Configure WLC with LDAP Authentication for 802.1x and Web-Auth WLANs

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Technical Background
Frequently Asked Questions
Configure
Create WLAN That Relies On LDAP Server To Authenticate Users Through 802.1x
Network Diagram
Create WLAN That Relies On LDAP Server To Authenticate Users Through Internal WLC Web Portal
Network Diagram
Use LDP Tool To Configure And Troubleshoot LDAP
Verify
Troubleshoot
Related Information

Introduction

This document describes the procedure to configure an AireOS Wireless LAN Controller (WLC) in order to authenticate clients with a Lightweight Directory Access Protocol (LDAP) Server as the users database.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Microsoft Windows Servers
- Active Directory

Components Used

The information in this document is based on these software versions:
Background Information

Technical Background

- LDAP is a protocol used to access directory servers.
- Directory servers are hierarchical, object oriented databases.
- Objects are organized in containers such as Organizational Units called OU, Groups or default Microsoft Containers as CN=Users.
- The most difficult part of this setup is to configure the LDAP server parameters correctly on the WLC.

For more detailed information about these concepts, refer to the Introduction section of How to configure Wireless Lan Controller (WLC) for Lightweight Directory Access Protocol (LDAP) authentication.

Frequently Asked Questions

- What username must be used to bind with the LDAP Server?
  There are two ways to bind against an LDAP Server, Anonymous or Authenticated (refer to in order to understand the difference between both methods). This bind username needs to have Administrator privileges to be able to query for other usernames/passwords.

  - If authenticated, you need to ask: is the bind username inside the same container than all users?
  The way to specify the username depends on the answer:

    If the answer is No, use the whole path. For example:

    \texttt{CN=Administrator,CN=Domain Admins,CN=Users,DC=labm,DC=cisco,DC=com}

    If the answer is Yes, then use the username only. For example:

    \texttt{Administrator}

- What if there are users in different containers? Do all involved wireless LDAP users need to be in the same container?
  No, a base DN that includes all the containers needed can be specified.

- What attributes must the WLC look for?
  The WLC matches the User Attribute and Object Type specified.
Note: `sAMAccountName` is case sensitive but person is not. Therefore, `sAMAccountName=RICARDO` and `sAMAccountName=ricardo` are the same and works whereas `samaccountname=RICARDO` and `samaccountname=ricardo` does not.

- Which Extensible Authentication Protocol (EAP) methods can be used?
  EAP-FAST, PEAP-GTC and EAP-TLS only. Android, iOS and MacOS default supplicants work with Protected Extensible Authentication Protocol (PEAP). For Windows, Anyconnect Network Access Manager (NAM) or the default Windows supplicant with Cisco:PEAP must be used on supported wireless adapters as shown in the image.

![Local-EAP Wireless Network Properties](image)

Note: The Cisco EAP Plug-ins for Windows include a version of Open Secure Socket Layer (OpenSSL 0.9.8k) that is affected by CSCva09670. Cisco does not plan to issue any more releases of the EAP Plug-ins for Windows, and recommends that customers instead use the AnyConnect Secure Mobility Client.

- Why can't the WLC find users?
  Users inside a Group cannot be authenticated. They need to be inside a Default Container (CN) or an Organizational Unit (OU) as shown in the image.
Configure

There are different scenarios in which an LDAP server can be employed, either with 802.1x authentication or Web authentication. For this procedure, only users inside the OU=SofiaLabOU must be authenticated. In order to learn how to use the Label Distribution Protocol (LDP) tool, configure and troubleshoot LDAP, refer to the [WLC LDAP Configuration Guide](#).

Create WLAN That Relies On LDAP Server To Authenticate Users Through 802.1x

Network Diagram

In this scenario, WLAN LDAP-dot1x uses an LDAP Server to authenticate the users with the use of 802.1x.

![Network Diagram](image)

Step 1. Create a user **User1** in the LDAP Server member of the SofiaLabOU and SofiaLabGroup as shown in the images.
Step 2. Create an EAP Profile at the WLC with the desired EAP method (use PEAP) as shown in the image.
Step 3. Bind the WLC with the LDAP Server as shown in the image.

**Tip**: If the bind Username is not in the User Base DN, you have to write the entire path to the **Admin** user as shown in the image. Otherwise, you can simply enter **Administrator**.

Step 4. Set the Authentication Order to be set to Internal Users + LDAP or LDAP only as shown in the image.
Step 5. Create the LDAP-dot1x WLANs as shown in the images.
Step 6. Set the L2 security method to WPA2 + 802.1x and set L3 security to none as shown in the image.
Step 7. Enable local EAP Authentication and ensure Authentication Servers and Accounting Servers options are disabled and LDAP is enabled as shown in the image.
All other settings can be left at defaults.

**Notes:**
Use the LDP tool to confirm the configuration parameters.
The Search Base cannot be a Group (such as SofiaLabGroup).
PEAP-GTC or Cisco:PEAP have to be used instead of Microsoft:PEAP at the supplicant if it is a Windows Machine. Microsoft:PEAP works by default with MacOS/iOS/Android.

**Create WLAN That Relies On LDAP Server To Authenticate Users Through Internal WLC Web Portal**

**Network Diagram**

In this scenario, WLAN LDAP-Web uses an LDAP server to authenticate the users with the internal WLC Web Portal.
Ensure Steps 1. through Steps 4. have been taken from the previous example. From there, the WLAN configuration is set differently.

Step 1. Create a user **User1** in the LDAP Server member of the OU SofiaLabOU and the Group SofiaLabGroup.

Step 2. Create an EAP Profile at the WLC with the desired EAP method (use PEAP).

Step 3. Bind the WLC with the LDAP Server.

Step 4. Set the Authentication Order to be set to Internal Users + LDAP.

Step 5. Create the LDAP-Web WLAN as shown in the images.
Step 7. Set the Authentication priority order for web-auth to use LDAP and ensure Authentication Servers and Accounting Servers options are disabled as shown in the image.
All other settings can be left at defaults.

Use LDP Tool To Configure And Troubleshoot LDAP

Step 1. Open the LDP tool either at the LDAP server or at a host with connectivity (Port TCP 389 must be allowed to the server) as shown in the image.

Step 2. Navigate to Connection > Bind, log in with an Admin user and select Bind with credentials radio button as shown in the image.

Step 3. Navigate to View > Tree and select OK in the base DN as shown in the image.

Step 4. Expand the tree to view the structure and look for the Search Base DN. Consider that it can be any container type except Groups. It can be the whole domain, a specific OU or a CN like CN=Users as shown in the image.
Step 5. Expand the SofiaLabOU in order to see which users are inside of it. There is the User1 that was created before as shown in the image.

Step 6. Everything needed to configure LDAP is as shown in the image.
Step 7. Groups like SofiaLabGroup cannot be used as a search DN. Expand the group and look for the users inside it, where the User1 previously created must be as shown in the image.

User1 was there but LDP was not able to find it. It means the WLC is not able to do it as well and which is why Groups are not supported as a Search Base DN.

Verify

Use this section to confirm that your configuration works properly.

```
(cisco-controller) >show ldap summary

Idx  Server Address  Port  Enabled  Secure
----  ---------------  ----  -------- ��过
   1  10.88.173.121   389  Yes    No
```
Server Index................................. 1
Address.......................................... 10.88.173.121
Port............................................. 389
Server State................................. Enabled
User DN.......................................... OU=SofiaLabOU,DC=labm,DC=cisco,DC=com
User Attribute......................... sAMAccountName
User Type................................. Person
Retransmit Timeout......................... 2 seconds
Secure (via TLS).............................. Disabled
Bind Method ................................. Authenticated
Bind Username............................ CN=Administrator,CN=Domain Admins,CN=Users,DC=labm,DC=cisco,DC=com

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Server Index................................. 1
Server statistics:
  Initialized OK............................... 0
  Initialization failed........................ 0
  Initialization retries......................... 0
  Closed OK.................................... 0
Request statistics:
  Received...................................... 0
  Sent.......................................... 0
  OK............................................ 0
  Success...................................... 0
  Authentication failed......................... 0
  Server not found............................ 0
  No received attributes........................ 0
  No passed username.......................... 0
  Not connected to server........................ 0
  Internal error................................ 0
  Retries...................................... 0

Related Information

- **LDAP - WLC 8.2 Configuration Guide**
- **How to configure Wireless Lan Controller (WLC) for Lightweight Directory Access Protocol (LDAP) authentication - by Vinay Sharma**
- **Web Authentication Using LDAP on Wireless LAN Controllers (WLCs) Configuration Example - by Yahya Jaber and Ayman Alfares**
- **Technical Support & Documentation - Cisco Systems**