Getting Ready for eduGAIN

Deprecated

Note that this page has been deprecated. The information it contains is no longer current.

Is your SAML deployment ready for eduGAIN?

Depending on your answers to the following questions, your SAML deployment may (or may not) be ready for eduGAIN. Your prompt action may be required.

Roadmap for Operationalizing eduGAIN

Here is a brief outline of the roadmap for operationalizing eduGAIN:

Phase 0: [**DONE**] Introduce the MD-RPI schema into production metadata (for more info: Registered By InCommon Category)
Phase 1: [**DONE**] Deploy user interfaces in the Federation Manager (for more info: Federation Manager Release Notes)
Phase 2: [**DONE**] Import eduGAIN metadata into the preview aggregate
Phase 3: [**DONE**] Sync the main production aggregate with the preview aggregate and begin exporting metadata at scale to eduGAIN
Phase 4: [**DONE**] Sync the fallback aggregate with the main production aggregate

For more info: Roadmap for Operationalizing eduGAIN

Contents

Issues labeled with ★ below are MUST DO items by February 15, 2016.

IdP Software Issues

Are you running the Shibboleth IdP V2 software?

Shibboleth IdP V2 deployments earlier than V2.4.5 are susceptible to a logging issue that masks an error message when the JVM runs out of memory. For more info: Protect Against Failed Metadata Processes

> **Plan to upgrade to Shibboleth IdP V3**
>
> Shibboleth IdP V3 is not a prerequisite for eduGAIN, but if you have to make your IdP ready for eduGAIN anyway, you may as well focus on V3.
>
> 1. **Goal**: Deploy a test instance of Shibboleth IdP V3 by the end of 2015
> 2. Allocate at least 1500MB heap in the JVM
> 3. Point your test IdP at the InCommon Preview Aggregate
> 4. Know your SP partners
>
> For more info: Upgrading to Shibboleth IdP V3

Are you running the Shibboleth IdP V3 software?

Shibboleth IdP V3 deployments earlier than V3.2.0 are susceptible to a logging issue that masks an error message when the JVM runs out of memory. For more info: Protect Against Failed Metadata Processes

Are you running the simpleSAMLphp IdP software?

All simpleSAMLphp deployments earlier than 1.13.2 are susceptible to performance issues when processing large metadata files. For more info: Protect Against Failed Metadata Processes

Does your IdP software support SAML2 Web Browser SSO?

As a matter of policy, an IdP deployment that does **not** support SAML2 Web Browser SSO will **not** be exported to eduGAIN. For more info: Interfederation Technical Policy

SP Software Issues

Are you running the simpleSAMLphp SP software?

All simpleSAMLphp deployments earlier than 1.13.2 are susceptible to performance issues when processing large metadata files. For more info: Protect Against Failed Metadata Processes

Also, if you need to filter metadata (see below), install the metarefresh patch contributed to the simpleSAMLphp project by Cirrus Identity.

Does your SP software support SAML2 Web Browser SSO?

As a matter of policy, an SP deployment that does **not** support SAML2 Web Browser SSO will **not** be exported to eduGAIN. For more info: Interfederation Technical Policy

IdP Configuration Issues

Are you running the Shibboleth IdP software?

All Shibboleth IdP deployers are strongly advised to allocate at least 1500MB of heap space in the JVM to Protect Against Failed Metadata Processes.

> This simple procedure **must** be done by February 15, 2016. If not, your IdP's metadata refresh process will almost certainly fail.

Is your IdP discoverable?

A *discoverable IdP* will be configured such that both of the following are true:

1. The IdP consumes the metadata of *all SPs*
2. The IdP responds to all authentication requests

An IdP that is unable (or unwilling) to do so is advised to self-assert membership in the Hide From Discovery Category.

If your IdP is discoverable, it therefore responds to all authentication requests, and so the next question is: *What is your IdP's default attribute release policy?* That question remains a local policy issue since InCommon does not mandate attribute release policy. That said, an IdP easily satisfies the basic requirements of discoverability by releasing the following (trivial) attribute bundle to all SPs:

Name Identifier: SAML2 Transient NameID
User Attribute: `eduPersonScopedAffiliation`

This attribute bundle provides only minimal interoperability, however. For other more interoperable alternatives, see: Default Attribute Release

Is your IdP's attribute release policy configured correctly?

Review your IdP's overall attribute release policy in the presence of global metadata. If necessary, reconfigure your IdP's attribute release policy using the Registered By InCommon Category.

Opt out of metadata export only as a last resort

If, for some reason, the desired policy has not or can not be configured, log into the Federation Manager and opt out of exporting your IdP metadata to eduGAIN. Do this as a last resort only!

Does your IdP consume metadata from multiple sources?

If your IdP consumes metadata from multiple sources (which is common), the introduction of global metadata may cause a race condition that results in interoperability issues. For example, suppose a Shibboleth IdP is configured with a chaining `MetadataProvider` as follows:

A chaining MetadataProvider for Shibboleth IdP 3.0 (and later)

```
<MetadataProvider id="ShibbolethMetadata" xsi:type="ChainingMetadataProvider"
                  xmlns="urn:mace:shibboleth:2.0:metadata">

  <!-- Refresh some pre-InCommon metadata aggregate -->
  <MetadataProvider id="preICMD" xsi:type="FileBackedHTTPMetadataProvider"
                    xmlns="urn:mace:shibboleth:2.0:metadata" ...>

      <!-- ... -->
  </MetadataProvider>

  <!-- Refresh the InCommon metadata aggregate -->
  <MetadataProvider id="ICMD" xsi:type="FileBackedHTTPMetadataProvider"
                    xmlns="urn:mace:shibboleth:2.0:metadata"
                    metadataURL="http://md.incommon.org/InCommon/InCommon-metadata.xml"
                    backingFile="%{idp.home}/metadata/InCommon-metadata.xml">

      <!-- ... -->
  </MetadataProvider>

  <!-- Refresh some post-InCommon metadata aggregate -->
  <MetadataProvider id="postICMD" xsi:type="FileBackedHTTPMetadataProvider"
                    xmlns="urn:mace:shibboleth:2.0:metadata" ...>

      <!-- ... -->
  </MetadataProvider>

</MetadataProvider>
```

Entity metadata normally refreshed post-InCommon may be pre-empted by global metadata imported into the InCommon metadata aggregate. Know your metadata sources!

Does your IdP rely on the Name XML attribute in InCommon metadata?

Do **not** rely on the `md:EntitiesDescriptor/@Name="urn:mace:incommon"` XML attribute in InCommon metadata. Once we transition to per-entity metadata, such a policy rule will have no effect.

Use of metadata group name is deprecated

Use of the `md:EntitiesDescriptor/@Name="urn:mace:incommon"` XML attribute in InCommon metadata is deprecated but the attribute will **not** be removed from InCommon metadata. It will remain as-is indefinitely. However, your IdP configuration should **not** rely on it in any way. Eventually you will be forced to ignore this legacy value in InCommon metadata.

Does your IdP rely on the incommon.org R&S entity attribute value in SP metadata?

Do **not** rely on the deprecated incommon.org R&S entity attribute value (http://id.incommon.org/category/research-and-scholarship) in SP metadata. This entity attribute value will be removed from SP metadata in the future. For more info: Migrating an IdP to Global Research and Scholarship

Does your IdP support the global Research & Scholarship Category?

To maximize interoperability with global SPs, **support the global Research & Scholarship Category**! If your IdP is not ready to support global R&S SPs, at least support R&S SPs registered by InCommon. For more info: Research and Scholarship for IdPs (old)

SP Configuration Issues

Does your SP refresh and verify InCommon metadata at least daily?

If your SP does **not** refresh and verify InCommon metadata at least daily, your SP may be lacking a proper signing certificate revocation mechanism and therefore blindly trusting signed SAML assertions. For more info: Metadata Consumption

> ⚠ To protect against a key compromise at the IdP, SP deployments are strongly advised to automatically refresh and verify metadata at least daily.

Deployers are advised to point their pre-productions SP deployments at the preview aggregate (which contains global metadata as of January 15, 2016).

Does your SP consume metadata from multiple sources?

If your SP consumes metadata from multiple sources, the introduction of global metadata may cause a race condition that results in interoperability issues. For more info, see the corresponding IdP configuration issue above.

Does your SP expose a dynamic discovery interface?

If your SP exposes a dynamic discovery interface, normally you will filter IdPs in the Hide From Discovery Category from your discovery interface. Also check to make sure your discovery interface scales to many 100s of IdPs.

If your SP exposes a dynamic discovery interface and you do **not** export your SP metadata, you should filter global metadata altogether, otherwise some users may have a failed login experience. If necessary, reconfigure your SP using the Registered By InCommon Category.

Does your SP accept SAML assertions from arbitrary IdPs?

If your SP accepts SAML assertions from arbitrary IdPs and you do **not** export your metadata, you should filter global metadata altogether, otherwise you may end up giving access to unauthorized users. If necessary, reconfigure your SP using the Registered By InCommon Category.

IdP Metadata Issues

Does your IdP support SAML V2.0 Web Browser SSO?

As a matter of policy, an IdP that does **not** support SAML V2.0 Web Browser SSO will **not** be exported. (An IdP advertises support for SAML V2.0 Web Browser SSO if its metadata contains a SAML2 `SingleSignOnService` endpoint that supports the HTTP-Redirect binding.) For more info: Interfederation Technical Policy

Is your IdP discoverable?

If your IdP is **not** discoverable, you should self-assert membership in the Hide From Discovery Category.

Do you have unneeded certificates in IdP metadata?

Remove any unneeded certificates from IdP metadata. Please do your part to keep global metadata file sizes to a minimum.

Is your contact information in IdP metadata current and up-to-date?

Publish technical and administrative Contacts in Metadata so that SP partners know how to contact you if necessary.

SP Metadata Issues

Does your SP support SAML V2.0 Web Browser SSO?

As a matter of policy, an SP that does **not** support SAML V2.0 Web Browser SSO will **not** be exported. (An SP advertises support for SAML V2.0 Web Browser SSO if its metadata contains at least one SAML2 `AssertionConsumerService` endpoint that supports the HTTP-POST binding.) For more info: Interfederation Technical Policy

Do you have unneeded certificates in SP metadata?

Remove any unneeded certificates from SP metadata. Please do your part to keep global metadata file sizes to a minimum.

Does your SP publish Requested Attribute elements in metadata?

A global SP is advised to publish Requested Attributes in metadata since some IdPs in other federations only release attributes in the presence of `<md:RequestedAttribute>` elements in SP metadata.

> **SAML1-format requested attributes are deprecated**
>
> InCommon no longer supports SAML1-format `<md:RequestedAttribute>` elements in SP metadata. Only SAML2-format `<md:RequestedAttribute>` elements are supported. Consequently, global SPs are advised to advertise support for SAML2 protocols only.

Is your contact information in SP metadata current and up-to-date?

Publish technical and administrative Contacts in Metadata so that IdP partners know how to contact you if necessary.

Other Issues

Is your service eligible for membership in the global Research & Scholarship Category?

Is your service operated for the purposes of supporting research and scholarship interaction, collaboration or management, at least in part? If so, then by all means **apply for membership in the Research & Scholarship Category**! For more info: Research and Scholarship for SPs

Does your organization have more than one IdP registered in metadata?

As a matter of policy, an organization that deploys multiple IdPs with competing DisplayNames must tag all but one of those IdPs with the `hide-from-discovery` entity attribute. For more info: Hide From Discovery Category

Does your organization publish entity metadata across multiple federations?

As it turns out, about 70 InCommon SPs are known to publish their metadata in other federations. We advise organizations with entity metadata published in multiple federations to begin the process of synchronizing disparate metadata sources so that the metadata are functionally equivalent across federations. Only then can you phase out redundant metadata instances without loss of service.