Shibboleth 2.0 IdP Deployment Guide

SWITCH
Serving Swiss Universities

Patrik Schnellmann
patrik.schnellmann@switch.ch

Shibboleth IdP 2.0 - What's new?

- Built-in SSO system in Shibboleth IdP
- Metadata updated by IdP webapp (no external cronjob needed)
- New entityId format (providerId): https://idp.example.org/idp/shibboleth
- Different (more) configuration files
- Attribute Push profile is the default
- Structured logging format

Shibboleth IdP 2.0 Deployment Guide

- Installation on Debian 4.0 (etch)
  - With Apache/Tomcat and built-in Single Sign-On
  - With Apache/Tomcat and CAS
  - Instructions to set up DB for persistent-id
  - ArpViewer requires CAS

- Easily adaptable to other Linux-based operating systems
  Sun JVM >= 1.5 (most common pitfall: gcj)
  Tomcat 5.5
  Apache 2.x

⇨ http://www.switch.ch/aai/howto/
http://spaces.internet2.edu/display/SHIB2/

Shibboleth IdP 2.0 Configuration

- attribute-resolver.xml (resolver.xml)
  Configures attribute collection, transformation, and encoding.
- attribute-filter.xml (arp.site.xml)
  Configures the release of attributes to SP's.
- handler.xml
  Configures how the IdP receives messages various message types.
- relying-party.xml (~ idp.xml)
  Configures how the IdP processes messages that are received.
- login.config
  Configuration for the Username/Password authentication mechanism.
- logging.xml, service.xml, internal.xml

Why update?

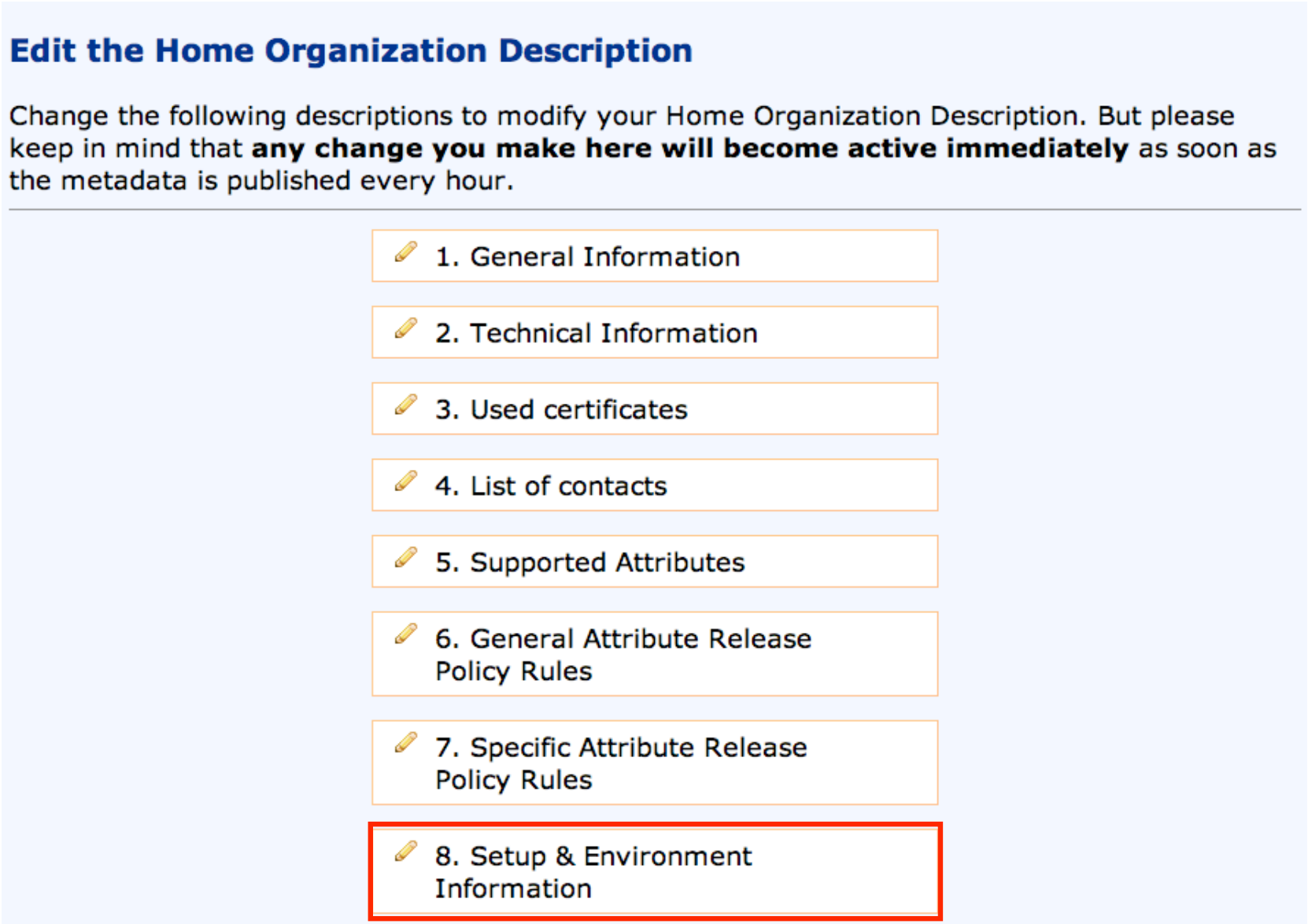
- Less problems with Service Provider interoperation
  (Attribute push is default, no AA connection needed.)

- Running a pre-1.3.3 Shibboleth IdP?
  - Have you missed a security update?
  - Support the ‘common-lib-terms’ entitlement attribute
    (see: http://www.switch.ch/aai/common-lib-terms)

- Be prepared for future functionalities:
  - AAA related projects most likely require a Shib 2.0 IdP
  - Smooth upgrade to Shib 2.1 IdP

- Interoperability with other SAML2 Service Providers

IdP information in the Resource Registry (I)



IdP information in the Resource Registry (II)

Setup & Environment Information		
Operating system	Debian Linux	
Webserver	Tomcat + Apache	
Authentication System	CAS 3	
IdP version	1.3.3	
Comments	with ArpViewer	

- Fill out the form for your IdP

SWITCH - Serving Swiss Universities switch.ch

Setup:
OS: Debian Linux | Webserver: Tomcat + Apache | SSO System: CAS 3 | IdP Version: 1.3.3
with ArpViewer

- Browse the list on: https://aai-rr.switch.ch/list_homeorgs.php