Delegated Administration

The InCommon Federation wiki has moved.

We have exciting news! An updated InCommon Federation wiki is now available. Please visit the new InCommon Federation Library for updated content.

Direct link to the new Federation Manager documentation.

This wiki is preserved for historical records only. It will no longer be updated.

We invite you to come check out the new Library. Don't forget to update your bookmarks accordingly.

search Visit the InCommon Federation Library wiki

Delegated Administration of Metadata

The term *delegated administration* refers to the ability of a site administrator to delegate responsibility for administering SP metadata to another administrator called a *delegated administrator*. The rationale for delegated administration was discussed in a blog post published early in 2012. The primary motivation for adding this feature to the Federation Manager (FM) is to simplify metadata management for those sites with large numbers of entities in metadata.

- Facts About Delegated Administration
  - Limitations
- For the Site Administrator
  - Preparing Your IdP
  - Provisioning a Delegated Administrator
  - Assigning Privileges to a Delegated Administrator
  - Approving Updates Made by a Delegated Administrator
- For the Delegated Administrator
  - Create New SP Metadata
  - Edit Existing SP Metadata
    - Unlinking a Certificate
- Security Considerations

Google Gateway in production!

As of 13 October 2013, the Google Gateway is a production service! Delegated administrators can now log into the Federation Manager with their Google accounts.

Facts About Delegated Administration

- A site administrator delegates the ability to administer SP metadata to a delegated administrator by providing the `eduPersonPrincipalName` and e-mail address of a prospective delegated administrator.
- A site administrator constrains the privileges of each delegated administrator, that is, the site administrator assigns delegated administrators to manage particular SPs.
- A delegated administrator is able to administer SP metadata only.
- A delegated administrator may create/modify/delete SP entity descriptors.
- A metadata update request submitted by a delegated administrator must be approved by a site administrator.
- The delegated administrative login interface accepts federated credentials only (i.e., InCommon Operations does not issue passwords to delegated administrators).
- The delegated administrator's IdP must support SAML V2.0 Web Browser SSO (i.e., SAML V1.1 is not supported).
- The delegated administrator's IdP must release a set of required attributes to the Federation Manager.

Limitations

- A site administrator for an organization may not function as a delegated administrator for the same organization.
- A delegated administrator for one organization may not function as a delegated administrator for another organization.
- Assigning two delegated administrators to the same entity descriptor can have undesirable side effects since the editing of entity descriptors is not constrained by the software in any way.

- A site administrator can not *unconditionally* delegate responsibility for administering SP metadata; that is, a site administrator must always approve update requests made by a delegated administrator.

For the Site Administrator

As a site administrator, you have the ability to provision one or more delegated administrators to manage SP metadata. You determine which entity descriptors may be edited by explicitly assigning a delegated administrator to one or more SPs. Any updates submitted by a delegated administrator are bounced back to you for approval, so the risk associated with the delegation of SP metadata is minimal.

Assigning SP Metadata to Existing Delegated Administrators

If you provisioned one or more delegated administrators prior to November 19, 2012 (when an upgrade to delegated administration occurred), please do the following:

1. Log into the Federation Manager and click the link “Delegated Administrators”
2. On the delegated administration page, click the link "Assign Metadata to Delegated Administrators"
3. Next to the entityID of some SP, select the desired delegated administrator from the drop-down menu and press the “Add” button
4. Repeat the previous step for every delegated administrator that needs to edit SP metadata

Each delegated administrator assigned as described above should now be able to edit SP metadata.

Preparing Your IdP

Since the delegated administrative login interface accepts federated credentials only, a site administrator must configure the IdP to release the following attributes to the Federation Manager (https://fm.incommon.org/sp):

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

Test Your IdP

You can test your IdP by logging into the following test SP: https://service1.internet2.edu/test/

Provisioning a Delegated Administrator

It's easy to provision a delegated administrator. To do so, a site administrator logs into the Federation Manager as usual and clicks the menu item "Delegated Administrators" along the left hand side of the page. After providing the `ePPN` and email address of a prospective delegated administrator, the system sends an email invitation to the given email address (copying all other site administrators as well). The prospective delegated administrator clicks the link in the email to continue with the boarding process.

Using the Google Gateway

If the delegated administrator will be using the Google Gateway, the `ePPN` asserted by the Gateway is based on the user's email address. Be sure to type in the correct `ePPN` when provisioning the delegated administrator. See the Google Gateway wiki page for more information.

Once the delegated administrator has successfully logged into the Federation Manager via SAML Web Browser SSO, a local account is provisioned. No local credentials are issued---the delegated administrator **always** logs in with a federated credential.

By provisioning a particular `ePPN`, a site administrator implicitly assumes the risk that the IdP **always** asserts that `ePPN` for the correct user. If you don't trust the IdP to do that, don't provision a delegated administrator with that `ePPN`.

Assigning Privileges to a Delegated Administrator

Login to the FM as a site admin

Login to the FM as a delegated admin

Delegated administrators are assigned to specific SPs. If you don't assign a delegated administrator to an SP, that delegated administrator will only be able to create new SP metadata. Typically, any given SP will have at most one delegated administrator assigned to it (although multiple delegated administrators may be assigned to a single SP if you choose).

> If multiple delegated administrators are assigned to a single SP, one delegated administrator may edit and submit metadata without being aware that another delegated administrator has already submitted an update request for the same entity descriptor. For this reason, it is recommended that *at most one delegated administrator be assigned to a particular SP*.

Approving Updates Made by a Delegated Administrator

Since all updates must be approved by a site administrator, the integrity of metadata is maintained.

> Since the site administrator approves all update requests, it is the site administrator who ultimately assumes the responsibility for all metadata submitted (which is the case in the absence of delegated administration as well).

For the Delegated Administrator

> Login to the FM as a delegated admin

As a delegated administrator, you will be able to create new SP metadata and edit existing SP metadata subject to policy. Your privileges have been assigned to you by a site administrator. If you are unable to perform some action, talk to your site administrator. Only a site administrator can assign privileges to a delegated administrator.

Create New SP Metadata

Click the link "Add a New Service Provider" to create *new* SP metadata. Visit the Metadata Administration wiki page for tips, recommendations, and requirements regarding the administration of SP metadata.

> Any new metadata you create must be approved by your site administrator.

Edit Existing SP Metadata

When you login as a delegated administrator, you will be presented with a list of all SPs owned by the organization. Those SPs you have been given permission to edit will have an "Edit" link next to their entity ID. Click the link to edit the metadata for that SP. If there is no "Edit" link next to the SP you want to edit, talk to your site administrator.

> Any metadata updates you submit must be approved by your site administrator.

Unlinking a Certificate

You may notice a link labeled "Unlink from the metadata" next to a certificate reference. This means the certificate was previously uploaded to the system by a site administrator and therefore can not be shown inline until you "Unlink" it. You should perform the following steps for each such certificate:

1. Scroll down to the bottom of the page and copy the content of the `<ds:X509Certificate>` element in metadata.
2. Paste the certificate content into an empty textarea.
3. Click the "Unlink from the metadata" link.
4. Submit an update request to your site administrator.

Once your site administrator approves the request, the certificate will appear inline where it is more easily reviewed and manipulated.

Security Considerations

For delegated administrators, the Federation Manager recognizes federated credentials only (no local credentials are issued to delegated admins). Currently there are no explicit assurance requirements associated with the federated credentials of delegated administrators. Since a trusted site administrator must approve any metadata update request submitted by a delegated administrator, the approval process mitigates any weakness in the delegated administrator's login credentials.