Network ports

Improve the security of your instance

6 of 9 in learning path

Next: Configuring built-in firewall rules

In this article

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

Administrative ports

Some administrative ports are required to configure your GitHub Enterprise Server instance and run certain features. Administrative ports are not required for basic application use by end users.

Port	Service	Description
8443	HTTPS	Secure web-based Management Console. Required for basic installation and configuration.
8080	HTTP	Plain-text web-based Management Console. Not required unless TLS is disabled manually.
122	SSH	Shell access for your GitHub Enterprise Server instance. Required to be open to incoming connections between all nodes in a high availability configuration. The default SSH port (22) is dedicated to Git and SSH application network traffic.
1194/UDP	VPN	Secure replication network

		tunnel in high availability configuration. Required to be open for communication between all nodes in the configuration.
123/UDP	NTP	Required for time protocol operation.
161/UDP	SNMP	Required for network monitoring protocol operation.

Application ports for end users

Application ports provide web application and Git access for end users.

Port	Service	Description
443	HTTPS	Access to the web application and Git over HTTPS.
80	HTTP	Access to the web application. All requests are redirected to the HTTPS port if TLS is configured.
22	SSH	Access to Git over SSH. Supports clone, fetch, and push operations to public and private repositories.
9418	Git	Git protocol port supports clone and fetch operations to public repositories with unencrypted network communication. If you have enabled private mode on your instance, then opening this port is only required if you also enabled anonymous Git read access. For more information, see "Enforcing repository management policies in your enterprise."

Warning: When terminating HTTPS connections on a load balancer, the requests from the load balancer to GitHub Enterprise Server also need to use HTTPS. Downgrading the connection to HTTP is not supported.

Email ports

Email ports must be accessible directly or via relay for inbound email support for end users.

Port	Service	Description
25	SMTP	Support for SMTP with encryption (STARTTLS).

GitHub Actions ports

GitHub Actions ports must be accessible for self-hosted runners to connect to your GitHub Enterprise Server instance. For more information, see "About self-hosted runners."

Port	Service	Description
443	HTTPS	Self-hosted runners connect to your GitHub Enterprise Server instance to receive job assignments and to download new versions of the runner application. Required if TLS is configured.
80	HTTP	Self-hosted runners connect to your GitHub Enterprise Server instance to receive job assignments and to download new versions of the runner application. Required if TLS is not configured.

If you enable automatic access to GitHub.com actions, GitHub Actions will always search for an action on your GitHub Enterprise Server instance first, via these ports, before checking GitHub.com. For more information, see "Enabling automatic access to GitHub.com actions using GitHub Connect."

GitHub Connect ports

If you enable GitHub Connect, the connection between GitHub Enterprise Server and GitHub.com uses HTTPS over ports 443 or 80, and TLS is required. For more information, see "About GitHub Connect."

Further reading

- "Configuring TLS"

Previous
Accessing the administrative shell (SSH)

Next
Configuring built-in firewall rules