

This version of GitHub Enterprise was discontinued on 2023-03-15. No patch releases will be made, even for critical security issues. For better performance, improved security, and new features, [upgrade to the latest version of GitHub Enterprise](#). For help with the upgrade, [contact GitHub Enterprise support](#).

Enabling encrypted assertions

In this article

About encrypted assertions

Prerequisites

Enabling encrypted assertions

You can improve your GitHub Enterprise Server instance's security with SAML single sign-on (SSO) by encrypting the messages that your SAML identity provider (IdP) sends.

Who can use this feature

Site administrators can configure encrypted assertions for a GitHub Enterprise Server instance.

About encrypted assertions

If your IdP support encryption of assertions, you can configure encrypted assertions on GitHub Enterprise Server for increased security during the authentication process.


Prerequisites

To enable encrypted assertions for authentication to GitHub Enterprise Server, you must configure SAML authentication, and your IdP must support encrypted assertions.

Enabling encrypted assertions

To enable encrypted assertions, you must provide your GitHub Enterprise Server instance's public certificate to your IdP, and configure encryption settings that match your IdP.

Note: GitHub strongly recommends that you verify any new configuration for authentication in a staging environment. An incorrect configuration could result in downtime for your GitHub Enterprise Server instance. For more information, see "[Setting up a staging instance](#)."

- 1 Optionally, enable SAML debugging. SAML debugging records verbose entries in GitHub Enterprise Server's authentication log, and may help you troubleshoot failed authentication attempts. For more information, see "[Troubleshooting SAML authentication](#)."
- 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 "🔗 Site admin" sidebar, click **Management Console**.
- 5 In the "Settings" sidebar, click **Authentication**.
- 6 Select **Require encrypted assertions**.
- 7 To the right of "Encryption Certificate", to save a copy of your GitHub Enterprise Server instance's public certificate on your local machine, click **Download**.
- 8 Sign into your SAML IdP as an administrator.
- 9 In the application for your GitHub Enterprise Server instance, enable encrypted assertions.
 - Note the encryption method and key transport method.
 - Provide the public certificate you downloaded in step 7.
- 10 Return to the management console on your GitHub Enterprise Server instance.
- 11 To the right of "Encryption Method", select the encryption method for your IdP from step 9.
- 12 To the right of "Key Transport Method", select the key transport method for your IdP from step 9.
- 13 Click **Save settings**.
- 14 Wait for the configuration run to complete.

If you enabled SAML debugging to test authentication with encrypted assertions, disable SAML debugging when you're done testing. For more information, see "[Troubleshooting SAML authentication](#)."

Legal

© 2023 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)