# Baseline Expectations Frequently Asked Questions

**This is archived content.**

The content on this page reflects the work of Baseline Expectations 1 in 2018/19. It is preserved for historical reference only.

For the latest on Baseline Expectations, please visit the Baseline Expectations wiki home page.

## Baseline Expectations FAQ

### General Questions

#### What is the background and purpose for developing the Baseline Expectations program?

The background, philosophy, and strategic direction of the program are in the document, "Baseline Expectations for Trust in Federation: Increasing Trust and Interoperability in InCommon."

#### What policy and legal changes were needed to implement the Baseline Expectations?

The InCommon Steering Committee reviewed the terms and conditions of the Federation Operating Policies and Practices ("FOPP") and the InCommon Participation Agreement (the "Participation Agreement") to determine what changes were necessary. The InCommon Steering Committee determined, through discussions with the Participant community, that in addition to referencing the Baseline Expectations in the documents, the Dispute Resolution process should also be changed, in order to more effectively resolve disputes among Participants and to better allow the Baseline Expectations to be enforced. The revised FOPP and Participation Agreement, which may be found on the InCommon website, include the full range of changes necessary to accommodate the Baseline Expectations. You can see the notice sent to Executive Contacts and Billing Contacts, which includes a list of changes, in this PDF.

#### Do Baseline Expectations affect the test IdP/SP(s) that I have registered in metadata?

Yes. If it is registered in the InCommon metadata, then Baseline Expectations apply.

#### What happens if I don't meet Baseline Expectations?

The community is not on a "gotcha" campaign to catch those not meeting the Baseline Expectations. That said, all organizations are expected to take action in a reasonable amount of time. There is a community dispute resolution process under development for use in cases when an organization does not meet the Baseline Expectations.

#### Do you have any examples of privacy policies?

We have had a lot of questions about privacy policies and whether there are examples. Most organizations have an existing privacy policy for how user data will be handled. We encourage you to point at an existing policy with the privacy URL, rather than create a new policy.

#### What's this "SIRTFI" thing? Is that a Baseline Expectation?

SIRTFI (Security Incident Response Trust Framework for Federated Identity) is an international framework that enables coordination of incident response across federated organizations. While adopting the SIRTFI framework is not a requirement of Baseline Expectations, it is a very good way of meeting the "generally accepted security practices" Baseline requirement. Also, including a security contact in metadata is a requirement. InCommon supports the SIRTFI framework and encourages all participants to adopt the framework and self-assert that fact via the Federation Manager.

### How does InCommon, as a Federation Operator, meet its Baseline Expectations?

Baseline Expectations calls out the following expectations of the Federation Operator. How we are meeting the requirement is listed immediately below each item.

1. **Focus on trustworthiness of their Federation as a primary objective and be transparent about such efforts**
*InCommon Operations is working with CTAB to implement Baseline Expectations. The Federation has a strong community governance structure (Steering, CTAB, TAC).*
2. **Generally-accepted security practices are applied to the Federation's operational systems**
*Federation infrastructure systems are patched on a scheduled basis, and all systems are updated as rapidly as possible, in cases where known vulnerabilities affect an operational component. We have highly secure key management processes in place around the keys used in the metadata signing process.*
3. **Good practices are followed to ensure accuracy and authenticity of metadata to enable secure and trustworthy federated transactions**
*Separation of duties is enforced between those submitting and those approving metadata changes. Security is a focus of software development within both the Federation Manager and the backend processes which handle metadata signing. Audit logs and chain of custody of the metadata are kept in accordance with Internet2 data retention procedures. InCommon maintains a Incident Handling process which helps enable secure and trustworthy federated transactions.*
4. **Frameworks that improve trustworthy use of Federation, such as entity categories, are implemented and adoption by Members is promoted**
*InCommon supports the REFEDS SIRTFI and Research and Scholarship entity categories. As others emerge and prove useful for scalable promotion of trustworthy use of the Federation, they will be considered for support based on the community need, their merits and the resources they require to implement and operate.*
5. **Work with relevant Federation Operators to promote realization of Baseline Expectations**
*InCommon participates in REFEDS and eduGAIN governance activities which promote the goals of Baseline Expectations.*

### My Executive and/or Site Administrators are no longer with the organization. How do I change them?

You can initiate the process to change your organization's Executive by completing this form. Your InCommon Executive can change your site admins using this form. As when your organization first joined InCommon, this will involve some phone calls to register your new representatives' identities. You will find more information about these roles on the InCommon website.

## Metadata Questions

### I have heard there are required metadata elements as part of Baseline Expectations, as well as recommended elements. Please clarify.

Required elements include three types of contacts (technical, admin, and security), MDUI (Metadata User Interface) information, and a URL pointing to a privacy policy. These are listed in the Baseline Expectations foundational document. In addition, we recommend including an error URL to provide a landing page for users to determine where to get help. InCommon has published a high-level document, "Baseline Expectations for InCommon Execs," that provides a description and purpose of each required and recommended element.

### Do the Baseline Expectations include requirements for endpoints in metadata?

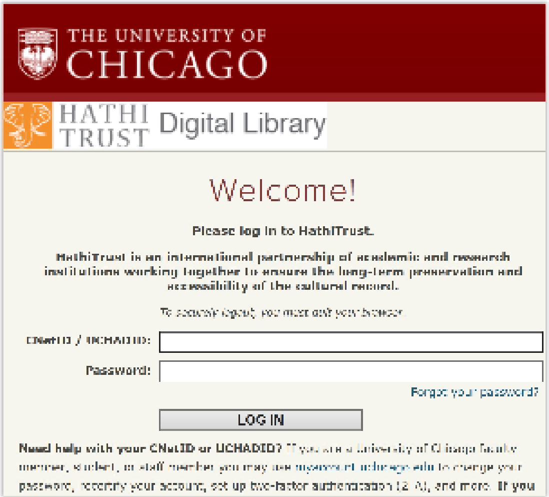
There are no specific requirements for endpoints as part of the Baseline Expectations. However, InCommon Operations has requirements and recommendations for endpoints documented in the wiki, https://spaces.at.internet2.edu/x/IImKAQ

### Do you have examples of XML syntax for placing the required elements in metadata?

You should not need to understand XML syntax for this purpose. An InCommon site administrator can edit and update metadata using the Federation Manager web interface. Information about each element in metadata, including those that are part of Baseline Expectations, is also available on the wiki.

### I'm getting questions about including a logo. What is the logo used for?

The logo significantly improves the user experience. When accessing a federated service, typically the user is presented with an Identity Provider discovery page. Having logos associated with each organization name makes for much faster scanning, so the user can pick out the appropriate organization quickly and continue with the sign-in process.  This shows how a service provider's DisplayName, Description, and Logo appear on an IdP login screen:



THE UNIVERSITY OF CHICAGO

HATHI TRUST Digital Library

Welcome!

Please log in to HathiTrust.

HathiTrust is an international partnership of academic and research institutions working together to ensure the long-term preservation and accessibility of the cultural record.

To securely logout, you must exit your browser.

CNetID / UCHADID:

Password:

Forgot your password?

LOG IN

**Need help with your CNetID or UCHADID?** If you are a University of Chicago faculty member, student, or staff member you may use myaccount.uchicago.edu to change your password, recover your account, set up two-factor authentication (2FA), and more. If you

Also, having a logo present in Service Provider metadata allows user consent information screens at Identity Providers to show the user a logo for the service to which they are asked to release information.

You can see more-detailed guidance and other screenshots demonstrating the use of logos, on this blog.

## SP metadata for a service that I have purchased is maintained by the organization that runs the SP. What is my responsibility?

It is the responsibility of the organization submitting SP metadata to maintain that metadata according to Baseline Expectations. If you have concerns about a service you run that is not complying with Baseline Expectations, please ask that organization to correct its SP metadata according to the documentation on the wiki.  If you run an SP that is hosted at your organization, and you (or a delegated administrator at your organization) submit the metadata for that SP, you are responsible for maintaining that metadata according to Baseline Expectations. Please consider the use cases noted in the previous FAQ answer when choosing elements such as logos. You want to choose a logo that tells the user something about the service they are accessing.

## I have heard the term "Metadata Health Check." What is that?

InCommon Operations has developed a process for alerting site admins and execs about the status of their metadata as it relates to the Baseline Expectations. InCommon Ops checks your metadata for the required elements and generates a report with the status of each element – a health check. InCommon will send email periodically with the results of the health check for your metadata.

## By when must I correct the issues identified in the Metadata Health Check?

Short answer: Each missing item reported in the health check contributes to poor user experience, reduced interoperability, and lower trust in the InCommon Federation. So please correct them as soon as possible.

Long answer: Baseline Expectations is in effect for all InCommon Federation Participants. After the announced deadline of December 14, 2018, enforcement will begin; issues that remain unaddressed will ultimately lead to the corresponding entities being reviewed by the CTAB, with eventual removal from federation metadata, until the IdP or SP entity issues are corrected. See the Community Dispute Resolution Process for more.

## My SAML software can't consume InCommon metadata, but its metadata is published in InCommon, does it need to meet baseline expectations?

Yes, all metadata registered by InCommon must meet Baseline Expectations. You can meet baseline expectations in InCommon metadata without having to modify the metadata of your SAML software. InCommon Site Administrators may update their organization's metadata via the InCommon Federation Manager.

## My Identity Provider is marked "Hide From Discovery," does that metadata need to meet baseline expectations?

Yes, all metadata registered by InCommon must meet Baseline Expectations. Hide from discovery does not opt your IdP out of the federation, it simply adds an entity attribute to metadata that must still meet baseline expectations. InCommon Site Administrators may update their organization's metadata via the InCommon Federation Manager.

## Is there documentation of the InCommon metadata elements, whether or not they are related to baseline expectations?

Yes, documentation is available in Metadata Administration.

### I am concerned that altering my metadata to meet baseline expectations will break downstream processes, how can I be certain that meeting baseline expectations will not break things?

Everything specified as required by baseline expectations in metadata is already in widespread use across not only InCommon, but over 50 other national research and education federations. The use of the required elements has over ten years of real-world use. Software which conforms with the OASIS Committee Specification, SAML V2.0 Metadata Interoperability Profile Version 1.0, August 2009 and the OASIS Committee Specification, Identity Provider Discovery Service Protocol and Profile, March 2008 will not break. All software deployed in InCommon and other federations by definition should already be able to meet these requirements.

**Is there a way for an organization to bulk update its metadata to meet Baseline Expectations?**

Yes, your InCommon Site Administrator(s) can use our new Baseline Expectations Bulk Update tool to update the following fields in all your entity descriptors which do not already contain the elements:

- mdui:LogoURL
- mdui:PrivacyStatementURL
- Administrative contact
- Security contact
- Technical contact

You cannot use this tool to update mdui:DisplayName, since that field should be different for each entity descriptor. This tool only allows adding missing elements, it does not allow you to change existing elements in metadata. For more information, visit the documentation for this feature.