Configuring host keys for your instance

In this article

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.

> **Who can use this feature**
> Site administrators can configure the host keys for a GitHub Enterprise Server instance.

About host keys for your instance

Servers that accept SSH connections advertise one or more cryptographic host keys to securely identify the server to SSH clients. To confirm the server's identity during the initialization of a connection, clients store and verify the host key. For more information, see SSH Host Key - What, Why, How on the SSH Academy website.

Each GitHub Enterprise Server instance accepts SSH connections over two ports. Site administrators can access the administrative shell via SSH, then run command-line utilities, troubleshoot, and perform maintenance. Users can connect via SSH to access and write Git data in the instance's repositories. Users do not have shell access to your instance. For more information, see the following articles.

- "Network ports"
- "Accessing the administrative shell (SSH)"
- "About SSH"

By default, your GitHub Enterprise Server instance generates and advertises host keys with OpenSSH-style host key rotation. To increase the security of SSH in your environment, you can enable additional algorithms for the generation of host keys.

> **Note**: If you enable additional host key algorithms, clients that do not use OpenSSH for SSH connections may experience warnings during connection, or fail to connect entirely. Some SSH implementations can ignore unsupported algorithms and fall back to a different algorithm. If the client does not support fallback, the connection will fail. For example, the SSH library for Go does not support fallback to a different algorithm.

Managing an Ed25519 host key

To improve security for clients that connect to your GitHub Enterprise Server instance, you can enable the generation and advertisement of an Ed25519 host key. Ed25519 is immune to some attacks that target older signature algorithms, without sacrificing speed. Older SSH clients may not support Ed25519. By default, GitHub Enterprise Server instances do not generate or advertise an Ed25519 host key. For more information, see the Ed25519 website.

1. SSH into your GitHub Enterprise Server instance. If your instance comprises multiple nodes, for example if high availability or geo-replication are configured, SSH into the primary node. If you use a cluster, you can SSH into any node. For more information about SSH access, see "Accessing the administrative shell (SSH)."

   ```
   ssh -p 122 admin@HOSTNAME
   ```

2. To enable generation and advertisement of the Ed25519 host key, enter the following command.

   ```
   ghe-config app.babeld.host-key-ed25519 true
   ```

3. Optionally, enter the following command to disable generation and advertisement of the Ed25519 host key.

   ```
   ghe-config app.babeld.host-key-ed25519 false
   ```

4. To apply the configuration, run the following command.

   > **Note**: During a configuration run, services on your GitHub Enterprise Server instance may restart, which can cause brief downtime for users.

   Shell

   ```
   ghe-config-apply
   ```

5. Wait for the configuration run to complete.

Legal