SAML configuration reference

In this article

You can see SAML metadata for your organization or enterprise on GitHub Enterprise Cloud, and you can learn more about available SAML attributes and response requirements.

About SAML configuration

To use SAML single sign-on (SSO) for authentication to GitHub Enterprise Cloud, you must configure both your external SAML identity provider (IdP) and your enterprise or organization on GitHub.com. In a SAML configuration, GitHub Enterprise Cloud functions as a SAML service provider (SP).

You must enter unique values from your SAML IdP when configuring SAML SSO for GitHub Enterprise Cloud, and you must also enter unique values from GitHub Enterprise Cloud on your IdP. For more information about the configuration of SAML SSO for GitHub Enterprise Cloud, see "Configuring SAML single sign-on for your enterprise" or "Enabling and testing SAML single sign-on for your organization."

SAML metadata

The SP metadata for GitHub Enterprise Cloud is available for either organizations or enterprises with SAML SSO. GitHub Enterprise Cloud uses the `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST` binding.

Organizations

You can configure SAML SSO for an individual organization in your enterprise. You can also configure SAML SSO for an organization if you use an individual organization on GitHub Enterprise Cloud and do not use an enterprise account. For more information, see "Managing SAML single sign-on for your organization."

The SP metadata for an organization on GitHub.com is available at `https://github.com/orgs/ORGANIZATION/saml/metadata`, where **ORGANIZATION** is the name of your organization on GitHub.com.

Value	Other names	Description	Example
SP Entity ID	SP URL, audience restriction	The top-level URL for your organization on GitHub.com	`https://github.com/orgs/ORGANIZATION`

SP Assertion Consumer Service (ACS) URL	Reply, recipient, or destination URL	URL where IdP sends SAML responses	`https://github.com/orgs/ORGANIZATION/saml/consume`
SP Single Sign-On (SSO) URL		URL where IdP begins SSO	`https://github.com/orgs/ORGANIZATION/sso`

Enterprises

The SP metadata for an enterprise on GitHub.com is available at `https://github.com/enterprises/ENTERPRISE/saml/metadata`, where **ENTERPRISE** is the name of your enterprise on GitHub.com.

Value	Other names	Description	Example
SP Entity ID	SP URL, audience restriction	The top-level URL for your enterprise on GitHub.com	`https://github.com/enterprises/ENTERPRISE`
SP Assertion Consumer Service (ACS) URL	Reply, recipient, or destination URL	URL where IdP sends SAML responses	`https://github.com/enterprises/ENTERPRISE/saml/consume`
SP Single Sign-On (SSO) URL		URL where IdP begins SSO	`https://github.com/enterprises/ENTERPRISE/saml/sso`

SAML attributes

The following SAML attributes are available for GitHub Enterprise Cloud.

Name	Required	Description
`NameID`	✓	A persistent user identifier. Any persistent name identifier format may be used. If you use an enterprise with Enterprise Managed Users, GitHub Enterprise Cloud will normalize the `NameID` element to use as a username unless one of the alternative assertions is provided. For more information, see "Username considerations for external authentication." **Note:** It's important to use a human-readable, persistent identifier. Using a transient identifier format like `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` will result in re-linking of accounts on every sign-in, which can be detrimental to authorization management.

`SessionNotOnOrAfter`	×	The date that GitHub Enterprise Cloud invalidates the associated session. After invalidation, the person must authenticate once again to access your enterprise's resources. For more information, see "Session duration and timeout."
`full_name`	×	If you configure SAML SSO for an enterprise and you use Enterprise Managed Users, the full name of the user to display on the user's profile page.
`emails`	×	The email addresses for the user. If you sync license usage between GitHub Enterprise Server and GitHub Enterprise Cloud, GitHub Connect uses `emails` to identify unique users across products. For more information, see "Syncing license usage between GitHub Enterprise Server and GitHub Enterprise Cloud."
`public_keys`	×	If you configure SAML SSO for an enterprise and you use Enterprise Managed Users, the public SSH keys for the user. You can specify more than one key.
`gpg_keys`	×	If you configure SAML SSO for an enterprise and you use Enterprise Managed Users, the GPG keys for the user. You can specify more than one key.

To specify more than one value for an attribute, use multiple `<saml2:AttributeValue>` elements.

```
<saml2:Attribute FriendlyName="public_keys" Name="urn:oid:1.2.840.113549.1.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml2:AttributeValue>ssh-rsa LONG KEY</saml2:AttributeValue>
    <saml2:AttributeValue>ssh-rsa LONG KEY 2</saml2:AttributeValue>
</saml2:Attribute>
```

SAML response requirements

GitHub Enterprise Cloud requires that the response message from your IdP fulfill the following requirements.

- Your IdP must provide the `<Destination>` element on the root response document and match the ACS URL only when the root response document is signed. If your IdP signs the assertion, GitHub Enterprise Cloud will ignore the assertion.
- Your IdP must always provide the `<Audience>` element as part of the `<AudienceRestriction>` element. The value must match your `EntityId` for GitHub

Enterprise Cloud.

  - If you configure SAML for an organization, this value is `https://github.com/orgs/ORGANIZATION`.
  - If you configure SAML for an enterprise, this URL is `https://github.com/enterprises/ENTERPRISE`.

- Your IdP must protect each assertion in the response with a digital signature. You can accomplish this by signing each individual `<Assertion>` element or by signing the `<Response>` element.
- Your IdP must provide a `<NameID>` element as part of the `<Subject>` element. You may use any persistent name identifier format.
- Your IdP must include the `Recipient` attribute, which must be set to the ACS URL. The following example demonstrates the attribute.

```
<samlp:Response ...>
  <saml:Assertion ...>
    <saml:Subject>
      <saml:NameID ...>...</saml:NameID>
      <saml:SubjectConfirmation ...>
        <saml:SubjectConfirmationData
Recipient="https://github.com/enterprises/ENTERPRISE/saml/consume" .../>
      </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:AttributeStatement>
      <saml:Attribute FriendlyName="USERNAME-ATTRIBUTE" ...>
        <saml:AttributeValue>monalisa</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Assertion>
</samlp:Response>
```

Session duration and timeout

To prevent a person from authenticating with your IdP and staying authorized indefinitely, GitHub Enterprise Cloud periodically invalidates the session for each user account with access to your enterprise's resources. After invalidation, the person must authenticate with your IdP once again. By default, if your IdP does not assert a value for the `SessionNotOnOrAfter` attribute, GitHub Enterprise Cloud invalidates a session 24 hours after successful authentication with your IdP.

To customize the session duration, you may be able to define the value of the `SessionNotOnOrAfter` attribute on your IdP. If you define a value less than 24 hours, GitHub Enterprise Cloud may prompt people to authenticate every time GitHub Enterprise Cloud initiates a redirect.

To prevent authentication errors, we recommend a minimum session duration of 4 hours. For more information, see "Troubleshooting SAML authentication."

Notes:

- For Azure AD, the configurable lifetime policy for SAML tokens does not control session timeout for GitHub Enterprise Cloud.
- Okta does not currently send the `SessionNotOnOrAfter` attribute during SAML authentication with GitHub Enterprise Cloud. For more information, contact Okta.