Guides for GitHub Enterprise

Learn how to increase developer productivity and code quality with GitHub Enterprise Server.

Enterprise administrators learning paths

Learning paths are a collection of guides that help you master a particular subject.

Deploy an instance

Install GitHub Enterprise Server on your platform of choice and configure SAML authentication.

Start learning path →

1. Overview System overview
2. How-to guide Installing GitHub Enterprise
3. How-to guide Administering your instance from the web UI
4. How-to guide Configuring the hostname for your instance
5. Using SAML for enterprise IAM
6. Reference Site admin dashboard

Upgrade your instance

Test upgrades in staging, notify users of maintenance, and upgrade your instance for the latest features and security updates.

Start learning path →

1. How-to guide Enabling automatic update checks
2. How-to guide Setting up a staging instance
3. Reference Upgrade requirements
4. How-to guide Customizing user messages for your enterprise
5. How-to guide Enabling and scheduling maintenance mode
6. How-to guide Upgrading GitHub Enterprise Server

Adopt GitHub Actions for your enterprise

Learn how to plan and implement a rollout of GitHub Actions in your enterprise.

Start learning path →

1. Overview About GitHub Actions for enterprises
2. Overview Understanding GitHub Actions
3. How-to guide Introducing GitHub Actions to your enterprise
4. How-to guide Migrating your enterprise to GitHub Actions
5. How-to guide Getting started with GitHub Actions for GitHub Enterprise Server
6. Quickstart Getting started with self-hosted runners for your enterprise
7. Overview Security hardening for GitHub Actions

Increase the fault tolerance of your instance

Back up your developers' code and configure high availability (HA) to ensure the reliability of GitHub Enterprise Server in your environment.

Start learning path →

1. How-to guide Accessing the administrative shell (SSH)
2. How-to guide Configuring backups on your instance
3. Overview About high availability configuration
4. How-to guide Creating a high availability replica
5. How-to guide Using GitHub Enterprise Server with a load balancer

Improve the security of your instance

Review network configuration and security features, and harden the instance running GitHub Enterprise Server to protect your enterprise's data.

Start learning path →

1. How-to guide Enabling private mode
2. How-to guide Configuring TLS
3. How-to guide Troubleshooting TLS errors
4. How-to guide Enabling subdomain isolation
5. How-to guide Accessing the administrative shell (SSH)
6. Reference Network ports
7. How-to guide Configuring built-in firewall rules
8. Reference Best practices for user security
9. How-to guide Promoting or demoting a site administrator

Configure GitHub Actions

Allow your developers to create, automate, customize, and execute powerful software development workflows for your GitHub Enterprise Server instance with GitHub Actions.

Start learning path →

1. How-to guide Getting started with GitHub Actions for GitHub Enterprise Server
2. How-to guide Enforcing policies for GitHub Actions in your enterprise
3. How-to guide Enabling automatic access to GitHub.com actions using GitHub Connect
4. Reference High availability for GitHub Actions
5. How-to guide Backing up and restoring GitHub Enterprise Server with GitHub Actions enabled
6. How-to guide Using a staging environment

Configure GitHub Advanced Security

Improve the quality and security of your developers' code with GitHub Advanced Security.

Start learning path →

1. Overview About billing for GitHub Advanced Security
2. How-to guide Enabling GitHub Advanced Security for your enterprise
3. How-to guide Configuring code scanning for your appliance
4. How-to guide Configuring dependency review for your appliance
5. How-to guide Configuring secret scanning for your appliance
6. How-to guide Enforcing policies for code security and analysis for your enterprise

All Enterprise administrators guides

102 guides found

Allowing built-in authentication for users outside your provider

HOW-TO GUIDE

You can configure fallback authentication to allow built-in authentication for people who don't have an account on your CAS, LDAP, or SAML authentication provider.

Accounts Authentication Enterprise Identity

Changing authentication methods

OVERVIEW

You can change the way GitHub Enterprise Server authenticates with your existing accounts at any time.

Accounts Authentication Enterprise Identity

Configuring authentication and provisioning for your enterprise using Azure AD

HOW-TO GUIDE

You can use a tenant in Azure Active Directory (Azure AD) as an identity provider (IdP) to centrally manage authentication and user provisioning for your GitHub Enterprise Server instance.

Accounts Authentication Enterprise Identity SSO

Configuring SAML single sign-on for your enterprise

HOW-TO GUIDE

You can control and secure access to your GitHub Enterprise Server instance by configuring SAML single sign-on (SSO) through your identity provider (IdP).

Accounts Authentication Enterprise Identity SSO

Configuring user provisioning with SCIM for your enterprise

HOW-TO GUIDE

You can configure System for Cross-domain Identity Management (SCIM) for your GitHub Enterprise Server instance, which automatically provisions user accounts when you assign the application for your instance to a user on your identity provider (IdP).

Accounts Authentication Enterprise Identity SSO

About SAML for enterprise IAM

OVERVIEW

You can use SAML single sign-on (SSO) to centrally manage access to your GitHub Enterprise Server instance.

Accounts Access management Authentication Enterprise Identity

---

Configuring SAML single sign-on for your enterprise

HOW-TO GUIDE

You can control and secure access to your GitHub Enterprise Server instance by configuring SAML single sign-on (SSO) through your identity provider (IdP).

Accounts Authentication Enterprise Identity SSO

Using CAS

HOW-TO GUIDE

If you use Central Authentication Service (CAS) to centralize access to multiple web applications, you can integrate GitHub Enterprise Server by configuring CAS authentication for your instance.

Accounts Authentication Enterprise Identity SSO

Using LDAP

HOW-TO GUIDE

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.

Accounts Authentication Enterprise Identity

Using SAML for enterprise IAM

You can centrally manage accounts and access to your GitHub Enterprise Server instance with SAML single sign-on (SSO).

Accessing the administrative shell (SSH)

HOW-TO GUIDE

SSH access allows you to run the GitHub Enterprise Server command line utilities to troubleshoot, run backups, and configure replication.

Enterprise Fundamentals SSH

Administering your instance from the web UI

HOW-TO GUIDE

To perform administrative tasks for your GitHub Enterprise Server instance, you can use the Management Console and site admin dashboard.

Enterprise

Configuring the hostname for your instance

HOW-TO GUIDE

You can provide reliable access to your GitHub Enterprise Server instance by assigning a hostname that's accessible over your network.

Enterprise Fundamentals Infrastructure

Changing the hostname for your instance

HOW-TO GUIDE

If you want to change the hostname for an existing GitHub Enterprise Server instance, you must restore the settings and data to a new instance.

Enterprise Fundamentals Infrastructure

Configuring backups on your instance

HOW-TO GUIDE

As part of a disaster recovery plan, you can protect production data on your GitHub Enterprise Server instance by configuring automated backups.

Backups Enterprise Fundamentals Infrastructure

Configuring built-in firewall rules

HOW-TO GUIDE

You can view default firewall rules and customize rules for your GitHub Enterprise Server instance.

Enterprise Fundamentals Infrastructure Networking

Configuring code scanning for your appliance

HOW-TO GUIDE

You can enable, configure and disable code scanning for your GitHub Enterprise Server instance. Code scanning allows users to scan code for vulnerabilities and errors.

Advanced Security | Code scanning | Enterprise | Security

Configuring dependency review for your appliance

HOW-TO GUIDE

To help users understand dependency changes when reviewing pull requests, you can enable, configure, and disable dependency review for your GitHub Enterprise Server instance.

Advanced Security | Enterprise | Dependency review | Security

---

Configuring DNS nameservers

HOW-TO GUIDE

GitHub Enterprise Server uses the dynamic host configuration protocol (DHCP) for DNS settings when DHCP leases provide nameservers. If nameservers are not provided by a dynamic host configuration protocol (DHCP) lease, or if you need to use specific DNS settings, you can specify the nameservers manually.

Enterprise | Fundamentals | Infrastructure | Networking

Configuring rate limits

HOW-TO GUIDE

You can set rate limits for GitHub Enterprise Server using the Management Console.

Enterprise | Infrastructure | Performance

Configuring secret scanning for your appliance

HOW-TO GUIDE

You can enable, configure, and disable secret scanning for your GitHub Enterprise Server instance. Secret scanning allows users to scan code for accidentally committed secrets.

Advanced Security | Enterprise | Secret scanning | Security

Configuring TLS

HOW-TO GUIDE

You can configure Transport Layer Security (TLS) on your GitHub Enterprise Server instance so that you can use a certificate that is signed by a trusted certificate authority.

Enterprise | Fundamentals | Infrastructure | Networking | Security

---

Verifying or approving a domain for your enterprise

HOW-TO GUIDE

You can verify your ownership of domains with GitHub to confirm the identity of organizations owned by your enterprise account. You can also approve domains where organization members can receive email notifications.

Enterprise | Notifications | Organizations | Policy

Managing GitHub Mobile for your enterprise

HOW-TO GUIDE

You can decide whether people can use GitHub Mobile to connect to your GitHub Enterprise Server instance.

Enterprise | Mobile

Configuring SSH connections to your instance

HOW-TO GUIDE

You can increase the security of your GitHub Enterprise Server instance by configuring the SSH algorithms that clients can use to

establish a connection.

Authentication Enterprise Infrastructure Networking Security SSH

Configuring host keys for your instance

HOW-TO GUIDE

You can increase the security of your GitHub Enterprise Server instance by configuring the algorithms that your instance uses to generate and advertise host keys for incoming SSH connections.

Authentication Enterprise Infrastructure Networking Security SSH

Enabling and scheduling maintenance mode

HOW-TO GUIDE

Some standard maintenance procedures, such as upgrading your GitHub Enterprise Server instance or restoring backups, require the instance to be taken offline for normal use.

Enterprise Fundamentals Maintenance Upgrades

Enabling automatic user license sync for your enterprise

HOW-TO GUIDE

You can manage license usage across your GitHub Enterprise environments by automatically syncing user licenses from your GitHub Enterprise Server instance to GitHub Enterprise Cloud.

Enterprise GitHub Connect Licensing

Enabling private mode

HOW-TO GUIDE

In private mode, GitHub Enterprise Server requires every user to sign in to access the installation.

Access management Authentication Enterprise Fundamentals Infrastructure Networking Privacy Security

---

Enabling subdomain isolation

HOW-TO GUIDE

You can set up subdomain isolation to securely separate user-supplied content from other portions of your GitHub Enterprise Server appliance.

Enterprise Fundamentals Infrastructure Networking Security

Enabling unified contributions for your enterprise

HOW-TO GUIDE

You can allow users to include anonymized contribution counts for their work on your GitHub Enterprise Server instance in their contribution graphs on GitHub.com.

Enterprise GitHub Connect

Enabling unified search for your enterprise

HOW-TO GUIDE

You can allow users to include repositories on GitHub.com in their search results when searching from your GitHub Enterprise Server instance.

Enterprise GitHub Connect GitHub search

Network ports

REFERENCE

Open network ports selectively based on the network services you need to expose for administrators, end users, and email support.

Enterprise Infrastructure Networking Security

Site admin dashboard

REFERENCE

You can use the site admin dashboard to manage users, organizations, and repositories on your GitHub Enterprise Server instance.

Enterprise Fundamentals

Troubleshooting TLS errors

HOW-TO GUIDE

If you run into TLS issues with your appliance, you can take actions to resolve them.

Enterprise Errors Infrastructure Networking Security Troubleshooting

---

Using GitHub Enterprise Server with a load balancer

HOW-TO GUIDE

Use a load balancer in front of a single GitHub Enterprise Server instance or a pair of instances in a High Availability configuration.

Enterprise High availability Infrastructure Networking

About high availability configuration

OVERVIEW

In a high availability configuration, a fully redundant secondary GitHub Enterprise Server appliance is kept in sync with the primary appliance through replication of all major datastores.

Enterprise High availability Infrastructure

Accessing the monitor dashboard

HOW-TO GUIDE

GitHub Enterprise Server includes a web-based monitoring dashboard that displays historical data about your GitHub Enterprise Server appliance, such as CPU and storage usage, application and authentication response times, and general system health.

Enterprise Fundamentals Infrastructure Monitoring Performance

---

Creating a high availability replica

HOW-TO GUIDE

In an active/passive configuration, the replica appliance is a redundant copy of the primary appliance. If the primary appliance fails, high availability mode allows the replica to act as the primary appliance, allowing minimal service disruption.

Enterprise High availability Infrastructure

Differences between clustering and high availability (HA)

REFERENCE

Learn about the differences between deployment topologies for the virtual machines (VMs) that comprise a GitHub Enterprise Server instance.

Clustering Enterprise High availability Infrastructure

Enabling automatic update checks

HOW-TO GUIDE

You can enable automatic update checks so that your GitHub Enterprise Server instance checks for and downloads the latest GitHub Enterprise Server release.

Enterprise Upgrades

Initiating a failover to your replica appliance

HOW-TO GUIDE

You can failover to a GitHub Enterprise Server replica appliance using the command line for maintenance and testing, or if the primary

appliance fails.

Enterprise | High availability | Infrastructure

Recommended alert thresholds

REFERENCE

You can configure an alert to notify you of system resource issues before they affect your GitHub Enterprise Server appliance's performance.

Enterprise | Infrastructure | Monitoring | Performance | Storage

---

Setting up external monitoring

HOW-TO GUIDE

You can monitor basic system resources on your GitHub Enterprise Server appliance using either the SNMP or collectd statistics collection protocols.

Enterprise | Infrastructure | Monitoring | Performance

Upgrade requirements

REFERENCE

Before upgrading GitHub Enterprise Server, review these recommendations and requirements to plan your upgrade strategy.

Enterprise | Upgrades

Upgrading GitHub Enterprise Server

HOW-TO GUIDE

Upgrade GitHub Enterprise Server to get the latest features and security updates.

Enterprise | Upgrades

About system logs

OVERVIEW

To help administrators understand activity and errors, GitHub Enterprise Server stores system logs.

Auditing | Enterprise | Logging | Security

About GitHub Support

You can contact GitHub Support for help troubleshooting issues you encounter while using GitHub.

Support

About using actions in your enterprise

OVERVIEW

GitHub Enterprise Server includes most GitHub-authored actions, and has options for enabling access to other actions from GitHub.com and GitHub Marketplace.

Actions | Enterprise

Backing up and restoring GitHub Enterprise Server with GitHub Actions enabled

HOW-TO GUIDE

To restore a backup of your GitHub Enterprise Server instance when GitHub Actions is enabled, you must configure GitHub Actions before restoring the backup with GitHub Enterprise Server Backup Utilities.

Actions | Backups | Enterprise | Infrastructure

Enabling automatic access to GitHub.com actions using GitHub Connect

HOW-TO GUIDE

To allow GitHub Actions in your enterprise to use actions from GitHub.com, you can connect your enterprise instance to GitHub Enterprise Cloud.

Actions Enterprise GitHub Connect

Enforcing policies for GitHub Actions in your enterprise

HOW-TO GUIDE

You can enforce policies for GitHub Actions within your enterprise's organizations, or allow policies to be set in each organization.

Actions Enterprise Policies

Getting started with GitHub Actions for GitHub Enterprise Server

HOW-TO GUIDE

Learn about enabling and configuring GitHub Actions on GitHub Enterprise Server for the first time.

Actions Enterprise

High availability for GitHub Actions

REFERENCE

There are some special considerations for administering GitHub Actions in a high availability configuration.

Actions Enterprise High availability Infrastructure Storage

Using a staging environment

HOW-TO GUIDE

Learn about using GitHub Actions with GitHub Enterprise Server staging instances.

Actions Enterprise Infrastructure Upgrades

About enterprise accounts

OVERVIEW

With GitHub Enterprise Server, you can use an enterprise account to give administrators a single point of visibility and management.

Accounts Enterprise Fundamentals

About upgrades to new releases

OVERVIEW

You can benefit from new features and bug fixes for GitHub Enterprise Server by upgrading your enterprise to a newly released version.

Enterprise Upgrades

Configuring package ecosystem support for your enterprise

HOW-TO GUIDE

You can configure GitHub Packages for your enterprise by globally enabling or disabling individual package ecosystems on your enterprise, including Container registry, Docker, and npm. Learn about other configuration requirements to support specific package ecosystems.

Enterprise Packages

Quickstart for configuring your MinIO storage bucket for GitHub Packages

QUICKSTART

Configure your custom MinIO storage bucket for use with GitHub Packages.

Packages Enterprise Storage

About pre-receive hooks

OVERVIEW

Pre-receive hooks are scripts that run on the GitHub Enterprise Server appliance that you can use to implement quality checks.

Enterprise | Policies | Pre-receive hooks

Creating a pre-receive hook environment

HOW-TO GUIDE

To execute pre-receive hooks, use either the default pre-receive environment, or create a custom environment.

Enterprise | Policies | Pre-receive hooks

Creating a pre-receive hook script

HOW-TO GUIDE

Use pre-receive hook scripts to create requirements for accepting or rejecting a push based on the contents.

Enterprise | Policies | Pre-receive hooks

Enforcing policies for code security and analysis for your enterprise

HOW-TO GUIDE

You can enforce policies to manage the use of code security and analysis features within your enterprise's organizations.

Advanced Security | Code scanning | Enterprise | Policies | Secret scanning | Security

---

Enforcing policies for GitHub Actions in your enterprise

HOW-TO GUIDE

You can enforce policies for GitHub Actions within your enterprise's organizations, or allow policies to be set in each organization.

Actions | Enterprise | Policies

Enforcing policies for security settings in your enterprise

HOW-TO GUIDE

You can enforce policies to manage security settings in your enterprise's organizations, or allow policies to be set in each organization.

Enterprise | Policies | Security

Enforcing policies for projects in your enterprise

HOW-TO GUIDE

You can enforce policies for projects and classic projects within your enterprise's organizations, or allow policies to be set in each organization.

Enterprise | Policies | Projects

Enforcing repository management policies in your enterprise

HOW-TO GUIDE

You can enforce policies for repository management within your enterprise's organizations, or allow policies to be set in each organization.

Enterprise | Policies | Repositories | Security

Enforcing team policies in your enterprise

HOW-TO GUIDE

You can enforce policies for teams in your enterprise's organizations, or allow policies to be set in each organization.

Enterprise | Policies | Teams

Restricting email notifications for your enterprise

HOW-TO GUIDE

You can prevent your enterprise's information from leaking into personal email accounts by restricting the domains where members can receive email notifications about activity in organizations owned by your enterprise.

Enterprise Notifications Organizations Policies

Managing pre-receive hooks on your instance

HOW-TO GUIDE

Configure how people will use pre-receive hooks on your GitHub Enterprise Server instance.

Enterprise Policies Pre-receive hooks

Auditing SSH keys

HOW-TO GUIDE

Site administrators can initiate an instance-wide audit of SSH keys.

Auditing Enterprise Security SSH

Auditing users across your enterprise

HOW-TO GUIDE

The audit log dashboard shows site administrators the actions performed by all users and organizations across your enterprise within the current month and previous six months. The audit log includes details such as who performed the action, what the action was, and when the action was performed.

Auditing Enterprise Organizations Security User account

Configuring Git Large File Storage for your enterprise

HOW-TO GUIDE

Git Large File Storage (Git LFS) is an open source extension to Git that allows you to work with large files the same way as other text files.

Git Enterprise LFS Storage

Configuring visibility for organization membership

HOW-TO GUIDE

You can set visibility for new organization members across your enterprise to public or private. You can also prevent members from changing their visibility from the default.

Enterprise Organizations User account

Continuous integration using Jenkins

REFERENCE

You can automatically trigger build jobs on a Jenkins server when pushes are made to a repository in your GitHub Enterprise Server instance.

CI Enterprise

Disabling Git SSH access on your enterprise

HOW-TO GUIDE

You can prevent people from using Git over SSH for certain or all repositories on your enterprise.

Enterprise Policies Security SSH

Managing dormant users

HOW-TO GUIDE

By default, a user account is considered to be dormant if it has not been active for 90 days. You can configure the length of time a user must be inactive to be considered dormant and choose to suspend dormant users to release user licenses.

Accounts Enterprise Licensing

About the audit log for your enterprise

OVERVIEW

To support debugging and internal and external compliance, GitHub Enterprise Server provides logs of audited system, user, organization, and repository events.

Auditing Enterprise Logging Security

Accessing the audit log for your enterprise

HOW-TO GUIDE

You can view aggregated actions from all of the organizations owned by an enterprise account in the enterprise's audit log.

Auditing Enterprise Logging

Searching the audit log for your enterprise

HOW-TO GUIDE

You can search an extensive list of audited actions in your enterprise.

Auditing Enterprise Logging

Configuring the audit log for your enterprise

HOW-TO GUIDE

You can configure settings for your enterprise's audit log.

Auditing Enterprise Logging

Streaming the audit log for your enterprise

TUTORIAL

You can stream audit and Git events data from GitHub to an external data management system.

Auditing Enterprise Logging Organizations

Using the audit log API for your enterprise

TUTORIAL

You can programmatically retrieve enterprise events with the REST API.

Auditing Enterprise Logging API

Audit log events for your enterprise

REFERENCE

Learn about audit log events recorded for your enterprise.

Auditing Enterprise Logging Security

Activity dashboard

The Activity dashboard gives you an overview of all the activity in your enterprise.

Enterprise

Viewing push logs

HOW-TO GUIDE

Site administrators can view a list of Git push operations for any repository on the enterprise.

Auditing Enterprise Git Logging

Log forwarding

HOW-TO GUIDE

GitHub Enterprise Server uses syslog-ng to forward system and application logs to the server you specify.

Auditing | Enterprise | Logging | Security

Managing global webhooks

HOW-TO GUIDE

You can configure global webhooks to notify external web servers when events occur within your enterprise.

Enterprise | Webhooks

Managing projects using Jira

HOW-TO GUIDE

You can integrate Jira with GitHub Enterprise Server for project management.

Enterprise | Project management

Inviting people to manage your enterprise

HOW-TO GUIDE

You can add and remove enterprise owners for your enterprise account.

Administrator | Enterprise | User account

Roles in an enterprise

Everyone in an enterprise is a member of the enterprise. To control access to your enterprise's settings and data, you can assign different roles to members of your enterprise.

Enterprise

Viewing people in your enterprise

To audit access to enterprise-owned resources or user license usage, enterprise owners can view every administrator and member of the enterprise.

Enterprise

Placing a legal hold on a user or organization

HOW-TO GUIDE

You can place a legal hold on a user or organization to ensure that repositories they own cannot be permanently removed from your enterprise.

Accounts | Auditing | Enterprise | Organizations | User account

---

Preventing users from creating organizations

HOW-TO GUIDE

You can prevent users from creating organizations in your enterprise.

Enterprise | Organizations | Policies

Rebuilding contributions data

HOW-TO GUIDE

You may need to rebuild contributions data to link existing commits to a user account.

Enterprise | Repositories | User account

Requiring two-factor authentication for an organization

Requiring two-factor authentication for an organization

HOW-TO GUIDE

You can require organization members and outside collaborators to enable two-factor authentication for their personal accounts in an organization, making it harder for malicious actors to access an organization's repositories and settings.

2FA Enterprise Organizations Policies Security

Suspending and unsuspending users

HOW-TO GUIDE

If a user leaves or moves to a different part of the company, you should remove or modify their ability to access your GitHub Enterprise Server instance.

Access management Enterprise Security User account

Restoring a deleted organization

HOW-TO GUIDE

You can partially restore an organization that was previously deleted on your GitHub Enterprise Server instance.

Administrator Enterprise Organizations

About the Management Console

OVERVIEW

From the Management Console, you can initialize, configure, and monitor your GitHub Enterprise Server instance.

Administrator Enterprise Fundamentals Networking Monitoring

Managing access to the Management Console

HOW-TO GUIDE

You can increase the security of your GitHub Enterprise Server instance by creating or deleting Management Console users. As the root site administrator, you can access the Management Console as well as configure Management Console authentication rate limits.

Enterprise Authentication SSH User account

Accessing the Management Console

HOW-TO GUIDE

You can access the Management Console as the root site administrator or a Management Console user.

Enterprise Authentication

Troubleshooting access to the Management Console

HOW-TO GUIDE

You can troubleshoot access problems for the Management Console.

Enterprise Authentication SSH Troubleshooting
