Troubleshooting SAML authentication

In this article

If you use SAML single sign-on (SSO) and people are unable to authenticate to access your GitHub Enterprise Server instance, you can troubleshoot the problem.

About problems with SAML authentication

GitHub Enterprise Server logs error messages for failed SAML authentication in the systemd journal logs for the `github-unicorn` container. You can review responses in this log, and you can also configure more verbose logging.

For more information about SAML response requirements, see "SAML configuration reference."

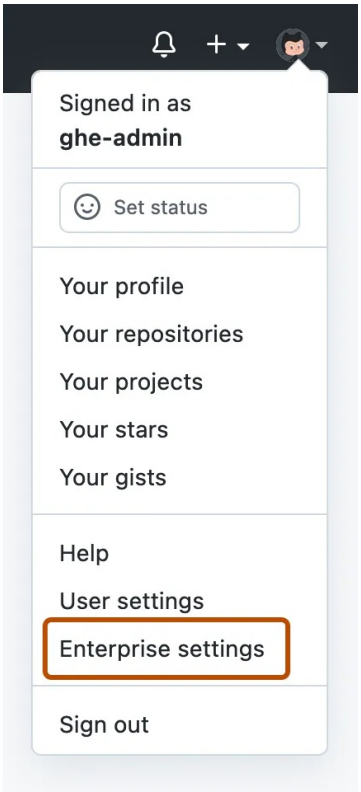
Configuring SAML debugging

You can configure GitHub Enterprise Server to write verbose debug logs for every SAML authentication attempt. You may be able to troubleshoot failed authentication attempts with this extra output.

Warnings:

- Only enable SAML debugging temporarily, and disable debugging immediately after you finish troubleshooting. If you leave debugging enabled, the size of the logs increases much faster than usual, which can negatively impact the performance of GitHub Enterprise Server.
- Test new authentication settings for your GitHub Enterprise Server instance in a staging environment before you apply the settings in your production environment. For more information, see "Setting up a staging instance."

1. In the top-right corner of GitHub Enterprise Server, click your profile photo, then click **Enterprise settings**.



2. In the enterprise account sidebar, click ⚖ **Policies**.
3. Under ⚖ **Policies**, click **Options**.
4. Under "SAML debugging", select the drop-down and click **Enabled**.
5. Attempt to sign into your GitHub Enterprise Server instance through your SAML IdP.
6. Review the debug output in the systemd journal for `github-unicorn` on your GitHub Enterprise Server instance. For more information, see "About system logs."
7. When you're done troubleshooting, select the drop-down and click **Disabled**.

Decoding responses

Some output in the systemd journal for `github-unicorn` may be Base64-encoded. You can access the administrative shell and use the `base64` utility on your GitHub Enterprise Server instance to decode these responses. For more information, see "Accessing the administrative shell (SSH)."

To decode the output, run the following command, replacing ENCODED_OUTPUT with the encoded output from the log.

```
base64 --decode ENCODED_OUTPUT
```

Error: "Another user already owns the account"

When a user signs into your GitHub Enterprise Server instance for the first time with SAML authentication, GitHub Enterprise Server creates a user account on the instance and maps the SAML `NameID` and `nameid-format` to the account.

When the user signs in again, GitHub Enterprise Server compares the account's `NameID` and `nameid-format` mapping to the IdP's response. If the `NameID` or `nameid-format` in

the IdP's response no longer matches the values that GitHub Enterprise Server expects for the user, the sign-in will fail. The user will see the following message.

> Another user already owns the account. Please have your administrator check the authentication log.

The message typically indicates that the person's username or email address has changed on the IdP. Ensure that the `NameID` and `nameid-format` mapping for the user account on GitHub Enterprise Server matches the user's `NameID` and `nameid-format` on your IdP. For more information, see "Updating a user's SAML NameID."

Error: Recipient in SAML response was blank or not valid

If the `Recipient` does not match the ACS URL for your GitHub Enterprise Server instance, one of the following two error messages will appear in the authentication log when a user attempts to authenticate.

```
Recipient in the SAML response must not be blank.
```

```
Recipient in the SAML response was not valid.
```

Ensure that you set the value for `Recipient` on your IdP to the full ACS URL for your GitHub Enterprise Server instance. For example, `https://ghe.corp.example.com/saml/consume`.

Error: "SAML Response is not signed or has been modified"

If your IdP does not sign the SAML response, or the signature does not match the contents, the following error message will appear in the authentication log.

```
SAML Response is not signed or has been modified.
```

Ensure that you configure signed assertions for the GitHub Enterprise Server application on your IdP.

Error: "Audience is invalid" or "No assertion found"

If the IdP's response has a missing or incorrect value for `Audience`, the following error message will appear in the authentication log.

```
Audience is invalid. Audience attribute does not match https://YOUR-INSTANCE-URL
```

Ensure that you set the value for `Audience` on your IdP to the `EntityId` for your GitHub Enterprise Server instance, which is the full URL to your instance. For example, `https://ghe.corp.example.com`.

Error: "Current time is earlier than NotBefore condition"

This error can occur when there's too large of a time difference between your IdP and

GitHub Enterprise Server, which commonly occurs with self-hosted IdPs.

To prevent this problem, we recommend pointing your appliance to the same Network Time Protocol (NTP) source as your IdP, if possible. If you encounter this error, make sure the time on your appliance is properly synced with your NTP server.

If you use ADFS as your IdP, also set `NotBeforeSkew` in ADFS to 1 minute for GitHub. If `NotBeforeSkew` is set to 0, even very small time differences, including milliseconds, can cause authentication problems.