Red Hat Single Sign-On 7.3

Release Notes

For Use with Red Hat Single Sign-On 7.3

Last Updated: 2020-05-07

Red Hat Single Sign-On 7.3 Release Notes

For Use with Red Hat Single Sign-On 7.3

Legal Notice

Abstract

This guide consists of release notes for Red Hat Single Sign-On

Table of Contents

CHAPTER 1. RED HAT SINGLE SIGN-ON 7.3

1.1. OVERVIEW

Red Hat is proud to announce the release of version 7.3 of Red Hat Single Sign-On (RH-SSO). RH-SSO is based on the Keycloak project, and enables you to secure your web applications by providing Web SSO capabilities based on popular standards such as OpenID Connect, OAuth 2.0, and SAML 2.0. The RH-SSO server acts as an OpenID Connect or SAML-based identity provider (IdP), allowing your enterprise user directory or third-party IdP to secure your applications via standards-based security tokens.

The following notes apply to the RH-SSO 7.3 release.

1.2. NEW OR IMPROVED FEATURES

Some of the new features in this release are technology preview features, which means they are available, but not fully supported. You may use these for testing, but features marked for technology preview are not supported for use in production. These are marked as technology preview in this list and in our documentation. Because they are not fully supported for production use, technology preview features are disabled by default, but the features can be enabled if you want to try them out. We are seeking feedback on the technology preview features, so please log a support ticket if you have comments on a technology preview feature. Once a feature transitions from technology preview to production supported, the API and functionality are fixed for the lifecyle of the major version, so comments during the tech preview period are critical to influencing a feature in the way you want.

Existing features that remain in tech preview in this release include:

- Token exchange
- Fine-grained authorization permissions
- Cross data-center replication
- Rules (Drools) based policies in Authorization Services

1.2.1. Authorization Services

Authorization Services was introduced as a technology preview feature in the RH-SSO 7.1 release. In 7.3 it is now fully supported, except for a small subcomponent related to custom rules implemented using Drools, which remains tech preview.

Authorization Services has been upgraded to be based on the new User Managed Access 2.0 (UMA 2.0) specification. Previous releases relied on the UMA 1.0 version. Upgrading introduced the ability for users to manage their resources, associated permissions, approve requests to access and share them with other users through the account management console.

Many smaller improvements and additions have also been made:

- Resource attributes - It is now possible to define attributes on resources in order to have them used by policies when evaluating permissions.
- Adapter improvement - NodeJS adapter support for authorization services has been added.
- Improvements to the Evaluation API - Access information from the current realm such as checking for user roles, groups and attributes. Push back arbitrary claims to the resource server in order to provide additional information on how a specific permissions should be enforced.

- Asynchronous authorization flow - Client applications can now choose whether or not an authorization request should start an authorization flow to ask for the resource owner approval. This functionality allows applications to ask for resource owner approval when trying to access one of his resources on behalf of another user.

- User-managed Permission API - Resource servers are now capable of associating additional policies to resources owned by a particular user. The new API provides operations to manage these permissions using different policy types such as role, group, user, client, or a condition using JavaScript.

- Pushed claims - Client applications are now able to send arbitrary claims to Keycloak along with an authorization request in order to evaluate permissions based on these claims. This is a very handy addition when access should be granted (or denied) in the scope of a specific transaction or based on information about the runtime.

- Policy enforcer - The policy enforcer now accepts regular access tokens, longer requiring to exchange access tokens with RPTs in order to access resources protected by a resource server (when not using UMA). Depending on how the policy enforcer is configured on the resource server side, regular access tokens as a bearer token can be leveraged.

- Additional changes - Performance improvements and optimizations with additional configuration options for further performance profiling depending on particular application needs.

1.2.1.1. Rule-based Policies in Authorization Services is in Tech Preview

There remains a subcomponent of Authorization Services related to custom rules implemented using Drools functionality that is in technology preview.

Features marked for technology preview are not supported for use in production.

1.2.2. OpenShift Integration

It is now possible to fully secure OpenShift 3.11 with Red Hat Single Sign-On, including the ability to automatically expose Service Accounts as OAuth clients as clients to Red Hat Single Sign-On. This feature is currently in technology preview.

Features marked for technology preview are not supported for use in production.

1.2.3. New Capabilities in Client Adapters

- Fuse 7 - Fuse adapter aligned with latest Fuse 7 release

- Sprint Boot 2 support

- JavaScript -

    - Native Promise Support - The JavaScript adapter now supports native promises. It retains support for the old style promises as well. Both can be used interchangeably.

    - JavaScript - Cordova mode now allows passing Cordova-specific options to login and other methods in the JavaScript adapter. We also added support for using browser tab and universal links in the JavaScript adapter for Cordova. This enables SSO between multiple applications as well as increases security.

- SAML adapter multitenancy support - allowing integrating with multiple Keycloak realms like already possible in OpenID Connect adapter.

1.2.4. New Signature Algorithms

RH-SSO server now has support for RS256, RS384, RS512, ES256, ES384, ES512, HS256, HS384 and HS512.

Elliptic Curve Digital Signature Algorithm (ES256/384/512) is now supported and provides similar security properties as RSA signatures, but use significantly less CPU.

HMAC (HS256/384/512) is now supported and allows preventing an application from attempting to verify the signature itself. Since these are symmetric signatures only Keycloak is able to verify the signature, which requires the application to use the token introspection endpoint to verify tokens.

RH-SSO adapters do not yet have support for the additional signature algorithms and currently only support RS256.

1.2.5. Hostname Handling

We introduced a more flexible way to configure the hostname for RH-SSO which gives greater flexibility when deployed in Cloud-related environments. It can be determined based on request headers or configured as a fixed hostname. The latter makes sure that only valid hostnames can be used and also allows internal applications to invoke RH-SSO through an alternative URL.

1.2.6. X509 Client Authenticator

The newly added Client Authenticator uses X509 Client Certificates and Mutual TLS to secure a connection from the client. In addition, the RH-SSO Server validates the Subject DN field of the client's certificate.

1.2.7. Client Scopes

We added support for Client Scopes, which replace Client Templates. Client Scopes are a more flexible approach and also provide better support for the OAuth scope parameter.

There are changes related to Client Scopes to the consent screen. The list on the consent screen is now linked to client scopes instead of protocol mappers and roles.

See the documentation and the migration guide for more details.

1.2.7.1. Improved Audience Support for OpenID Connect Clients

It is now possible to specify the audiences in the tokens issued for OpenID Connect clients. There is also support for verification of audience on the adapter side.

1.2.8. OAuth 2 Certificate Bound Access Tokens

We now have a partial implementation of the specification OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens. Specifically, we now have support for the Certificate Bound Access Tokens. If your confidential client is able to use 2-way SSL, RH-SSO will be able to add the hash of the client certificate into the tokens issued for the client. At this moment, it is just RH-SSO itself which verifies the token hashes (for example during refresh token requests). We plan to add support to adapters as well. We also plan to add support for Mutual TLS Client Authentication. Themes and Theme Resources

It is now possible to hot-deploy themes to RH-SSO through a regular provider deployment. We have also added support for theme resources, which allows adding additional templates and resources without creating a theme. This is useful for custom authenticators that require additional pages to be added to the authentication flow.

We have also added support to override the theme for specific clients. If that is not adequate for your needs, then there is also a new Theme Selector SPI that allows you to implement custom logic to select the theme.

1.2.9. UI improvements

The design of the following pages are updated in the 7.3 release:

- The welcome page
- The login page

1.2.10. Enhanced Remember Me

Introduced the ability to specify different session idle and max timeouts for remember me sessions. This enables remember me sessions to live longer than regular sessions.

1.2.11. Pagination support for Groups

Large numbers of groups have previously caused issues in the admin console. This is now resolved by the introduction of pagination of groups.

1.2.12. Improve startup time with large number of offline sessions

In the past, starting RH-SSO could take a long time if there were many offline sessions. This startup time has now been significantly reduced.

1.2.13. Support for DB2 removed

DB2 support has been deprecated for a while. With this release we have removed all support for DB2.

1.2.14. Minor Improvements

- Authenticator to automatically link Identity Provider identity to an existing account after first Idp authentication.
- Allow passing current locale to OAuth2 IdPs
- Support Content-Security-Policy-Report-Only security header
- Script based ProtocolMapper for SAML
- We have added support to login with Instagram
- Search by User ID in Admin Console
- Support Hosted Domain for Google Logins using the **hd** parameter
- Added option to create claims with dots (.) in them

1.3. FIXED ISSUES

More than 1,200 issues were resolved in this release.

- https://issues.redhat.com/issues/?filter=12337585

1.4. KNOWN ISSUES

The following are known issues for this release.

- KEYCLOAK-6127 - Role manage-users still required for some operations regardless granted permission
- KEYCLOAK-8043 - prompt=none doesn't work with default identity provider
- KEYCLOAK-8049 - Nullpointer when create group policy for the root node
- KEYCLOAK-8766 - CORS with OIDC requests fails when using elytron adapter
- KEYCLOAK-8821 - When KeycloakApplication is not successfully deployed server.log's content is erased
- KEYCLOAK-8867 - Return resource associated with policies when querying via uma-policy
- KEYCLOAK-8957 - Federated ID Login results in broken user accounts
- KEYCLOAK-9093 - False-Positive UMA Policy Evaluation
- KEYCLOAK-9095 - NullpointerException in AuthenticatedActionsHandler when Web Origins is null
- KEYCLOAK-9183 - NullPointerException when validating password via LDAPStorageProvider for a no longer existing LDAP entry
- KEYCLOAK-9272 - NullPointer if truststore password is missing
- KEYCLOAK-9310 - Removing custom required action provider corrupts the Realm model
- KEYCLOAK-10211 - SSSD integration is not working on RHEL8 because libunix-dbus-java is missing
- KEYCLOAK-10238 - The Securing Applications and Services Guide is missing instructions for adapter installation on RHEL 8. The installation process is the same as in the previous release, but requires RHEL 8 repository names. Be sure to install EAP from the same repository first.
- KEYCLOAK-10239 - The Securing Applications and Services Guide has obsolete package names in the RPM installation section.
- KEYCLOAK-10260 - Invalid permissions on the .installation directory prevents installing a patch. To work around this issue, navigate to the rhsso-7.3 directory and issue this command: chmod 775 .installation

1.5. SUPPORTED CONFIGURATIONS

The set of supported features and configurations for RH-SSO Server 7.3 is available on the Customer Portal.

1.6. COMPONENT VERSIONS

The list of supported component versions for RH-SSO 7.3 is available on the Customer Portal.