Using LDAP

In this article

If you use Lightweight Directory Access Protocol (LDAP) to centralize access across applications, you can integrate GitHub Enterprise Server by configuring LDAP authentication for your instance.

About LDAP authentication for GitHub Enterprise Server

LDAP is a popular application protocol for access and maintenance of directory information services, and is one of the most common protocols for integration of third-party software with large company user directories. For more information, see "Lightweight Directory Access Protocol" on Wikipedia.

If you use an LDAP directory for centralized authentication, you can configure LDAP authentication for the people who use your GitHub Enterprise Server instance.

Note: You can use either SAML or LDAP, but not both.

If you want to allow authentication for some people who don't have an account on your external authentication provider, you can allow fallback authentication to local accounts on your GitHub Enterprise Server instance. For more information, see "Allowing built-in authentication for users outside your provider."

Supported LDAP services

GitHub Enterprise Server integrates with these LDAP services:

- Active Directory
- FreeIPA
- Oracle Directory Server Enterprise Edition
- OpenLDAP
- Open Directory

- 389-ds

Username considerations with LDAP

GitHub Enterprise Server normalizes a value from your external authentication provider to determine the username for each new personal account on your GitHub Enterprise Server instance. For more information, see "Username considerations for external authentication."

Configuring LDAP with your GitHub Enterprise Server instance

After you configure LDAP, users will be able to sign into your instance with their LDAP credentials. When users sign in for the first time, their profile names, email addresses, and SSH keys will be set with the LDAP attributes from your directory.

When you configure LDAP access for users via the Management Console, your user licenses aren't used until the first time a user signs in to your instance. However, if you create an account manually using site admin settings, the user license is immediately accounted for.

> **Warning:** Before configuring LDAP on your GitHub Enterprise Server instance, make sure that your LDAP service supports paged results.

1. From an administrative account on GitHub Enterprise Server, in the upper-right corner of any page, click 🚀.
2. If you're not already on the "Site admin" page, in the upper-left corner, click **Site admin**.
3. In the "🚀 Site admin" sidebar, click **Management Console**.
4. In the "Settings" sidebar, click **Authentication**.
5. Under "Authentication", select **LDAP**.
6. Optionally, to allow people without an account on your external authentication system to sign in with built-in authentication, select **Allow built-in authentication**. For more information, see "Allowing built-in authentication for users outside your provider."
7. Add your configuration settings.

LDAP attributes

Use these attributes to finish configuring LDAP for your GitHub Enterprise Server instance.

Attribute name	Required	Description
`Host`	✓	The LDAP host, e.g. `ldap.example.com` or `10.0.0.30`. If the hostname is only available from your internal network, you may need to configure your GitHub Enterprise Server instance's

		DNS first so it can resolve the hostname using your internal nameservers.
`Port`	✓	The port the host's LDAP services are listening on. Examples include: 389 and 636 (for LDAPS).
`Encryption`	✓	The encryption method used to secure communications to the LDAP server. Examples include plain (no encryption), SSL/LDAPS (encrypted from the start), and StartTLS (upgrade to encrypted communication once connected).
`Domain search user`	✗	The LDAP user that looks up other users that sign in, to allow authentication. This is typically a service account created specifically for third-party integrations. Use a fully qualified name, such as `cn=Administrator,cn=Users,dc=Example,dc=com`. With Active Directory, you can also use the `[DOMAIN]\[USERNAME]` syntax (e.g. `WINDOWS\Administrator`) for the domain search user with Active Directory.
`Domain search password`	✗	The password for the domain search user.
`Administrators group`	✗	Users in this group are promoted to site administrators when signing into your appliance. If you don't configure an LDAP Administrators group, the first LDAP user account that signs into your appliance will be automatically promoted to a site administrator.
`Domain base`	✓	The fully qualified `Distinguished Name` (DN) of an LDAP subtree you want to search for users and groups. You can add as many as you like; however, each group must be defined in the same domain base as the users that belong to it. If you specify restricted user groups, only users that belong to those groups will be in scope. We recommend that you specify the top level of your LDAP directory tree as your domain base and use restricted user groups to control access.
`Restricted user groups`	✗	If specified, only users in these

		groups will be allowed to log in. You only need to specify the common names (CNs) of the groups, and you can add as many groups as you like. If no groups are specified, *all* users within the scope of the specified domain base will be able to sign in to your GitHub Enterprise Server instance.
`User ID`	✓	The LDAP attribute that identifies the LDAP user who attempts authentication. Once a mapping is established, users may change their GitHub Enterprise Server usernames. This field should be `sAMAccountName` for most Active Directory installations, but it may be `uid` for other LDAP solutions, such as OpenLDAP. The default value is `uid`.
`Profile name`	✗	The name that will appear on the user's GitHub Enterprise Server profile page. Unless LDAP Sync is enabled, users may change their profile names.
`Emails`	✗	The email addresses for a user's GitHub Enterprise Server account.
`SSH keys`	✗	The public SSH keys attached to a user's GitHub Enterprise Server account. The keys must be in OpenSSH format.
`GPG keys`	✗	The GPG keys attached to a user's GitHub Enterprise Server account.
`Disable LDAP authentication for Git operations`	✗	If selected, turns off users' ability to use LDAP passwords to authenticate Git operations.
`Enable LDAP certificate verification`	✗	If selected, turns on LDAP certificate verification.
`Synchronization`	✗	If selected, turns on LDAP Sync.

Disabling password authentication for Git operations

To enforce use of personal access tokens or SSH keys for Git access, which can help prevent your server from being overloaded by LDAP authentication requests, you can disable password authentication for Git operations.

We recommend this setting because a slow-responding LDAP server, especially combined with a large number of requests due to polling, is a frequent source of performance issues and outages.

To disable password authentication for Git operations, select **Disable username and**

password authentication for Git operations in your LDAP settings.

When this option is selected, if a user tries to use a password for Git operations via the command line, they will receive an error message that says, `Password authentication is not allowed for Git operations. You must use a personal access token.`

Enabling LDAP certificate verification

You can validate the LDAP server certificate you use with TLS by enabling LDAP certificate verification.

To enable LDAP certificate verification, select **Enable LDAP certificate verification** in your LDAP settings.

When this option is selected, the certificate is validated to make sure:

- If the certificate contains at least one Subject Alternative Name (SAN), one of the SANs matches the LDAP hostname. Otherwise, the Common Name (CN) matches the LDAP hostname.
- The certificate is not expired.
- The certificate is signed by a trusted certificate authority (CA).

Enabling LDAP Sync

You can establish role-based access control for users from your LDAP server by synchronizing GitHub Enterprise Server users and team membership against your established LDAP groups. For more information, see "Creating a team."

Note: Using LDAP Synchronization with groups that exceed 1499 members may lead to team membership synchronization failures.

If you use Active Directory specifically, user lookups and team synchronization may fail when the LDAP groups configured for teams or in the Management Console exceed 1500 members, due to the `MaxValRange` limit in Active Directory. As a workaround, you can use Active Directory groups that contain less than 1500 members, or you can work with your Active Directory administrator to increase the `MaxValRange` value for your domain controllers. For more information, see View and set LDAP policy in Active Directory by using Ntdsutil.exe in Microsoft Learn.

If you need help determining if modifying the `MaxValRange` is the right approach for your Active Directory environment, contact Microsoft Support.

To enable LDAP Sync, in your LDAP settings, select **Synchronize Emails**, **Synchronize SSH Keys**, or **Synchronize GPG Keys** .

After you enable LDAP sync, a synchronization job will run at the specified time interval to perform the following operations on each user account:

- If you've allowed built-in authentication for users outside your identity provider, and the user is using built-in authentication, move on to the next user.
- If no LDAP mapping exists for the user, try to map the user to an LDAP entry in the directory. If the user cannot be mapped to an LDAP entry, suspend the user and move on to the next user.
- If there is an LDAP mapping and the corresponding LDAP entry in the directory is missing, suspend the user and move on to the next user.
- If the corresponding LDAP entry has been marked as disabled and the user is not already suspended, suspend the user and move on to the next user.
- If the corresponding LDAP entry is not marked as disabled, and the user is suspended, and *Reactivate suspended users* is enabled in the Admin Center, unsuspend the user.
- If one or more restricted user groups are configured on the instance and the

corresponding LDAP entry is not in one of these groups, suspend the user.

- If one or more restricted user groups are configured on the instance, the corresponding LDAP entry is in one of these groups, and *Reactivate suspended users* is enabled in the Admin Center, unsuspend the user.
- If the corresponding LDAP entry includes a `name` attribute, update the user's profile name.
- If the corresponding LDAP entry is in the Administrators group, promote the user to site administrator.
- If the corresponding LDAP entry is not in the Administrators group, demote the user to a normal account, unless the account is suspended. Suspended administrators will not be demoted and will remain listed on the "Site admins" and "Enterprise owners" pages.
- If an LDAP User field is defined for emails, synchronize the user's email settings with the LDAP entry. Set the first LDAP `mail` entry as the primary email.
- If an LDAP User field is defined for SSH public keys, synchronize the user's public SSH keys with the LDAP entry.
- If an LDAP User field is defined for GPG keys, synchronize the user's GPG keys with the LDAP entry.

> **Note**: LDAP entries can only be marked as disabled if you use Active Directory and the `userAccountControl` attribute is present and flagged with `ACCOUNTDISABLE`. Some variations of Active Directory, such as AD LDS and ADAM, don't support the `userAccountControl` attribute.

A synchronization job will also run at the specified time interval to perform the following operations on each team that has been mapped to an LDAP group:

- If a team's corresponding LDAP group has been removed, remove all members from the team.

- If LDAP member entries have been removed from the LDAP group, remove the corresponding users from the team. If the user is no longer a member of any team in the organization and is not an owner of the organization, remove the user from the organization. If the user loses access to any repositories as a result, delete any private forks the user has of those repositories.

  > **Note:** LDAP Sync will not remove a user from an organization if the user is an owner of that organization. Another organization owner will need to manually remove the user instead.

- If LDAP member entries have been added to the LDAP group, add the corresponding users to the team. If the user regains access to any repositories as a result, restore any private forks of the repositories that were deleted because the user lost access in the past 90 days.

As part of its optimization configuration, LDAP Sync will not transfer your nested team structure. To create child and parent team relationships, you must manually recreate the nested team structure and sync it with the corresponding LDAP group. For more information, see "Creating a team"

> **Security Warning:**
>
> When LDAP Sync is enabled, site admins and organization owners can search the LDAP directory for groups to map the team to.
>
> This has the potential to disclose sensitive organizational information to contractors or other unprivileged users, including:
>
> - The existence of specific LDAP Groups visible to the *Domain search user*.
> - Members of the LDAP group who have GitHub Enterprise Server user accounts, which is disclosed when creating a team synced with that LDAP group.

If disclosing such information is not desired, your company or organization should restrict the permissions of the configured *Domain search user* in the admin console. If such restriction isn't possible, contact us by visiting GitHub Enterprise Support.

Supported LDAP group object classes

GitHub Enterprise Server supports these LDAP group object classes. Groups can be nested.

- `group`
- `groupOfNames`
- `groupOfUniqueNames`
- `posixGroup`

Viewing and creating LDAP users

You can view the full list of LDAP users who have access to your instance and provision new users.

1. Sign in to your GitHub Enterprise Server instance at `http(s)://HOSTNAME/login`.
2. From an administrative account on GitHub Enterprise Server, in the upper-right corner of any page, click 🚀.
3. If you're not already on the "Site admin" page, in the upper-left corner, click **Site admin**.
4. In the left sidebar, click **LDAP users**.
5. To search for a user, type a full or partial username and click **Search**. Existing users will be displayed in search results. If a user doesn’t exist, click **Create** to provision the new user account.

Updating LDAP accounts

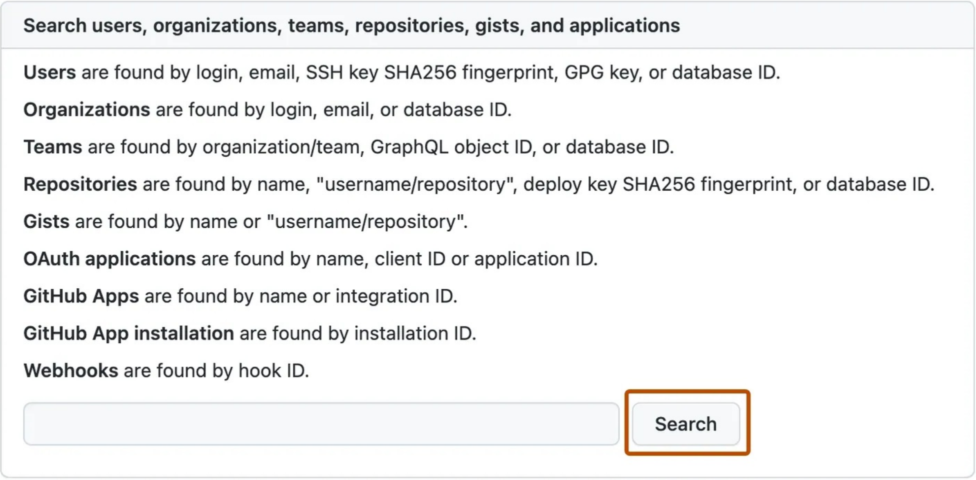
Unless LDAP Sync is enabled, changes to LDAP accounts are not automatically synchronized with GitHub Enterprise Server.

- To use a new LDAP admin group, users must be manually promoted and demoted on GitHub Enterprise Server to reflect changes in LDAP.
- To add or remove LDAP accounts in LDAP admin groups, promote or demote the accounts on GitHub Enterprise Server.
- To remove LDAP accounts, suspend the GitHub Enterprise Server accounts.

Manually syncing LDAP accounts

1. Sign in to your GitHub Enterprise Server instance at `http(s)://HOSTNAME/login`.
2. From an administrative account on GitHub Enterprise Server, in the upper-right corner of any page, click 🚀.
3. If you're not already on the "Site admin" page, in the upper-left corner, click **Site admin**.
4. Under "Search users, organizations, teams, repositories, gists, and applications", type the name of the user in the text field.

5. To the right of text field, click **Search**.



Search users, organizations, teams, repositories, gists, and applications

Users are found by login, email, SSH key SHA256 fingerprint, GPG key, or database ID.

Organizations are found by login, email, or database ID.

Teams are found by organization/team, GraphQL object ID, or database ID.

Repositories are found by name, "username/repository", deploy key SHA256 fingerprint, or database ID.

Gists are found by name or "username/repository".

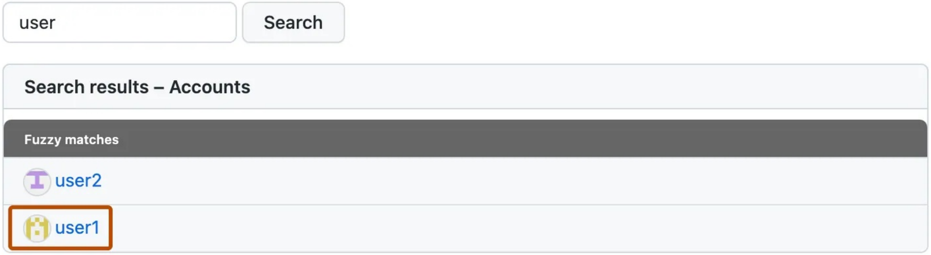
OAuth applications are found by name, client ID or application ID.

GitHub Apps are found by name or integration ID.

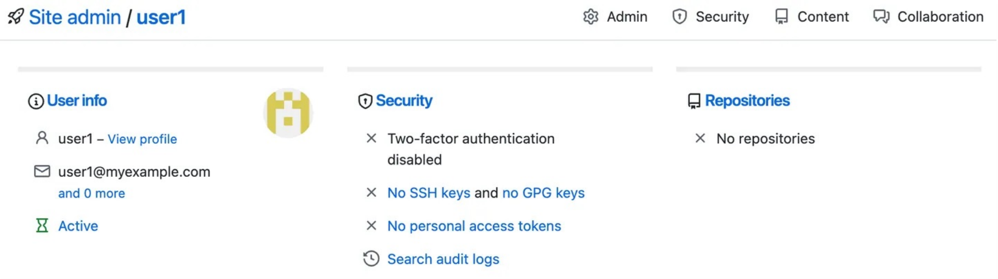
GitHub App installation are found by installation ID.

Webhooks are found by hook ID.

   - If an exact account name match isn't found, under "Search results – Accounts", in the "Fuzzy matches" section, click the name of the user you want to manage.



6. Review the user details in the site admin page to confirm you have identified the correct user.



user1 – View profile

user1@myexample.com
and 0 more

Active

Two-factor authentication disabled

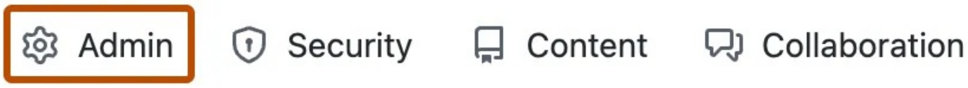
No SSH keys and no GPG keys

No personal access tokens

Search audit logs

No repositories

7. In the upper-right corner of the page, click ⚙ **Admin**.



8. Under "LDAP," click **Sync now** to manually update the account with data from your LDAP server.

You can also [use the API to trigger a manual sync](#).

Revoking access to your GitHub Enterprise Server

instance

If LDAP Sync is enabled, removing a user's LDAP credentials will suspend their account after the next synchronization run.

If LDAP Sync is **not** enabled, you must manually suspend the GitHub Enterprise Server account after you remove the LDAP credentials. For more information, see "Suspending and unsuspending users".

About logging for LDAP

Log events for LDAP appear in systemd journal logs on your GitHub Enterprise Server instance. You'll find events related to LDAP operations in the logs for `github-unicorn` and `github-resqued`. For more information, see "About system logs."