Federation Manager

InCommon Federation Manager

The *InCommon Federation Manager* (FM) is a web application for managing InCommon Federation metadata. The interface supports the management of both IdP and SP metadata. The following pages provide information on various aspects of the Federation Manager:

⚠ Login to the Federation Manager as a site admin

- Password Reset for site administrators
- Delegated Administration of specific SPs
- Bulk Update of metadata for Baseline Expectations
- Federation Manager Authentication Risk Assessment
- FM Change Log

To create metadata for a new IdP or SP, or to edit the metadata for an existing IdP or SP, a site administrator logs into the Federation Manager with credentials previously issued by InCommon Operations. A site administrator may also delegate administration of SP metadata to another individual.

Federation Manager Users

There are three types of Federation Manager users:

1. Registration Authority (RA) administrators
2. Site administrators
3. Delegated administrators

See Identity and Access Management for more information about Registration Authority administrators, Site administrators, as well as InCommon Executives.

Registration Authority (RA) Administrators

A Registration Authority administrator vets and approves submitted metadata. In some cases, a Registration Authority administrator may modify metadata directly without the intervention of the site administrator.

A Registration Authority administrator logs into the Federation Manager with two-factor authentication.

Site Administrators

Site administrators are provisioned by Registration Authority administrators. A site administrator may create, update, or delete any type of metadata, either IdP or SP metadata. A Registration Authority administrator must approve any metadata update request submitted or approved by a site administrator.

A site administrator may provision a delegated administrator (without the intervention of a Registration Authority administrator). A delegated administrator manages SP metadata on behalf the site administrator.

Today a site administrator logs into the Federation Manager with a strong password issued by InCommon Operations.

Delegated Administrators

Delegated administrators are provisioned by site administrators. A delegated administrator may create, update, or delete SP metadata only. A site administrator must approve any metadata update request submitted by a delegated administrator.

A delegated administrator logs into the Federation Manager with any federated credential (no assurance requirements) but every metadata update request made by a delegated administrator must be approved by a site administrator. The identity provider must provide certain identity attributes for the delegated administrator to gain access to the Federation Manager. These attributes positively identify the authenticated user to be the delegated administrator previously provisioned by the site administrator.

Every time a delegated administrator tries to access the Federation Manager, the attributes received from the identity provider are compared with the attributes stored in the identity management system. These attributes determine: 1) whether the authenticated user is allowed access, and if so, 2) what metadata the delegated administrator is allowed to update.