# Google Gateway

## Google Gateway

Internet2 and InCommon Operations jointly run a Google Gateway for select Internet2 services. The Gateway functions as a "catch-all IdP," sometimes called an IdP of Last Resort. If a user can not access an Internet2 SP, either because 1) their campus does not deploy an IdP, or 2) their campus IdP does not release the required attributes to that SP, that user can use the Google Gateway to log into the SP.

> ⚠ **For Internet2 services only!**
>
> The Google Gateway is **not** a centralized service for all InCommon participants. The Gateway is for select Internet2 services only.

*Note*: Not all Internet2 SPs use the Google Gateway. See below for a complete list.

**Contents**



See the Google Gateway FAQ for more information.

## Integrated Applications

Currently the Google Gateway is integrated with the following Internet2 services:

- InCommon Federation Manager
- Internet2 Collaboration Platform

Over time, other Internet2 services will be integrated with the Gateway.

### Federation Manager

> ⚠ View a static demo of a Google login to the FM

The InCommon Federation Manager uses the Google Gateway to authenticate a class of users called Delegated Administrators. The term Delegated Administration refers to the ability of a Site Administrator (who is a privileged user) to delegate responsibility for administering SP metadata to another administrator called a *Delegated Administrator*. A Delegated Administrator (DA) logs into the Federation Manager (FM) with a federated password, that is, the DA must have an account on an InCommon IdP. (InCommon Operations does not issue passwords to DAs.) If a site wishes to use the Delegated Administration feature of the FM, that site must deploy an IdP or use the Google Gateway.

In the eyes of a Delegated Administrator, the Google Gateway is just another IdP. Specifically, a DA sees an IdP called “Google Sign In” on the FM’s discovery interface. If the DA chooses to sign in with Google, the FM redirects the DA’s browser to the Google IdP via the Google Gateway.

## Privacy

The Google Gateway provides the following privacy-enhancing features:

1. Google requires explicit user consent to release attributes.
2. The Gateway filters any extra attributes released by Google.
3. The Gateway is stateless, that is, no user information is stored at the Gateway.
4. Since Google transacts with the Gateway only, the browsing habits of users are hidden from Google.

### User Consent

Google requires explicit user consent before releasing attributes to an application for the first time. If you approve the release of attributes to an application, your choice is recorded by Google. The next time you try to access that application, attributes will be automatically released.

You can view the applications you have consented to on your personal Google Accounts page:

https://accounts.google.com/IssuedAuthSubTokens

If you revoke consent previously given for a particular application, the next time you attempt to access that application, you will be asked to approve the release of attributes.

### Attribute Filter

The Gateway actively filters attributes released by Google. Only three attributes are allowed to transit the Gateway: email, first name, and last name. (One additional attribute, `eduPersonPrincipalName`, is manufactured by the Gateway itself.) Any other attributes asserted by Google are totally ignored.

### Stateless Gateway

Except for transaction data stored in log files and used for troubleshooting, no user information is stored at the Gateway. User attributes are asserted downstream and then forgotten. Consult the end application's privacy policy to understand how it handles user attributes.

### Safe Browsing

At the protocol level, Google transacts with a single host (google.incommon.org), so in that sense the interactions between the Gateway and SPs in the InCommon Federation are hidden from Google. Since each application integrated with the Gateway has its own API key and secret, Google knows when and how often requests are made but it doesn't know the terminal endpoint of that request. Only the Gateway knows that.

## Attribute Release

The current version of the Google Gateway asserts the following attributes:

- `eduPersonPrincipalName`
- `mail`
- `givenName`
- `sn` (surName)

The `mail`, `givenName`, and `sn` attributes are obtained from Google and always pass through the Gateway as-is.

> ⚠ **Extra attributes are ignored**
>
> At most the `mail`, `givenName`, and `sn` attributes will transit the Gateway. Any other attribute that Google chooses to assert is routinely dropped on the Gateway floor, that is, *any extra attributes are totally ignored* by the Gateway.

### Computing eduPersonPrincipalName

The value of the `eduPersonPrincipalName` (`ePPN`) attribute is computed as shown in the following example.

**Example**. Suppose the Google IdP asserts the following email address:

```
user@gmail.com
```

The Gateway is configured to compute the corresponding `ePPN` as follows:

```
user+gmail.com@google.incommon.org
```

In other words, the value of the `ePPN` attribute is completely dependent on the email address obtained from Google.

> ⚠ **Google email addresses**
>
> Google email addresses do not always end in “@gmail.com”. In fact, a Google email address can be virtually anything since Google Apps accounts are based on arbitrary DNS domains.

On the other hand, the Gateway asserts an `ePPN` with a fixed scope (“@google.incommon.org”). No configuration at the SP is necessary since by default the SP performs scoped attribute checking based on a fixed set of `<shibmd:Scope>` elements in Gateway metadata. In fact, there is one such `<shibmd:Scope>` element in Gateway metadata, namely:

```
<shibmd:Scope regexp="false">google.incommon.org</shibmd:Scope>
```

and so the `ePPN` shown above will be accepted by the SP by default. The acceptance of any other `ePPN` is left entirely to the discretion of the SP.

---