LDAP and AD Authentication

This page provides an overview of LDAP and AD Authentication configuration in LoopEdge.

- Overview
- Add an LDAP/AD Provider
- LDAP Provider Details
  - General Settings
  - Find LDAP Distinguished Names (DN)
  - Bind DN
  - Connection Settings
  - LDAP User Settings
  - Group Settings
    - User Groups
- Log In with Authentication

Overview

Each LoopEdge instance contains a default user registry for authentication and authorization. Loopedge LDAP and AD settings allow you to integrate the LoopEdge login system with an external authentication registry. For example, this external registry might be the username and password combinations for your company network.

LoopEdge Supports:

- Active Directory (AD).
- LDAP directories using the RFC2307/2307bis schema.
- Other LDAP directories are supported via direct attribute mapping.

What is LDAP?

Lightweight Directory Access Protocol (LDAP) provides centralized services for login authentication and storage/access of usernames and passwords within a network directory. LDAP uses group mechanisms to facilitate user authentication management. The Active Directory (AD) service authenticates users and devices in a Windows or UNIX-based domain network, and verifies permissions to determine the user access level at log in.

Add an LDAP/AD Provider

You must configure providers in LoopEdge to activate this type of authentication. The LoopEdge device contains a client that communicates with the LDAP server and receives information based on the client access level.

- LoopEdge Authentication Providers do not support nested groups. Create a separate group for each LoopEdge role in the LDAP Registry, and add users to these groups.
- Once you have added a provider, you need to select a provider on the LoopEdge login screen.
- LoopEdge should always have at least one administrator user. LDAP administrator users can meet this requirement.
To add an LDAP/AD provider:

1. In the LoopEdge navigation panel, choose **System > LDAP/AD Auth**.

2. Click **Add** to launch the Add Provider dialog.
3. Enter the configuration details, as described in **LDAP Provider Details**. Click **Create**.

**LDAP Provider Details**

For more information on LDAP / AD providers, see the following section. Use this guide to configure LDAP / AD with LoopEdge.

**General Settings**

**Name**: Enter a user-defined name.

**Type**: Currently only **generic** is valid.

**Add Provider**

1. **Generic**

   **Name**: [Input field]

   **Type**: **generic**

   [Next]

2. **Connection**

3. **User**

**Find LDAP Distinguished Names (DN)**

To configure LDAP for LoopEdge, you must have the DN information from the LDAP server.

**Bind DN**
An LDAP Bind DN supplies the user and the user location in the LDAP directory tree. The LDAP client configuration file contains this information. You can access it in the following directory:

/etc/ldap.conf

To find the Bind DN:

1. Log in to the Windows server connected to the Active Directory.
2. Identify the domain to query, for example: litmusautomation.com.
3. At the Windows command prompt, type the following command to retrieve a specific user.

   ```
   dsquery user dc=<domain_name>,dc=<domain_extension> -name <user_name>
   ```

   **Command Info:**
   - `dc` means domain component or context
   - `<domain_name>`: Replace this with your domain name, without the extension, like litmusautomation.
   - `<domain_extension>`: Replace this with your domain’s extension, like com.
   - `<user_name>`: Replace this with the user name to search.

4. To retrieve all users, enter the following into the command prompt:

   ```
   dsquery user dc=<domain_name>,dc=<domain_extension>
   ```

Connection Settings
**Host**: Enter the hostname, the fully qualified domain name or IP address, of your LDAP server.

**Port**: Enter the LDAP host port number. The default LDAPS (Secure LDAP) port is 636; the default LDAP port is 389.

**TLS**: Check this box to indicate that you want to use LDAP over Transport Layer Security (TLS) to authenticate Active Directory sessions. The TLS protocol provides authentication and data encryption between servers and applications on a network. **Note**: When this box is not checked, LoopEdge expects to find a configured Custom Certificate.

**TLSSCRT**: Enter the root SSL/TLS certificate.

**Sample Certificate**:

Make sure to include -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- when entering the certificate. See the following example for a sample certificate:

```
-----BEGIN CERTIFICATE-----
MIIFoYCCAgYgAwIBAgIBATANBgkqhkiG9w0BAQsFADBAMRowGAYDVQQKExFMaXRt
-----END CERTIFICATE-----
```

**Bind DN**: The bind DN identifies the user and the location of the user in the LDAP directory tree. In the following example:

CN=common name, OU=organizational unit, and DC=domain component.

```
CN=user1,CN=Users,DC=examplecompany,DC=com
CN=Manager,OU=IT,DC=examplecompany,DC=com
```

**Bind DN Password**: Enter the DN (distinguished name) password.

---

**LDAP User Settings**
**User Search Base DN:** This Base DN (Distinguished Name) is the point in the LDAP directory tree that the LDAP service uses to initiate a user search. The Base DN is the latter part of the Bind DN. See Find the LDAP Bind DN.

**Search Scope:** Select one of the following: base, one, sub. **Base** limits the search to the base object. **One** restricts the search to "one level" or in other words, the immediate children of the base object. **Sub** enables a full LDAP tree search, including all children of the base object.

**User Search Filter:** Enter a filter to search LDAP users.

**Attribute for Unique UserID:** Enter the unique user ID number (uidNumber).

**Attribute for Username:** Enter the unique user ID (uid).

**First Name:** Enter the given name of the user.

**Last Name:** Enter the surname of the user.

---

**Group Settings**

**User Groups**

⚠️ You must define the following groups on the LDAP / AD server to have users with different permissions in LoopEdge:

- **`loopedge-administrator`**: Full access to all features and all system configuration settings.
- **`loopedge-developer`**: Can view LoopEdge and use all of its features. Developers cannot alter the system configuration.
- **`loopedge-observer`**: Only views LoopEdge and cannot use any features, such as adding devices and tags. Observers cannot make any configuration changes.
**Group Search Base DN:** This Base DN (Distinguished Name) is the starting point that the LDAP service uses to find a group in the LDAP directory tree.

**Search Scope:** Select one of the following: base, one, sub. **Base** limits the search to the base object. **One** restricts the search to "one level", as in the immediate children of the base object. **Sub** enables a full LDAP tree search, including all children of the base object.

**Group Search Filter:** Enter a filter to query the Active Directory. Click here for a reference to help guide you in creating search filters.

**Group Name Attribute:** Enter the common name (CN) for the group to search.

**Group Membership Attribute:** Enter the distinguished name (DN) for the group to search.

**Member Value Type:** Enter the value type for members in the group, DN or CN.

---

**LDIF Info:**

The LDAP LDIF (LDAP Interchange Format) file can define attributes, such as user access control permissions. The following example shows the LDIF format for the mydom organization.

```
 dn: cn=employees,ou=Groups,dc=mydom,dc=com
 changetype: modify
 add: memberUid
 memberUid: arc815
```

**Example of a Group Base DN:**

```
CN=Users,CN=Builtin,DC=MyDomain,DC=com
```

**Example of a filter to query group objects with a common name (CN) starting with Admin:**

```
(&(objectCategory=group)(cn=Admin*))
```
Log In with Authentication

After configuring LDAP, users must select a **Provider ID** when they log in to LoopEdge.

⚠️ The **Username** is from the LDAP server. The **Password** must match the **Bind DN Password** from the configuration.
The internal authentication provider appears in the ID selection list. If you do not select another ID, LoopEdge uses this non-configurable, default provider ID.