

# federation-manager-introduction

Jump to:

[Using Federation Manager to manage your metadata](#) | [Diving deeper](#)

Federation Manager is the web portal for administering the InCommon metadata. Participants and Federation Operations staff use this application to register, update, and publish metadata.

*Federation Manager is used by Site Administrators responsible for creating and maintaining SAML metadata on behalf of their organization.*

## How does Federation Manager work?

Each Participant organization designates up to 2 authorized individuals to manage metadata on its behalf. These individuals are called Site Administrators.

The metadata submitted by a site administrator is vetted and approved by the InCommon Registration Authority (RA). The RA checks submissions to make sure that the [entity ID](#) and endpoints ([IdP SSO Settings](#), [SP SSO Settings](#)) in metadata meet accuracy and information integrity requirements.

## Designate Site Administrators

Upon joining the InCommon Federation, a participant needs to designate one (preferably two) Site Administrator(s) to manage metadata. Beyond the obvious advantages of having a trained administrator for backup purposes, multiple Site Administrators has security advantages as well. Like password changes, metadata updates generate email notifications to **all** designated Site Administrators, which helps prevent both honest mistakes and malicious activity.

## Using Federation Manager to manage your metadata

- [Add a new Identity Provider](#)
- [Update an existing Identity Provider](#)
- [Un-publish an Identity Provider from the InCommon metadata](#)
- [Declare support for Research and Scholarship category](#)
- [Declare Sirtfi compliance](#)
- [Hide an identity provider from discovery](#)
  
- [Add a new Service Provider](#)
- [Update an existing Service Provider](#)
- [Un-publish \(deactivate\) an Service Provider from the InCommon metadata](#)

## Diving deeper

The following deployment strategy forces all protocol traffic over the front channel, which is easier to troubleshoot, manage, and maintain.



### Recommended Protocol Support for New IdPs

- **DO** support SAML2 Web Browser SSO on the front channel
- **DO NOT** support back-channel SAML protocols

## In this section

### Related content

- [Signing and Encryption Keys](#)
- [Signaling Encryption Method Support for a Service Provider](#)
- [Federation references](#)
- [Introduction to Federation Manager](#)
- [Working with SAML metadata](#)
- [Tagging an entity with Research and Scholarship entity attribute](#)

## Get help

Can't find what you are looking for?

[help Ask the community](#)