Discovery Service FAQ

This is a list of frequently asked questions (FAQ) for the Discovery Service, one of numerous discovery services available to participants of the InCommon Federation.

General Questions

What is a "discovery service?"

Generally speaking, a *discovery service* is a solution to the identity provider discovery problem, a longstanding problem in the federated identity management space. As the term is used here, a discovery service provides a browser-based interface where a user selects his or her home organization (i.e., identity provider). A service provider uses this information to initiate SAML Web Browser SSO.

The phrase "Where Are You From?" (WAYF) is often used to characterize identity provider discovery. Historically, the term "WAYF" has referred to both software and protocol. The WAYF software has all but been eliminated by newer discovery service implementations (such as the InCommon Discovery Service), but the WAYF protocol lives on, mainly for backwards compatibility with SAML V1.1.

In addition to the legacy WAYF protocol, a true discovery service implements the *SAML V2.0 Identity Provider Discovery Protocol*. This protocol differs from the WAYF protocol in one very important respect. Whereas the WAYF protocol forwards an authentication request directly to the identity provider, the *Identity Provider Discovery Protocol* returns control to the service provider, which provides increased flexibility, privacy and security.

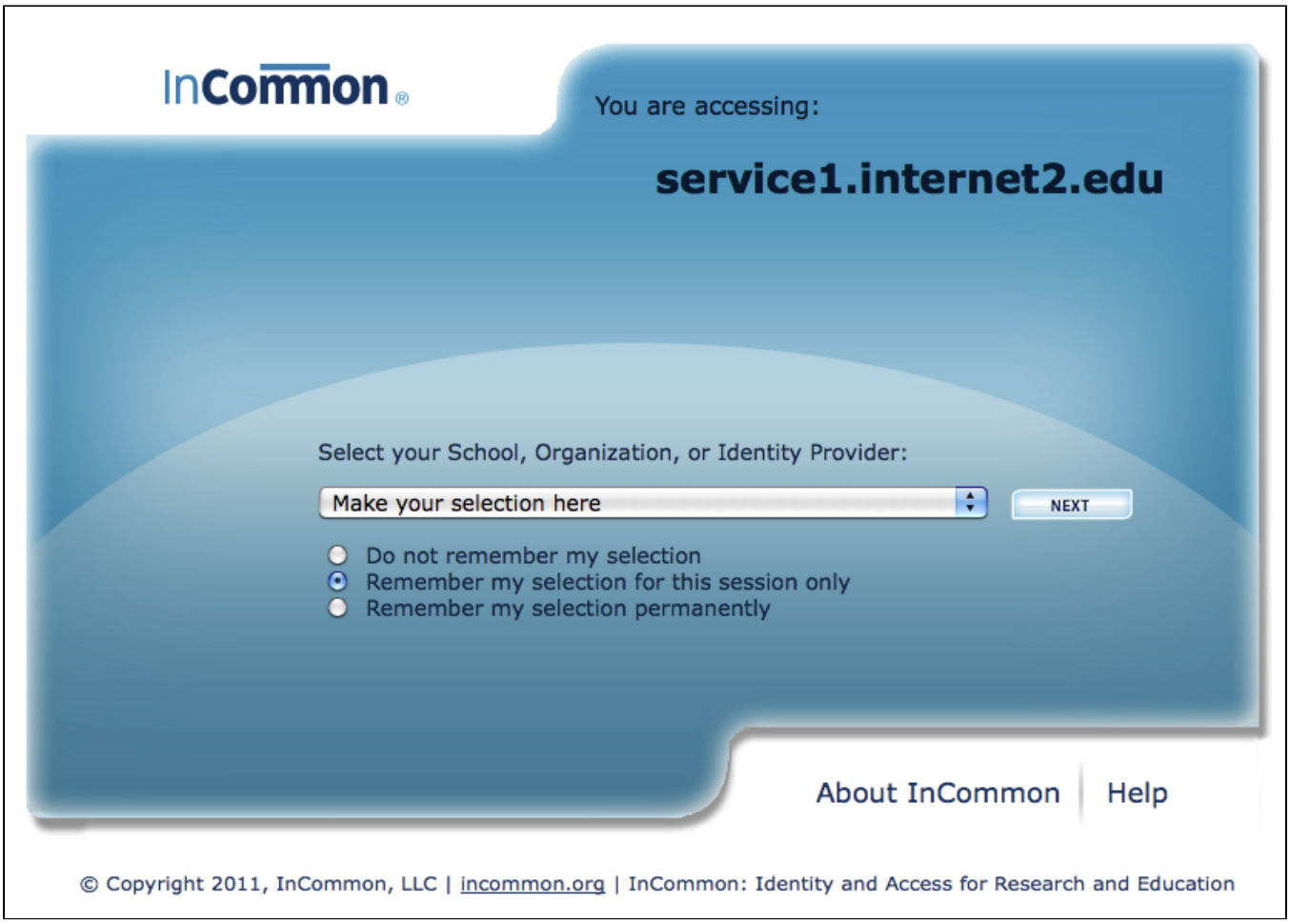
To learn how a discovery service works, the SWITCH federation has an excellent series of demos that describe and illustrate how a discovery service integrates into a typical SAML flow.

What is the InCommon Discovery Service?

The *InCommon Discovery Service* is a deployment of the *SWITCHwayf* software implementation, a software project of the SWITCH federation. The InCommon Discovery Service will replace the InCommon WAYF (Where Are You From?) with a Federation-wide discovery service that supports the *SAML V2.0 Identity Provider Discovery Protocol and Profile*. To ease the transition from the WAYF, the InCommon Discovery Service is backwards compatible with the InCommon WAYF.

What does the InCommon Discovery Service look like?

Here's a recent screen shot of the InCommon Discovery Service:



What if my organization is not listed in the pull-down menu of the InCommon Discovery Service?

If your organization is not listed in the pull-down menu, please check to see whether your organization is a current InCommon Participant. If not, encourage your organization to join the InCommon Federation.

My users are receiving the following error message: "Error: Invalid Query". What gives?

That means the SP does not have the required `<idpdisc:DiscoveryResponse>` elements in metadata. Please see the Discovery Service technical page for details.

Which SAML Service Provider implementations support the InCommon Discovery Service?

The InCommon Discovery Service works with **all** supported versions of the Shibboleth Service Provider software. To use the native *SAML V2.0 Identity Provider Discovery Protocol*, Shibboleth SP version 2.0 (or later) is required.

There may be other SP implementations that support the InCommon Discovery Service. If you find one that does, please share your experiences with other InCommon participants (incommon-participants@incommon.org).

Which discovery protocol should I use?

The InCommon Discovery Service supports two protocols:

1. The legacy WAYF protocol, which is based on the proprietary *Shibboleth 1.x AuthnRequest Protocol* defined in the Shibboleth Protocol Specification
2. The *SAML V2.0 Identity Provider Discovery Protocol*

SAML V2.0 is preferred over the legacy WAYF protocol. If your SP implementation supports SAML V1.1 only, however, then there is no choice---configure your SP to use the legacy WAYF protocol. Likewise if your SP implementation supports SAML V2.0 only, use the *SAML V2.0 Identity Provider Discovery Protocol*. If your SP implementation supports both SAML V1.1 and SAML V2.0, you have a choice, but clearly SAML V2.0 is preferred since it offers a much richer set of deployment options.

Should I use an "embedded discovery service" in lieu of the InCommon Discovery Service?

The InCommon Discovery Service is a *centralized discovery service* for general use within the InCommon Federation. For those service providers that implement their own discovery service through an embedded service, a companion application or service, or some other centralized service, the InCommon Discovery Service is unlikely to be applicable or appropriate. In that sense, the InCommon Discovery Service is a "service of last resort" for service providers that are unable to implement their own discovery solution.

How you handle discovery in conjunction with particular federated services is completely up to you. That said, it is well known that an *embedded* discovery service, or any kind of selection process more closely integrated with your federated application, provides the best overall experience for users, and gives you the most flexibility to offer a choice of identity providers to your users. You should by all means consider an embedded service as an alternative to centralized services such as the InCommon Discovery Service.

For More Information

- SWITCH demos http://www.switch.ch/aai/demo/
- SAML V2.0 Identity Provider Discovery Protocol and Profile http://wiki.oasis-open.org/security/IdpDiscoSvcProtonProfile
- Consult Shibboleth Discovery Config for more information about configuring a Shibboleth SP for discovery.