Security Incident Response Trust Framework for Federated Identity (SIRTFI) Category

What is SIRTFI?

The Security Incident Response Trust Framework for Federated Identity (SIRTFI) is an international standard to enable the coordination of incident response across federated organizations. The standard was developed by the international federation operators organization REFEDS and is documented at https://refeds.org/sirtfi.

SIRTFI provides a framework for effective incident response collaboration among federation and interfederation participants. One compromised account can create a security problem for a multitude of services across the interfederation community. When an organization complies with the SIRTFI framework, it agrees to participate in a federated incident response process. SIRTFI stipulates high-level practices and procedures, and identifies organizations that are capable of participating in a federated incident handling process. Federation participants that comply with SIRTFI are marked in the federation's metadata, raising the bar for operational security across federations.

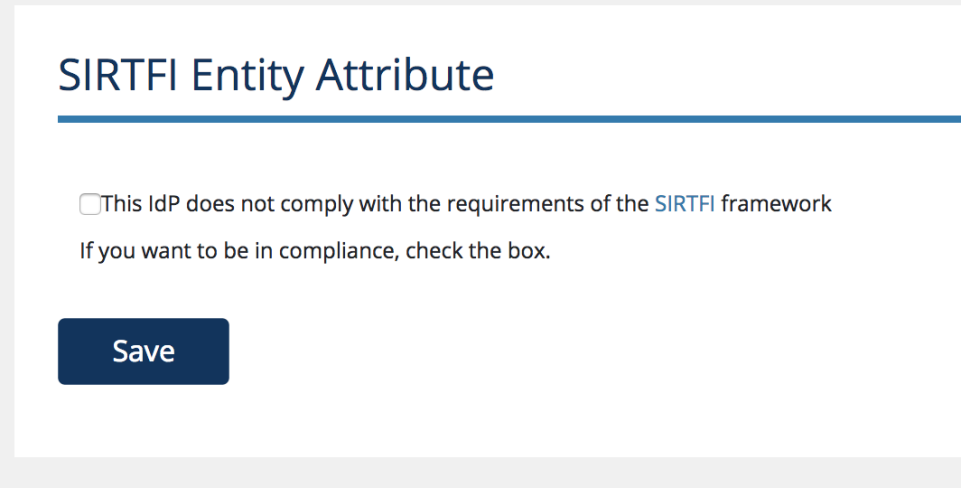
What does it mean to be compliant with SIRTFI?

REFEDS, an organization of federation operators and participants from around the world, has published the SIRTFI framework, which specifies a set of assertions that comprises SIRTFI compliance. The assertions are divided into four areas: operational security, incident response, traceability, and participant responsibilities. Details are available on the REFEDS website (PDF). An organization agrees to abide by these assertions, which is demonstrated by the relevant Identity Provider or Service Provider metadata carrying the SIRTFI assurance entity attribute, and updating its security contact with the new REFEDS security contact type.

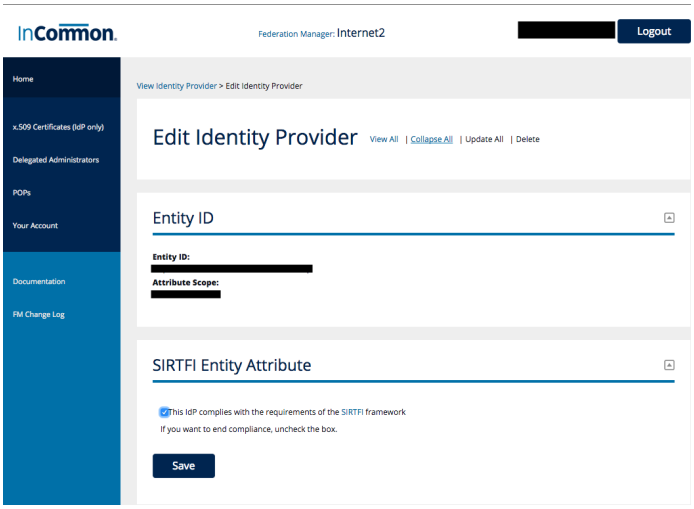
To self-assert compliance for an existing IdP or SP:

Log into the Federation Manager as a site admin.

1. From the site home page, scroll down to "Existing Identity Providers" or "Existing Service Providers".
2. Click "Update" for the IdP or SP you wish to assert SIRTFI for.
3. See the section titled "SIRTFI Entity Attribute"
4. There is a check box that is unchecked if your IdP or SP does not comply with SIRTFI, and looks like this:

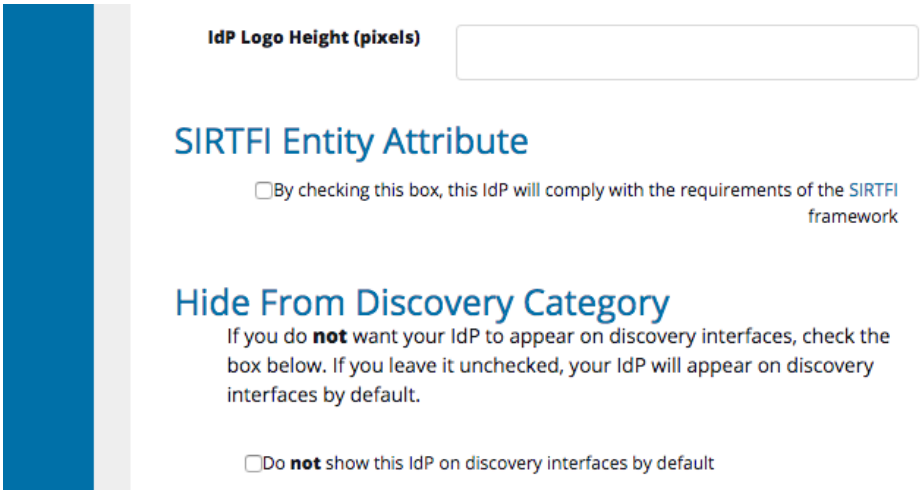


5. Check the box next to "This IdP does not comply with the requirements of the SIRTFI framework" (SP will be the same, except for the substitution of SP for IdP).
6. If you do not already have a "Security" contact type in the IdP or SP metadata, add one. You will not be able to add SIRTFI without adding a Security contact type. See also: more info about Contacts in Metadata
7. Click Save.
8. After you check the box and hit Save, the text will update to show that the IdP complies with the SIRTFI framework, as below. You must now submit metadata for your IdP or SP to complete the process.



To assert compliance for a new IdP or SP:

When creating a new IdP or SP, there is a new checkbox on the metadata entry page for self-assertion of SIRTFI compliance. Simply check the box when creating the new IdP or SP. If you do not already have a "Security" contact type in the IdP or SP metadata, add one. You will not be able to add SIRTFI without adding a Security contact type. See also: more info about Contacts in Metadata



More Information

See Incident Handling for more information about InCommon's federated incident response.

- Security Incident Response Trust Framework for Federated Identity (SIRTFI) Category