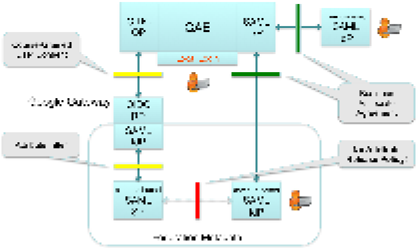
Using a Google Gateway as an Alternative IdP

Using a Google Gateway as an Alternative IdP

Internet2 and InCommon Operations jointly run a Google Gateway for select Internet2 services. For example, you can log into the Spaces wiki using your Google account. Choose “Social Providers” and then “Google Sign In” on the Spaces discovery interface. (You may have to delete cookies for spaces.at.internet2.edu to see the discovery interface.)

Google Apps for Education

If your campus is a *Google Apps for Education* (GAE) campus, you may have more Google accounts than you think. For example, as an Internet2 employee, I can log into the Spaces wiki using either the Internet2 IdP or the Google Gateway since Internet2 is a GAE campus, and moreover, using the Google Gateway, I can log in with my Internet2 credentials or my Google credentials.



Any GAE campus can use their campus credentials with the Google Gateway. When you choose “Google Sign In” on the Spaces discovery interface, one of three things will happen:

1. If you are currently logged into Google, and you’ve logged into Spaces with Google before, Spaces may already have permission to access your Google account, in which case you will immediately be given access to Spaces.
2. If you are currently logged into Google, but you’ve never logged into Spaces with Google before (or you haven’t given permission to Google to trust Spaces), the Google user consent page will appear. Press the “Accept” button to log into Spaces.
3. If you are not currently logged into Google, the Google Sign In page will appear. Type your campus email address into the “Email” text field but **do not enter a password on the Google Sign In page** (which is Google's way of doing IdP discovery). When you press the “Sign In” button, Google will redirect you to your campus IdP. Once you log into your IdP with your campus credentials, the Google user consent page will appear, depending on whether you’ve logged into Spaces with Google before.

You can revoke permission previously given to an app on the Google Permissions page.

A Real Use Case

Bradley University is a GAE campus. They use CAS to log into Google Apps. A Bradley user has an email address of the form:

```
user@fsmail.bradley.edu
```

When a Bradley user selects "Google Sign In" on the discovery interface and logs in via CAS, the Google Gateway asserts the following attributes:

```
eduPersonPrincipalName: user+fsmail.bradley.edu@google.incommon.org
mail: user@fsmail.bradley.edu
(and person name)
```

Now suppose Bradley University joins InCommon, partners with an Affiliate, and deploys its own Google Gateway. In this case, a Bradley user selects "Bradley University" on the discovery interface. After logging in via CAS, the Google Gateway asserts the following attributes:

```
eduPersonPrincipalName: user@bradley.edu
mail: user@fsmail.bradley.edu
(and person name)
```

Note that the ePPN is different. Since Bradley University now owns the Gateway, they can assert their own scoped attributes.

What about eduPersonTargetedID? Even though the Google IdP asserts an opaque, targeted, persistent identifier for the user, the Internet2 Google Gateway with DisplayName "Google Sign In" intentionally does not assert ePTID (since that is a commitment we’re not yet prepared to make). The Bradley University Google Gateway, OTOH, could assert ePTID straightaway, and its value would be exactly what you would expect.

In summary, a GAE campus can deploy a Google Gateway that asserts at least the following attributes out of the box:

- eduPersonPrincipalName
- eduPersonTargetedID
- mail
- displayName
- givenName
- sn (surname)

The campus can either let Google manage passwords or federate with Google Apps using CAS SAML or some other SAML software.

Google Apps for Business

Everything we’ve said so far about Google Apps for Education is true of any Google Apps account. For example, Cirrus Identity has a Google Apps for Business account, so Cirrus deployed a Google Gateway and registered an IdP in the InCommon Federation. Looking at the Cirrus IdP entity descriptor in metadata, you can’t tell that it’s backed by a Google Gateway; that is, Cirrus IdP metadata looks like any other IdP in metadata.