GettingStarted

This is a summary of the primary changes required to the initial configuration of the SP software (in *shibboleth2.xml*, unless otherwise noted). These changes apply generically to any of the platforms and web servers, and are supplemented by additional work specific to the web server you're using.

- Change the `entityID` attribute located in the `<ApplicationDefaults>` element to one that's appropriate for your service. An `https://` URL is recommended, ideally containing a logical DNS-derived name associated with your service that will not change over time as physical servers do. See the EntityNaming topic for more on this concept.

- Customize the various HTML error templates and error properties specified in the `<Errors>` element. Obviously the software will still run if you skip this, but frankly if you don't do it up front there's a decent chance you won't do it later, and that looks bad for you and your service as a whole. You will look like an idiot and people will treat you accordingly. At **least** provide a suitable email address in the `supportContact` property.

- For testing purposes, it's simplest to start with a single IdP and point the SP to it by modifying the `entityID` property in the `<SSO>` element. You will need to supply metadata for that IdP in the next step. Note that this has the same property name as the one mentioned above, but it's the opposite. This setting names the IdP to use, whereas the one in the first step names the SP you're setting up.

- Supply or link to at least one IdP's metadata using one or more `<MetadataProvider>` elements. There are a few common scenarios for acquiring metadata:
    - Join a federation. Usually you will be provided with a certificate to use to verify the metadata's signature to ensure its validity. Most of the time the federation will provide you with detailed instructions or examples of how to configure the software, and you should follow those instructions.
    - Work with a dedicated, "local" IdP. This is common in internal deployments. With a single IdP, you may also be given explicit instructions on how to get and verify the metadata you need, or you may simply be forced to download the metadata and could be on your own in verifying its validity. Understand that the entire basis for your SP's security will typically come from that file and how you get and maintain it.
    - If the metadata you need doesn't exist, then you will have to create it yourself. The information you'll need is typically at least its name (entityID), the location of its services, and its public key or certificate. An example file you can work from is also included with the SP.
- Complete the configuration process that's specific to your web server. These topics include both initial and advanced/reference material, but are short enough to read and understand up front.
    - Apache
    - IIS
    - FastCGI

Most installations will also want to:

- Adjust various session policy settings in the `<Sessions>` element.

- Review and adjust the extraction and mapping of attributes to environment variables or headers using the *attribute-map.xml* file. For more on this, see the Attribute Access topic.

Possible next steps:

- Learn more about Metadata and check out some of the conceptual material, if you haven't already.
- Generalize your discovery solution if you have to handle more than one IdP.