Troubleshooting identity and access management for your organization

In this article

Review and resolve common troubleshooting errors for managing your organization's SAML SSO, team synchronization, or identity provider (IdP) connection.

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 Cloud, which commonly occurs with self-hosted IdPs.

If you encounter this error, make sure the time on your IdP 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.

Users are repeatedly redirected to authenticate

If users are repeatedly redirected to the SAML authentication prompt in a loop, you may need to increase the SAML session duration in your IdP settings.

The `SessionNotOnOrAfter` value sent in a SAML response determines when a user will be redirected back to the IdP to authenticate. If a SAML session duration is configured for 2 hours or less, GitHub.com will refresh a SAML session 5 minutes before it expires. If your session duration is configured as 5 minutes or less, users can get stuck in a SAML authentication loop.

To fix this problem, we recommend configuring a minimum SAML session duration of 4 hours. For more information, see "SAML configuration reference."

Some users are not provisioned or deprovisioned by SCIM

When you encounter provisioning issues with users, we recommend that you check if the users are missing SCIM metadata.

If SCIM provisioning is implemented for your organization, any changes to a user's organization membership should be triggered from the identity provider. If a user is invited to an organization manually instead of by an existing SCIM integration, their user account may not get properly linked to their SCIM identity. This can prevent the user account from being deprovisioned via SCIM in the future. If a user is removed manually instead of by an existing SCIM integration, a stale linked identity will remain, which can lead to issues if the user needs to re-join the organization.

If an organization member has missing SCIM metadata, then you can re-provision SCIM for the user manually through your IdP.

Auditing users for missing SCIM metadata

If you suspect or notice that any users are not provisioned or deprovisioned as expected, we recommend that you audit all users in your organization.

To check whether users have a SCIM identity (SCIM metadata) in their external identity, you can review SCIM metadata for one organization member at a time on GitHub or you can programatically check all organization members using the GitHub API.

When the IdP sends a provisioning call to the GitHub SCIM API, the SCIM `userName` in that API call needs to match the stored SAML `nameID` in the user's linked SAML identity in the organization. If these two values do not match, the SCIM metadata will not get populated, and the SCIM identity will not get successfully linked. To check whether these values match, use the GitHub API.

Auditing organization members on GitHub

As an organization owner, to confirm that SCIM metadata exists for a single organization member, visit this URL, replacing `<organization>` and `<username>`:

> `https://github.com/orgs/<organization>/people/<username>/sso`

If the user's external identity includes SCIM metadata, the organization owner should see a SCIM identity section on that page. If their external identity does not include any SCIM metadata, the SCIM Identity section will not exist.

Auditing organization members through the GitHub API

As an organization owner, you can also query the SCIM REST API or GraphQL to list all SCIM provisioned identities in an organization.

Using the REST API

The SCIM REST API will only return data for users that have SCIM metadata populated under their external identities. We recommend you compare a list of SCIM provisioned identities with a list of all your organization members.

For more information, see:

- "SCIM"
- "Organizations"

Using GraphQL

This GraphQL query shows you the SAML `NameId`, the SCIM `UserName` and the GitHub username (`login`) for each user in the organization. To use this query, replace `ORG` with your organization name.

```
{
  organization(login: "ORG") {
    samlIdentityProvider {
      ssoUrl
      externalIdentities(first: 100) {
        edges {
          node {
            samlIdentity {
              nameId
            }
            scimIdentity {
              username
            }
            user {
              login
            }
          }
        }
      }
    }
  }
}
```

```
curl -X POST -H "Authorization: Bearer YOUR_TOKEN" -H "Content-Type:
application/json" -d '{ "query": "{ organization(login: \"ORG\") {
samlIdentityProvider { externalIdentities(first: 100) { pageInfo { endCursor
startCursor hasNextPage } edges { cursor node { samlIdentity { nameId }
scimIdentity {username}  user { login } } } } } }" }'
https://api.github.com/graphql
```

For more information on using the GraphQL API, see:

- "Guides"
- "Explorer"

Re-provisioning SCIM for users through your identity provider

You can re-provision SCIM for users manually through your IdP. For example, to resolve provisioning errors for Okta, in the Okta admin portal, you can unassign and reassign users to the GitHub app. This should trigger Okta to make an API call to populate the SCIM metadata for these users on GitHub. For more information, see "Unassign users from applications" or "Assign users to applications" in the Okta documentation.

To confirm that a user's SCIM identity is created, we recommend testing this process with a single organization member whom you have confirmed doesn't have a SCIM external identity. After manually updating the users in your IdP, you can check if the user's SCIM identity was created using the SCIM API or on GitHub. For more information, see "Auditing users for missing SCIM metadata" or the REST API endpoint "SCIM."

If re-provisioning SCIM for users doesn't help, please contact GitHub Support.

Further reading

- "Troubleshooting identity and access management for your enterprise"