Secure LDAP

This chapter guides administrators through configuring secure LDAP on Cisco wireless controllers, detailing prerequisites, restrictions, TLS certificate requirements, CLI and GUI steps for server and AAA group setup, search/bind options, attribute mapping, and verification.

Lightweight Directory Access Protocol (LDAP)

A Lightweight Directory Access Protocol (LDAP) is a client-server protocol that

- allows clients to access and manage directory information stored on servers
- supports user authentication and authorization using operations such as bind and search, and
- operates over TCP/IP on port 389, optionally using Transport Layer Security (TLS) for secure communications.

Transport Layer Security (TLS)

Transport Layer Security (TLS) is an application-level protocol that enables secure data transactions by providing privacy, authentication, and data integrity. TLS relies on certificates, public keys, and private keys to prove the identity of clients.

Certificate Authorities (CAs) issue the certificates.

Each certificate includes these:

- The name of the authority that issued it.
- The name of the entity to which the certificate was issued.
- The public key of the entity.
- The timestamps indicating the expiration date of the certificate.

TLS support for LDAP is described in RFC 2830, which is an extension to the LDAP protocol.

LDAP Operations

Bind

The bind operation authenticates a user to the server and starts a connection with the LDAP server. LDAP is a connection-oriented protocol. The client specifies the protocol version and authentication information.

LDAP supports these binds:

- Authenticated bind: An authenticated bind is performed when a root Distinguished Name (DN) and password are available.
- Anonymous bind: An anonymous bind is performed when no root DN and password are provided.

In LDAP deployments, the search operation is commonly performed before the bind operation. If a password attribute is returned as part of the search operation, the LDAP client can verify the password locally, eliminating the need for an extra bind operation. If the password attribute is not returned, the bind operation can occur later. Another advantage of performing the search operation first is that the LDAP client can use the DN received in the search result as the user DN, instead of constructing it by prefixing the username (cn attribute) with the base DN. All entries stored in an LDAP server have a unique DN.

The DN consists of two parts:

- Relative Distinguished Name (RDN)
- Location in the LDAP server where the record resides.

Most of the entries that you store in an LDAP server will have a name, and the name is frequently stored in the Common Name (cn) attribute. Because every object has a name, most objects stored in an LDAP server use their cn value as the basis for their RDN.

Search

A search operation is used to search the LDAP server. The client specifies the starting point (base DN) of the search, the search scope (either the object, its children, or the subtree rooted at the object), and a search filter.

For authorization requests, the search operation is performed without a bind operation. The LDAP server must be configured with sufficient privileges for the search operation to succeed. These privileges are established during the bind operation.

An LDAP search operation can return multiple entries for a specific user. When this occurs, the LDAP client returns an error code to AAA. To prevent these errors, configure search filters to match only a single entry.

Compare

The compare operation replaces a bind request for authentication and helps maintain the initial bind parameters for the connection.

LDAP Dynamic Attribute Mapping

The Lightweight Directory Access Protocol (LDAP) is a powerful and flexible protocol for communication with AAA servers. LDAP attribute maps provide a method to cross-reference attributes retrieved from a server with Cisco attributes supported by security appliances.

When a user authenticates to a security appliance, the appliance authenticates the server and uses LDAP to retrieve the user's record. The record consists of LDAP attributes associated with fields displayed on the server's user interface. Each attribute retrieved includes a value entered by the administrator responsible for updating user records.

SLDAP prerequisite

This section lists the prerequisite for setting up SLDAP on a wireless controller and describes when to configure certificates.

- If you are using a Transport Layer Security (TLS) secure connection, you must configure X.509 certificates.

SLDAP restrictions

- LDAP referrals are not supported.
- The LDAP server's unsolicited messages or notifications are not handled.
- LDAP authentication is not supported for interactive terminal sessions.

Configure SLDAP (CLI)

Set up Secure LDAP (SLDAP) for authentication and directory queries on the wireless controller using commands.

Before you begin

Ensure you have administrator access to the controller. Gather LDAP server details (IP address, base DN, credentials).

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
Device# enable
```

Enter your password if prompted.

Step 2 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 3 Define a Lightweight Directory Access Protocol (LDAP) server and enter the LDAP server configuration mode.

Example:

```
Device(config)# ldap server server-name
```

Step 4 Specify the LDAP server IP address using IPv4.

Example:

```
Device(config-ldap-server)# ipv4 ipv4-address
```

Step 5 Specify the number of seconds the Cisco Catalyst 9800 Series Wireless Controller or the embedded wireless controller waits for a reply to a LDAP request before retransmitting the request.

Example:

```
Device(config-ldap-server)# timeout retransmit seconds
```

Step 6 Specify a shared secret text string used between the Cisco Catalyst 9800 Series Wireless Controller or the embedded wireless controller and a LDAP server.

Example:

```
Device(config-ldap-server)# bind authenticate root-dn
CN=ldapipv6user,CN=Users,DC=ca,DC=ssh2,DC=com password Cisco12345
```

Use the **0** line option to configure an unencrypted shared secret.

Use the **7** line option to configure an encrypted shared secret.

Step 7 Specify the base Distinguished Name (DN) of the search.

Example:

```
Device(config-ldap-server)# base-dn string CN=Users,DC=ca,DC=ssh2,DC=com
```

Step 8 Configure LDAP to initiate the TLS connection and specify the secure mode.

Example:

```
Device(config-ldap-server)# mode secure no- negotiation
```

Step 9 Return to the privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Example:

```
Device(config-ldap-server)# end
```

Configure a AAA server group (GUI)

Configure a AAA server group using the GUI for RADIUS, TACACS+, or LDAP server hosts using the GUI.

Configuring a device to use AAA server groups helps you group existing server hosts, select a subset of those hosts, and assign them for a particular service. A server group is used with a global server-host list. The server group lists the IP addresses of the selected server hosts.

You can create these server groups:

Before you begin

Procedure

Step 1 RADIUS

a) Choose **Services** > **Security** > **AAA** > **Server Groups** > **RADIUS**.
b) Click the **Add** button. The **Create AAA Radius Server Group** dialog box appears.
c) Enter a name for the RADIUS server group in the **Name** field.
d) Select a desired delimiter from the **MAC-Delimiter** drop-down list. The available options are colon, hyphen, and single-hyphen.
e) Select a desired filter from the **MAC-Filtering** drop-down list. The available options are mac and Key.

f) Enter a value in the **Dead-Time (mins)** field to make a server non-operational. You must specify a value between 1 and 1440.
g) Choose any of the available servers from the **Available Servers** list and move them to the **Assigned Servers** list by clicking the **>** button.
h) Click the **Save & Apply to Device** button.

Step 2 TACACS+

a) Choose **Services** > **Security** > **AAA** > **Server Groups** > **TACACS+**.
b) Click the **Add** button. The **Create AAA Tacacs Server Group** dialog box appears.
c) Enter a name for the TACACS server group in the **Name** field.
d) Choose any of the available servers from the **Available Servers** list and move them to the **Assigned Servers** list by clicking the **>** button.
e) Click the **Save & Apply to Device** button.

Step 3 LDAP

a) Choose **Services** > **Security** > **AAA** > **Server Groups** > **LDAP**.
b) Click the **Add** button. The **Create AAA Ldap Server Group** dialog box appears.
c) Enter a name for the LDAP server group in the **Name** field.
d) Choose any of the available servers from the **Available Servers** list and move them to the **Assigned Servers** list by clicking the **>** button.
e) Click the **Save & Apply to Device** button.

Configure a AAA server group (CLI)

Establish a AAA server group for centralized authentication, authorization, and accounting using commands.

AAA server groups allow you to centrally manage user access and policy enforcement with protocols such as LDAP, RADIUS, or TACACS+.

Procedure

Step 1 Enable the privileged EXEC mode.

Example:

```
Device# enable
```

Enter your password if prompted.

Step 2 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 3 Enable AAA.

Example:

```
Device(config)# aaa new-model
```

Step 4 Define the AAA server group with a group name and enter the LDAP server group configuration mode.

Example:

```
Device(config)# aaa group server ldap group-name
```

All members of a group are of the same type: RADIUS, LDAP, or TACACS+.

Step 5 Associate a particular LDAP server with the defined server group.

Example:

```
Device(config-ldap-sg)# server server-name
```

Each security server is identified by its IP address and UDP port number.

Step 6 Exit the LDAP server group configuration mode.

Example:

```
Device(config-ldap-sg)# exit
```

Configure search and bind operations for authentication requests (CLI)

Enable LDAP-based authentication by defining how the controller searches and binds user credentials during authentication requests using commands.

Configuring search and bind operations determines whether the LDAP server first binds the user and then performs a search, or compares credentials without binding. This affects how authentication requests are processed on the controller.

Procedure

Step 1 Enable the privileged EXEC mode.

Example:

```
Device# enable
```

Enter your password if prompted.

Step 2 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 3 Enable AAA.

Example:

```
Device(config)# aaa new-model
```

Step 4 Define a Lightweight Directory Access Protocol (LDAP) server and enter the LDAP server configuration mode.

Example:

```
Device(config)# ldap server server-name
```

Step 5 Configure the sequence of search and bind operations for an authentication request.

Example:

```
Device(config-ldap-server)# authentication bind-first
```

Step 6 Replace the bind request with the compare request for authentication.

Example:

```
Device(config-ldap-server)# authentication compare
```

Step 7 Exit the LDAP server group configuration mode.

Example:

```
Device(config-ldap-server)# exit
```

Configure a dynamic attribute map on a SLDAP server (CLI)

Configure dynamic LDAP attribute maps to ensure seamless interoperability between user-defined attribute names and Cisco attribute requirements on a wireless controller using commands.

You must create LDAP attribute maps that map your existing user-defined attribute names and values to Cisco attribute names and values that are compatible with the security appliance. You can then bind these attribute maps to LDAP servers or remove them as required.

Note To use the attribute mapping features correctly, make sure you understand Cisco LDAP and user-defined attribute names and values.

Before you begin

Procedure

Step 1 Enable privileged EXEC mode.

Example:

```
Device# enable
```

Enter your password if prompted.

Step 2 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 3 Configure a dynamic LDAP attribute map and enter the attribute-map configuration mode.

Example:

```
Device(config)# ldap attribute-map map-name
```

Step 4 Define an attribute map.

Example:

```
Device(config-attr-map)# map type ldap-attr-type aaa-attr-type
```

Step 5 Exit the attribute-map configuration mode.

Example:

```
Device(config-attr-map)# exit
```

Verify the SLDAP configuration

To view details about the default LDAP attribute mapping, use this command:

```
Device# show ldap attributes
```

To view the LDAP server state information and various other counters for the server, use this command:

```
Device# show ldap server
```