ReleaseNotes

Please review these release notes before upgrading your system. You should review all the versions subsequent to the one you're running prior to upgrade.

3.0.4 (March 11, 2019)

7 issues

A patch has been released to fix a number of minor issues and to address a security issue.

3.0.3 (December 19, 2018)

9 issues

A patch has been released to fix a few more minor issues and to address a security issue.

3.0.2 (August 2, 2018)

5 issues

A second patch has been released to fix a few more minor issues and a major bug in the new IIS module that prevented its use in some significant cases.

This patch also prevents some of the unintentional changes to the *attribute-map.xml* and *attribute-policy.xml* files during RPM upgrades in cases where the original files hadn't been modified. The files will still be replaced but the removed mappings are historical and deprecated and this is outlined down in the main 3.0.0 section and in the upgrade material.

Finally, the Windows installer includes an update to the xml-security-c library to 2.0.1.

3.0.1 (July 18, 2018)

A patch has been released to address a couple of serious regressions and a few minor nits. The xmltooling library was also updated to 3.0.1 as part of this release, and subsequently to 3.0.2 to correct a linking issue in the makefiles on non-Windows platforms.

7 issues

3.0.0 (July 17, 2018)

85 issues

This is the first release of the third-generation Service Provider software. The key documentation links are located on the SP3 space Home page, such as System Requirements, Installation, and Upgrading material.

This release interoperates with all previous releases of Shibboleth and other software that supports the same standards. While this is a major upgrade, that primarily reflects changes to the internals, which do not in general impact deployers. It is a fundamentally backward-compatible release that introduces new options but fully supports the V2 configuration format and makes relatively few changes to existing system behavior.

It is designed to be applied as an upgrade directly to existing systems, and while we strongly advise testing in a non-production environment, the majority of deployments should operate successfully following an upgrade with little or no effort.

Significant Behavioral Changes

Absent explicit configuration, the default digest algorithm used when creating signed messages has been updated from SHA-1 to SHA-256, reflecting industry guidance and matching the IdP V3 default. If compatibility with older systems is required, the default algorithm can be explicitly set via the `<ApplicationDefaults>` element, or specific rules for those IdPs may be specified via `<RelyingParty>` overrides. Note that in the majority of deployments, SPs rarely sign (and rarely need to sign) anything except for SAML logout messages.

The new software has an *attribute-map.xml* file that removes the older, incorrect form of the eduPersonTargetedID attribute from the file, and the strongly discouraged "unscoped" form of eduPersonAffiliation. In RPM installs, this file will overwrite the older default file if it hasn't been modified by the deployer, so this can result in changed behavior unless the file is restored. If you want to prevent this, a simple edit to that file (add a comment) will do the trick, and the old file is available under a different name in any case.

For macOS systems, Apple has deprecated their Apache software and the SP "port" is now built against the apache2 port, which affects port upgrades. The module built by the upgraded port may not function in the Apple Apache software and is not meant to be used with it.

Finally, be aware that RPMs are not going to be officially available for a handful of older/unsupported OS versions, including RHEL 5, SUSE 10, and some older SUSE 11 versions. CentOS 5, while unsupported, continues to have a package stream available, which should work for RHEL 5.

Changed Defaults

Excepting as noted above, most actual underlying system defaults have remained unchanged but there have been changes to the default configuration files included with new installations, and some defaults have been adjusted when the system detects that the configuration is not a legacy one.

Instead of generating a single key pair, new installs will have two key pairs generated, one for signing and one for encryption. Some SPs do not need a signing key, but all SPs should support encryption, so this isolates the more-used key from the lesser-used key, and improves the overall hygiene of the system by keeping keys used for different purposes separate. Upgrades of existing systems will leave the original key untouched and continue to operate with a single key for both.

The default configuration specifies a more restrictive and secure set of TLS ciphers to support when contacting other systems. This can be changed if interoperability is impacted.

SAML 1.1 support is not enabled by default; add back the string "SAML1" inside the <SSO> element to enable it.

Support for Attribute Queries is not enabled by default to eliminate a common source of confusion. This will impact behavior when interacting with out of date Shibboleth IdPs relying on SAML 1.1 without pushed attributes. Such systems should be migrated to SAML 2.0, but query support can be re-enabled if necessary by adding `<AttributeResolver type="Query" subjectMatch="true"/>` to the <ApplicationDefaults> element.

The default <TrustEngine> configuration (when nothing is specified, as in most cases) is now ExplicitKey-only and does not enable PKIX support.

New Windows installs default to use of a new IIS7+ native module instead of the older ISAPI module, which includes some functional differences that, while much safer, may impact application code.

Logs from the web server modules (the so called "native" log) now default to local syslog or the Windows Event Log, rather than a file. This eliminates a huge source of file handle leaks and permission problems that have plagued the software. The default logging level has also been adjusted to WARN.

The format of the transaction log has been updated to something more useful and parseable.

The attribute mapping rules and priority for populating REMOTE_USER have been refreshed to reflect modern (and post-modern utopian) practices.

In addition to these changes, some settings have different default settings based on whether the configuration file is an upgraded V2 file or a newly installed V3 file, based on the XML namespace of the file (further explained below).

- The `cacheAssertions` default in the StorageServiceSessionCache has changed from true to false when the V3 namespace is used.

Configuration Format and Compatibility

To maintain appropriate behavior during upgrades, the name of the default configuration file remains *shibboleth2.xml,* despite the possible confusion this may create. However, the XML namespace has been "forked" to create a new configuration format that allows the software to easily detect whether it should operate in a legacy or updated manner in a few cases.

The old namespace is/was `urn:mace:shibboleth:2.0:native:sp:config` and the schema supported in V2.6 has been included.

The new namespace, which is used by default, is `urn:mace:shibboleth:3.0:native:sp:config` and its schema includes both some new settings and omits a number of deprecated settings.

Thus, it is a relatively simple matter to "upgrade" one's configuration:

1. With the original configuration, verify a working system, and check the log(s) for any DEPRECATED warnings.
2. Fix any settings causing those warnings until they're gone.
3. Update the namespace at the top of the file.
4. Restart, test, and fix any straggling errors.

Most of the changed defaults noted above will not apply to such a migrated system since they depend on actual changes to the configuration, and the vast majority of deployments can simply do a bit of testing, make the bump, and be good to go.

Deprecated Settings

Some syntax has been deprecated in V3. As a rule of thumb, if something is documented in this SP3 wiki space, then it is not deprecated. Otherwise a warning will usually be found in the log when the original configuration is used, and an error may occur if the configuration namespace is bumped.

Time permitting, a summary of deprecated options will be provided here.

- Various plugins relying on external XML files or resources used to support a number of equivalent settings (e.g., `file`, `uri`) for specifying the local or remote resource, and these have been eliminated, with only `path` and `url` remaining. Sometimes the error messages can be obscure if you don't fix these up, but the warnings are clear when the V2 namespace is used, so always review those first.

Significant New Functionality

IIS7

A new IIS plugin is available for recent (IIS7+) versions of IIS. This is a significant improvement on the older module:

- It supports Server Variables rather than relying on HTTP Headers for the presentation of attributes, which eliminates a range of concerns and prev entative overhead regarding header spoofing/smuggling.
- It is significantly easier and less error prone to integrate into IIS.
- It supports the optional preservation of post data.
- It supports REMOTE_USER properly, and can be configured to support native IIS Role-based Authorization.

Stateless Clustering

A form of session recovery across clustered SP nodes using encrypted cookies is available. While making clustering much simpler, it does affect the behavior of logout in some cases, but it offers more flexibility for deployers willing to make trade-offs.

Simplified Virtual Hosting Support

A set of virtual hosts can be auto-assigned a distinct entityID without the creation of `<ApplicationOverride>` elements to do so, using the new `entityIDSelf` content setting. While this does not eliminate the overhead of managing metadata for each host, it does eliminate most actual configuration overhead within the SP itself.

In addition, when overrides are still required for other purposes, it is now possible to load XML fragment files containing just the override configurations from a directory at runtime, including adding additional overrides on the fly without configuration reload.

Dynamic Metadata

The Dynamic metadata providers have been enhanced along with many bugs fixed, to match and in some cases surpass the features available with the Identity Provider, including simpler support for MDQ-capable federation servers, local file-based lookup via hash, and greatly enhanced caching and robustness features.

Administrative Logout

An endpoint is available to programmatically remove sessions based on the SP-assigned session ID, with associated communication to an IdP via SOAP where possible (though this is rarely possible). While complex, it is possible to create a more limited shared store of revoked sessions that prevents the stateless session recovery feature from re-creating the session in some cases, without requiring a fully-shared session store.