appropriate Group for mapping.

Note: When an account has multiple attributes mapping to different Groups, the Controller will use the first mapping.

Account information can also be queried using Account Attributes.
3 Conclusion

In this technical guide, steps to configure LDAP server integration with the EWS Controller are shown, where a Windows server that supports Windows Active Directory is used as an example of LDAP servers. After authentication, users can also be assigned to different Groups on the Controller based on different LDAP attributes using the Attribute-Group Mapping function to provide flexible user management.

4 Remarks

Please contact Edgecore's Technical Support Team at ecwifi@edge-core.com for additional inquiries.