SAML configuration reference

In this article

You can see SAML metadata for your GitHub Enterprise Server instance, 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 Server, you must configure both your external SAML identity provider (IdP) and your GitHub Enterprise Server instance. In a SAML configuration, GitHub Enterprise Server functions as a SAML service provider (SP).

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

SAML metadata

The SP metadata for your GitHub Enterprise Server instance is available at `http(s)://HOSTNAME/saml/metadata`, where **HOSTNAME** is the hostname for your instance. GitHub Enterprise Server uses the `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST` binding.

Value	Other names	Description	Example
SP Entity ID	SP URL, audience restriction	Your top-level URL for GitHub Enterprise Server	`http(s)://HOSTNAME`
SP Assertion Consumer Service (ACS) URL	Reply, recipient, or destination URL	URL where IdP sends SAML responses	`http(s)://HOSTNAME/saml/consume`
SP Single Sign-On (SSO) URL		URL where IdP begins SSO	`http(s)://HOSTNAME/sso`

SAML attributes

The following SAML attributes are available for GitHub Enterprise Server. You can change

the attribute names in the Management Console, with the exception of the `administrator` attribute. For more information, see "Administering your instance from the web UI."

Name	Required	Description
`NameID`	✓	A persistent user identifier. Any persistent name identifier format may be used. GitHub Enterprise Server 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 Server invalidates the associated session. After invalidation, the person must authenticate once again to access your GitHub Enterprise Server instance. For more information, see "Session duration and timeout."
`administrator`	×	When the value is `true`, GitHub Enterprise Server will automatically promote the user to be a site administrator. Setting this attribute to anything but `true` will result in demotion, as long as the value is not blank. Omitting this attribute or leaving the value blank will not change the role of the user.
`username`	×	The username for your GitHub Enterprise Server instance.
`full_name`	×	The full name of the user to display on the user's profile page.
`emails`	×	The email addresses for the user. You can specify more than one address. 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`	×	The public SSH keys for the user. You can specify more than one key.
`gpg_keys`	×	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 Server 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 Server 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 Server. This value is the URL where you access your GitHub Enterprise Server instance, such as `http(s)://HOSTNAME`.
- 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://HOSTNAME/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 Server periodically invalidates the session for each user account with access to your GitHub Enterprise Server instance. 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 Server invalidates a session two weeks 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 Server may prompt people to authenticate every time GitHub Enterprise Server initiates a redirect.

Notes:

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