Configuring secret scanning for your appliance

Configure GitHub Advanced Security
5 of 6 in learning path

Next: Enforcing policies for code security and analysis for your enterprise

In this article

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.

Secret scanning is available for organization-owned repositories in GitHub Enterprise Server if your enterprise has a license for GitHub Advanced Security. For more information, see "About secret scanning" and "About GitHub Advanced Security."

About secret scanning

If someone checks a secret with a known pattern into a repository, secret scanning catches the secret as it's checked in, and helps you mitigate the impact of the leak. Repository administrators are notified about any commit that contains a secret, and they can quickly view all detected secrets in the **Security** tab for the repository. For more information, see "About secret scanning."

Checking whether your license includes GitHub Advanced Security

You can identify if your enterprise has a GitHub Advanced Security license by reviewing your enterprise settings. For more information, see "Enabling GitHub Advanced Security for your enterprise."

Prerequisites for secret scanning

- The SSSE3 (Supplemental Streaming SIMD Extensions 3) CPU flag needs to be enabled on the VM/KVM that runs your GitHub Enterprise Server instance. For more information about SSSE3, see Intel 64 and IA-32 Architectures Optimization

Reference Manual in the Intel documentation.

- A license for GitHub Advanced Security (see "About billing for GitHub Advanced Security")
- Secret scanning enabled in the management console (see "Enabling GitHub Advanced Security for your enterprise")

Checking support for the SSSE3 flag on your vCPUs

The SSSE3 set of instructions is required because secret scanning leverages hardware accelerated pattern matching to find potential credentials committed to your GitHub repositories. SSSE3 is enabled for most modern CPUs. You can check whether SSSE3 is enabled for the vCPUs available to your GitHub Enterprise Server instance.

1. Connect to the administrative shell for your GitHub Enterprise Server instance. For more information, see "Accessing the administrative shell (SSH)."
2. Enter the following command:

   ```
   grep -iE '^flags.*ssse3' /proc/cpuinfo >/dev/null | echo $?
   ```

   If this returns the value `0`, it means that the SSSE3 flag is available and enabled. You can now enable secret scanning for your GitHub Enterprise Server instance. For more information, see "Enabling secret scanning" below.

   If this doesn't return `0`, SSSE3 is not enabled on your VM/KVM. You need to refer to the documentation of the hardware/hypervisor on how to enable the flag, or make it available to guest VMs.

Enabling secret scanning

> **Warning**: Changing this setting will cause user-facing services on GitHub Enterprise Server to restart. You should time this change carefully, to minimize downtime for users.

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 **Security**.
5. Under "Security," select **Secret scanning**.
6. Under the "Settings" sidebar, click **Save settings**.

   > **Note:** Saving settings in the Management Console restarts system services, which could result in user-visible downtime.

7. Wait for the configuration run to complete.

Disabling secret scanning

Warning: Changing this setting will cause user-facing services on GitHub Enterprise Server to restart. You should time this change carefully, to minimize downtime for users.

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 **Security**.

5. Under "Security," deselect **Secret scanning**.

6. Under the "Settings" sidebar, click **Save settings**.

   Note: Saving settings in the Management Console restarts system services, which could result in user-visible downtime.

7. Wait for the configuration run to complete.

Previous
Configuring dependency review for your appliance

Next
Enforcing policies for code security and analysis for your enterprise

Legal