



How to Set Up Active Directory and LDAP on Mattermost

Introduction

Companies of all shapes and sizes use directory services to help them manage users and resources within their organization. A “directory service” is defined as a repository for storing and managing information in a hierarchical structure. Most companies prefer to manage user identity and access policies in one place for greater ease and efficiency. In this case, your directory service becomes the “system of truth”—the go-to authority on the most current user data.

Most likely, your company maintains a constellation of systems that store user accounts and require login. Mattermost may be one such system. With a simple point-and-click UI, Mattermost makes it easy to establish a secure connection with your directory service and use the same policies and attributes to authenticate users, synchronize data, and control access to your messaging platform.

Some high-compliance enterprises, such as government agencies, need to be able to show regulators how they are controlling access to sensitive data. Mattermost gives you full control over user data behind your firewall or in your AWS or Azure private cloud. When syncing user data between your directory service and Mattermost, data is handled securely and in compliance with your company policies.

If your company uses Active Directory with the LDAP protocol, this guide will walk you through the basics of AD/LDAP setup on Mattermost. AD/LDAP integrated support is available with Mattermost Professional and Enterprise Editions.

“We originally started by using the Mattermost version that came bundled in the GitLab Omnibus package, but we eventually migrated to Mattermost Enterprise Edition in order to get LDAP authentication and enterprise support.”

Dan West, IT Systems Administrator, Galois

In This Guide

Part 1: Overview of AD/LDAP

LDAP Objects and Information Structure

How Mattermost Connects to LDAP

Part 2: User Authentication & Synchronization

Basic Configuration

Advanced Configuration

Part 3: Group Synchronization

Basic Configuration

Group-Synced Teams/Channels

Next Steps

Overview of AD/LDAP

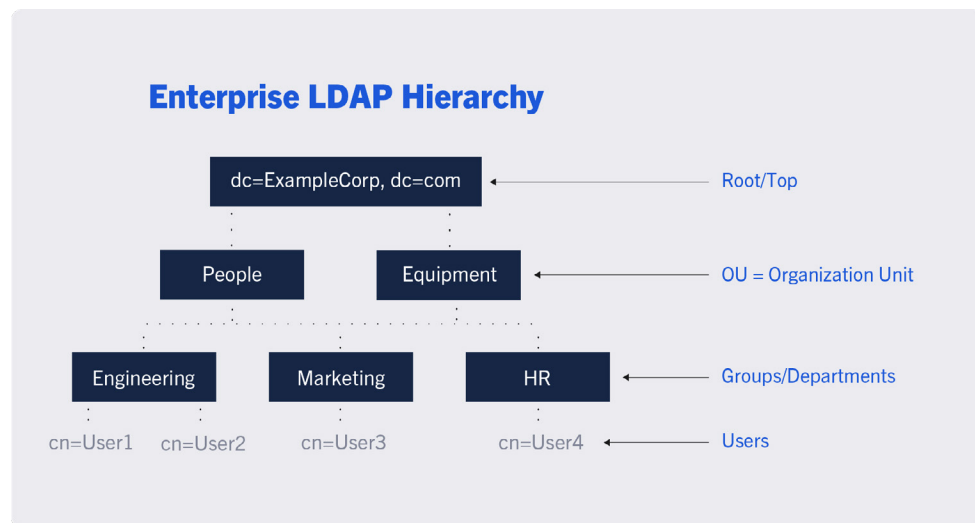
Active Directory (AD) is Microsoft's implementation of a directory service that supports the Lightweight Directory Access Protocol (LDAP) for querying and accessing data. LDAP is a TCP/IP network protocol and set of access methods for interfacing and querying directory information. It's not necessarily its own system; it's how you access data in a system. There are many different variations of AD/LDAP setups and structures using services such as OpenLDAP, Active Directory Federation Services (ADFS), Active Directory forests, Azure Active Directory, and more.

Regardless of your organization's unique AD/LDAP setup, a few foundational concepts can help you better understand how to map user and group data in Active Directory to Mattermost.

LDAP Objects and Information Structure

When you run a query, LDAP uses a particular information hierarchy and syntax to return the correct data. Within a directory, a typical enterprise LDAP hierarchy stems from the root, which would be your company domain. From there, data is handled as distinct objects.

The first level specifies high-level “organizational units,” which may be people or a category of “things,” such as equipment or network resources. The next level determines groupings of individual records (e.g., users or things), such as by department or location, which may be shared across relevant organizational units. Finally, individual records are mapped to a particular group. The object’s entire path back to the root is called a “distinguished name.”



LDAP Syntax:

- **dc** = domain component. This is your company’s domain.
- **ou** = organizational unit. It may hold objects or other ous.
- **cn** = common name. This can be an individual or group.
- **dn** = distinguished name. It includes the object’s entire path to the root.

Here's an example:

Carlos Santana is a marketing manager at Acme Corp. His record is stored as an LDAP object in the cn=Users container, which is linked to the cn=Marketing group and falls within the ou=People organizational unit. The full distinguished name path would be:

```
cn=CSantana, cn=Marketing, ou=People, dc=AcmeCorp
```

To specify a particular object—in this case, CSantana—you must specify the distinguished name.

How Mattermost Connects to LDAP

When Mattermost connects to an Active Directory system via LDAP, it uses a process called “binding.” This happens in three basic steps:

1. Mattermost establishes a session with the AD/LDAP server by specifying the host name or IP address and port number of your organization's listening AD/LDAP server. This connection can include TLS encryption that's configurable.
2. Your server authenticates the Mattermost LDAP client with a username and password.
3. Your server grants the client access to your directory data and starts to perform operations. In Mattermost, this entails searching for objects (based on filters) and reading data (e.g., entries and attributes).

The binding process enables you to synchronize data between your Active Directory and Mattermost. Once set, Mattermost will be able to read information from your AD/LDAP server and apply that information to the Mattermost database.

Case Study



As their globally-distributed community and team grew, Rocky Linux ultimately decided that they needed a messaging and collaboration solution that delivered a modern feature set and could connect with other messaging platforms. LDAP integration is a must-have, since Rocky Linux provides account services for identity management across various platforms. “We liked the fact that we could host Mattermost on our own infrastructure, granting us sovereignty over our data and the flexibility to architect our infrastructure how we see fit,” says Jordan Pisaniello, Rocky Linux community manager.

[Read their story »](#)

User Authentication & Synchronization

Mattermost's AD/LDAP integration provides a secure way to authenticate users (based on your Active Directory stored attributes) and synchronize data as you onboard or update users. This makes it easier for system administrators to control who gets access to Mattermost and prevent unauthorized usage. User authentication and synchronization with AD/LDAP are available in Mattermost Professional and Enterprise Editions.

By using this feature, you can streamline three key functions for both users and administrators:

Centralized Identity Management

- User attributes are mapped from your AD/LDAP server to Mattermost and other applications, so each user is identified in the same way across multiple systems.
- Attributes are updated in Mattermost when they're changed on the LDAP server. This helps to maintain the "source of truth" for each user.

Single Sign-on

- Users can use the same AD/LDAP credentials for Mattermost as they do for other systems within your organization. There's no need for users to create or maintain a unique Mattermost login profile.

Automatic Account Provisioning

- When users first log in to Mattermost, they are verified by LDAP as “active” in your system and an account is automatically created.
- When users are identified as “deactivated” by the AD/LDAP server, they are subsequently deactivated on Mattermost and their sessions are revoked on the next synchronization or login attempt.

Basic Configuration

Mattermost gives you two options for setting up your AD/LDAP integration. The following guidelines describe the most common method, which is using Mattermost’s simple, straightforward UI in the System Console. Alternatively, you can choose to edit the `config.json` file. For full information, read the documentation for [AD/LDAP Setup](#) and [AD/LDAP Configuration Settings](#).

1. Enable sign-in with AD/LDAP

Configure Mattermost to allow users to log in with their Active Directory credentials.

Note: If you want users to only use AD/LDAP to sign in, you have the option to disable email address account creation.

2. Enable synchronization with AD/LDAP

Choose how you want Mattermost to synchronize users and pull attributes from the AD/LDAP server. You can have Mattermost run this

process periodically or only during user login.

3. Bind Mattermost to your LDAP server

Create the connection needed to synchronize data by entering the domain or IP address of your AD/LDAP server. Configure other connection settings, such as port, security, and certificate verification.

Note: A button further down on this screen allows you to manually test the connection and ensure that it's set up correctly.

4. Set your BaseDN

Configure the distinguished name path that specifies where Mattermost should begin its search for users in your AD/LDAP hierarchy.

5. Set the bind username/password

Configure the login that your authorized administrator(s) will use to perform an AD/LDAP search. Typically, this is an account created specifically for use with Mattermost that allows access to the portion of the AD/LDAP tree specified in the BaseDN field.

6. Set user filters (Optional)

If you want only a subset of users in your organization to access Mattermost, enter an AD/LDAP filter to use when searching for user objects. Use this filter to also define an LDAP-disabled user. Note that a good way to test that everything is working as expected is in a separate

testing environment before deploying to production.

7. Map user attributes

Enable a range of user attributes to sync from your AD/LDAP server to Mattermost. Users will not be able to edit attributes that are synced. However, you can choose to leave some attributes blank and allow users to set their own. Keep the following tips in mind:

- **User ID** — This uniquely identifies a user in Mattermost and should be an AD/LDAP attribute with a value that does not change. If a user's ID attribute changes, it will create a new Mattermost account that is not associated with their old one, which may cause confusion for users and administrators.
- **Login ID** — This is what the user uses to sign in to Mattermost (usually the same as the Username attribute). However, if your team typically uses “domain/username” to log in to other services with AD/LDAP credentials, then you may want to specify the same format in this field to maintain consistency between sites.

8. Set up synchronization and query preferences

You can configure how often you want to synchronize data (the default interval is 60 minutes), the maximum number of objects in each query, and the query timeout.

Note: A button further down on this screen allows you to manually synchronize data whenever needed.

Advanced Configuration

Mattermost supports more complex use cases associated with user authentication and data synchronization. The following are a few typical advanced scenarios.

Using AD/LDAP with SAML

If your organization authenticates using Security Assertion Markup Language (SAML), you can include it in your AD/LDAP setup on Mattermost. SAML is an open standard that allows identity providers, like OneLogin, to pass authorization credentials to service providers, like Mattermost. AD/LDAP with SAML is available in Mattermost Professional and Enterprise Editions. For more information, read [Mattermost's SAML documentation](#).

In this setup, SAML is the primary authentication method for single sign-on. When configured:

- Mattermost queries AD/LDAP for relevant account information and updates SAML-authenticated Mattermost accounts based on changes to attributes (e.g., first name, last name, and nickname).
- Accounts disabled in AD/LDAP are made inactive in Mattermost, and their active sessions are revoked once Mattermost synchronizes.

Active Directory Forest

Mattermost currently supports single forest structures with multiple

domains. Find more information on this in the [AD/LDAP Setup documentation](#).

Multiple LDAP systems

Mattermost currently does not provide in-product support for multiple LDAP systems. However, customers have been successful using an IdP broker or Azure Active Directory to map multiple systems into a single system. Learn more about these solutions in [this blog post](#).

Case Study



As they prepared for NASA's first asteroid sample collection mission, the OSIRIS-REx team needed a collaboration solution that would let them maintain data sovereignty and protect highly sensitive mission data. Mattermost helps keep their data secure while working well with other essential tools, including Git, Jira, and their LDAP instance.

[Read their story »](#)

Group Synchronization

Mattermost makes user onboarding and account management even easier by allowing you to set default team and channel membership based on your AD/LDAP groups. This is useful when you have a large number of users to onboard at one time, you onboard users frequently, or you want to ensure users are automatically added to specific teams and channels.

Additionally, Mattermost also allows you to create teams and channels that are only accessible to specific synced groups. The LDAP group sync feature is available to customers using Mattermost Enterprise Edition. For more information, read the [AD/LDAP Groups documentation](#).

This feature makes it easier for administrators to onboard users and manage accounts:

Onboarding

- Users can be grouped based on department, security classification level, location, or other designation. Groups can then be mapped to default teams and channels based on the structure of your organization.

Mattermost Adoption

- Users already have access to the teams and channels most pertinent to them and can start messaging upon first login. This speeds up adoption as users don't have to search and discover channels of interest themselves.

Access Controls

- Users outside of a group can be prevented from accessing private teams or channels.
- Users can be automatically removed from a team or channel when removed from the group.

Basic Configuration

In both your AD/LDAP structure and in Mattermost, a user group is defined as a collection of individual users and is handled as a unique object designated with a common name (e.g., cn=Marketing). At this time, user groups in Mattermost can only be created by linking AD/LDAP groups to Mattermost groups. Currently, it isn't possible to manually create a user group directly in Mattermost.

The Mattermost System Console makes it easy to set up groups based on AD/LDAP attributes, synchronize group data, and designate private “group constrained” teams and channels. For full information, read the [documentation for LDAP Group Sync](#).

Steps to Configure AD/LDAP Group Sync in the Mattermost System Console:

1. In Authentication > AD/LDAP:

- Set Group Display Name - This is the attribute in the AD/ LDAP server used to populate the group display names.
- Map Group ID - Similar to the User ID, this is a unique Access Controls identifier associated with a user group. This should be an AD/LDAP attribute with a value that does not change.
- Users outside of a group can be prevented from accessing private teams or channels.
- Users can be automatically removed from a team or channel when removed from the group.
- Set Group Filters (optional) - Similar to user filters, if you want only certain groups to access Mattermost, enter an AD/LDAP filter to use when searching for user group objects.

Note: Only manually linked groups are available to Mattermost (regardless of whether this filter is left blank or not). However, if you find that the groups list view is loading slowly or the background sync job is slow, then the filter may help. Try setting a filter to limit the number of groups that Mattermost must load and parse.

2. Synchronize group data:

You can either let your synchronization process run per your usual setup or you can run a manual synchronization from the AD/LDAP Set Up screen.

3. In User Management > Groups:

Based on your filters, Mattermost returns a list of groups during synchronization. When they come in the first time, they will all be unlinked. The next step is to finalize the connection with to Mattermost for each group individually:

- Manually select the group(s) you want to link to Mattermost.
- Set default team and channel membership for the selected groups (optional).
- Once a group member logs in to Mattermost, the user will be associated with the Mattermost group and the username will be populated in this view.
- Users will also be automatically added into the designated team or channel as they're added to the group.
- Once the group is configured, you can go back and edit or remove channels as needed.

Group-Synced Teams/Channels

Team administrators already have the ability to create public and private channels and invite users. However, they can also enlist the Mattermost system administrator to help them set a group policy for a team or channel, which limits access to a particular user group.

The following guidelines describe how to set a group policy for a team. Setting a group policy for a channel would follow the same steps.

1. In User Management > Teams:

- Locate the profile page of a particular team.
- Configure access settings. Options include:
 - » Allow anyone to discover and join the team.
 - » Allow only specific whitelisted email domains to join the team.
 - » Allow only synced group members. When enabled, this controls membership of this team to this group. Adding and removing users from the group will add or remove them from this team. In this option, the only way of inviting members to this team is by adding them to the group, which will override public access to the team.
 - » If users leave a group-synced team (or channel), they can be re-added with an at-mention, the team invite flow, or the /join slash command.

2. In Authentication > AD/LDAP:

- Manually run the AD/LDAP synchronization process by clicking the button further down on the screen.

Next Steps

Mattermost is an open source platform for secure collaboration across the entire software development lifecycle. Active Directory and LDAP are available on two versions of Mattermost:

- **Mattermost Professional Edition** is a scalable solution for growing teams with requirements for data security and commercial support.
- **Mattermost Enterprise Edition** includes added data control and compliance capabilities for the most security-conscious organizations. It is ideal for companies in regulated industries, government organizations, and DevOps and IT security teams.

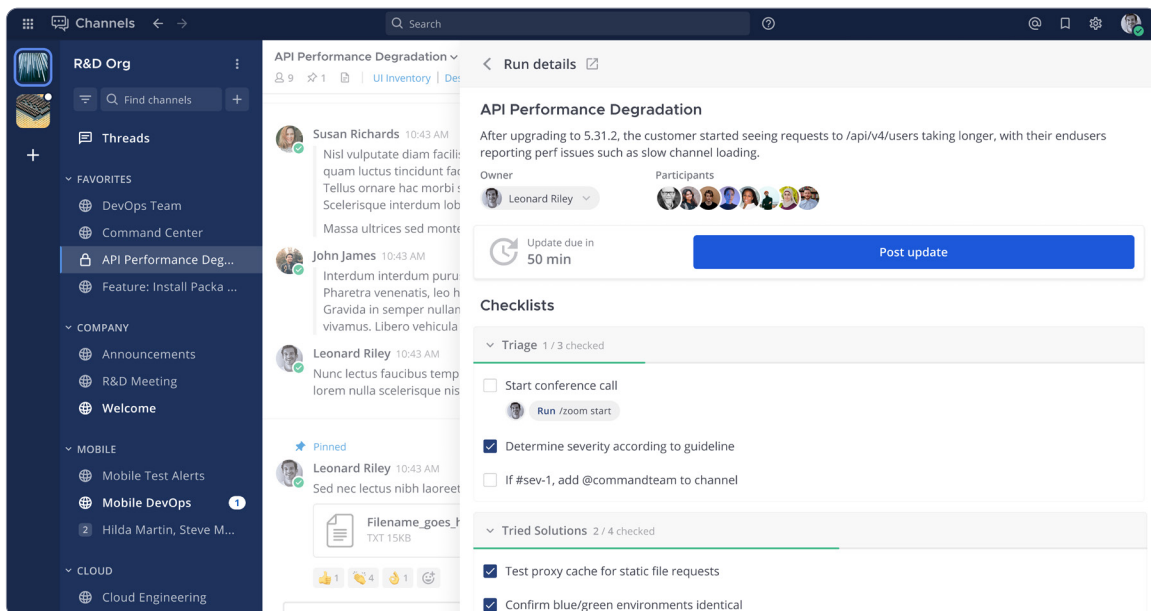
About Mattermost

Mattermost is the leading collaboration platform for mission-critical work. We serve national security, government, and critical infrastructure enterprises, from the U.S. Department of Defense, to global tech giants, to utilities, banks and other vital services. We accelerate out-of-band incident response, Dev/Sec/Ops workflow, and self-sovereign collaboration to bolster the focus, adaptability and resilience of the world's most important organizations.

Our enterprise software and single-tenant SaaS platforms are built to meet the custom needs of rigorous and complex environments while offering a secure and unrivaled collaboration experience across web, desktop and mobile with channel-based messaging, file sharing, audio calling and screen share, with integrated tooling, workflow automation and AI assistance.

Mattermost is developed on an open core platform vetted by the world's leading security organizations, and co-built with over 4,000 open source project contributors who've provided over 30,000 code improvements towards our shared vision of accelerating the world's mission critical work.

For more information visit www.mattermost.com.





Mattermost