Google SAML

Note, other SAML providers may also work with EMS. Contact EMS support to discuss your options.

See also Delegated Authentication for single sign-on (SSO) integration.

Setup

To enable authentication with Google SAML, the following needs to be done:

- Go to your Google apps admin panel: https://admin.google.com/ac/apps/unified
- Add a new application by clicking `Add app` and choosing `Add custom SAML app`.
- Choose a name for the application (can be anything). Click next.
- Choose option 1 and download the metadata XML. Click next.
- Add some values, replacing the `homeserver` in `https://homeserver.ems.host` with whatever the hostname will be chosen in EMS. Note, this is the EMS hostname, not the custom server domain name.
  - ACS URL: `https://homeserver.ems.host/_synapse/client/saml2/authn_response`
  - Entity ID: `https://homeserver.ems.host/_synapse/client/saml2/metadata.xml`
  - Signed response: yes
  - Click next
- Click add new mapping 3 times, adding the following:
  1. Application attribute: `email`
     - Category: Basic Information
     - Field: Primary Email
  2. Application attribute: `firstName`
     - Category: Basic Information
     - Field: First Name
  3. Application attribute: `lastName`
     - Category: Basic Information
     - Field: Last Name
- Click `Finish` and then `OK`.
- In the settings for the app, turn on for everyone.

Update metadata

When the certificate expires (by default after 5 years) a new metadata file is required. The file can be downloaded from Google:

- Go to your Google apps admin panel: https://admin.google.com/ac/apps/unified
- Click on your app for Element.
- Click `Download metadata` in the sidebar.
- Click `Download metadata` in the modal.
- Store the metadata XML on your computer to upload it to EMS.

Upload metadata to EMS

The previously downloaded metadata XML is required by EMS to establish a secure connection to your GSuite environment.

- Go to your EMS hosts: https://ems.element.io/user/hosting
- Click on the tab `Integrations`.
- Select the host you wish to update.
- Under `Advanced Authentication` click on the `Google SAML` integration.
- Copy paste the contents of your downloaded metadata XML into the text field.
- Click `Purchase` or `Update` and wait for your host to apply the change.
- **Test your changes by logging into the EMS host.**

DRAFT Okta SAML

These instructions are a draft and might not be accurate

- Go to your Okta Applications panel: https://your-app-admin.okta.com/admin/apps/active
- Add a new application by clicking `Create App Integration` and choosing `SAML 2.0`.
- Choose a name for the application (it can be anything). Click next.
- Add some values, replacing the `homeserver` in `https://homeserver.ems.host` with whatever the hostname will be chosen in EMS. Note that this is the EMS hostname, not the custom server domain name.
  - Single sign on URL: `https://homeserver.ems.host/_synapse/client/saml2/authn_response`
  - Make sure `Use this for Recipient URL and Destination URL` is checked
  - Audience URI (SP Entity ID): `https://homeserver.ems.host/_synapse/client/saml2/metadata.xml`
  - Name ID format: Unspecified
  - Application username: (None)
  - Click Show Advanced Settings
  - Response: Signed
  - Attribute Statements. Name format: `Basic` for all
    - Name: `email` - Value: `user.email`
    - Name: `firstName` - Value: `user.firstName`
    - Name: `lastName` - Value: `user.lastName`
  - Click `Preview the SAML Assertion`. If you get the message `Please review the form to correct the following errors:` - correct errors shown
  - Click Next, then Finish
  - Click the `Assignments` tab for the application and assign it to everyone or a subset of your users
  - Click the `Sign On` tab
  - Click `View Setup Instructions`
  - Copy everything from the `Provide the following IDP metadata to your SP provider.` text box
- Continue from Upload metadata to EMS above

Revision #5
Created 18 April 2022 14:19:49 by Karl Abbott
Updated 4 May 2023 14:44:39 by Twilight Sparkle