Red Hat Single Sign-On 7.2

Release Notes

For Use with Red Hat Single Sign-On 7.2

Last Updated: 2018-02-01

Red Hat Single Sign-On 7.2 Release Notes

For Use with Red Hat Single Sign-On 7.2

Legal Notice

Abstract

These release notes contain important information related to Red Hat Single Sign-On 7.2

Table of Contents

CHAPTER 1. OVERVIEW **3**

CHAPTER 2. FEATURE OVERVIEW **4**
2.1. CLUSTERED DATABASE SUPPORT 4
2.2. NO-IMPORT LDAP OPTION 4
2.3. BLACKLISTED PASSWORD POLICY 4
2.4. X.509 USER AUTHENTICATION 4
2.5. NEW ADAPTERS 4
2.6. ADDITIONAL SOCIAL LOGINS 4
2.7. CROSS-DATACENTER REPLICATION MODE 4
2.8. TOKEN EXCHANGE 4
2.9. FINE-GRAINED PERMISSIONS FOR ADMIN ENDPOINTS/CONSOLE 5
2.10. AUTHORIZATION SERVICES REMAINS IN TECH PREVIEW 5

CHAPTER 3. SUPPORTED CONFIGURATIONS **6**
3.1. SUPPORTED CONFIGURATIONS 6

CHAPTER 4. COMPONENT VERSIONS **7**
4.1. COMPONENT VERSIONS 7

CHAPTER 5. KNOWN ISSUES **8**
5.1. KNOWN ISSUES 8

CHAPTER 6. FIXED ISSUES **9**
6.1. FIXED ISSUES 9

CHAPTER 1. OVERVIEW

The Red Hat Single Sign-On (RH-SSO) Server, based on the Keycloak project, enables you to secure your web applications by providing Web SSO capabilities based on popular standards such as SAML 2.0, OpenID Connect, and OAuth 2.0. The Server can act as a SAML or OpenID Connect–based identity provider (IdP), mediating with your enterprise user directory or third-party identity provider for identity information and your applications using standards-based tokens.

The following notes apply to the RH-SSO 7.2 release.

CHAPTER 2. FEATURE OVERVIEW

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 will not be supported if used in production and 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, please log a support ticket if you have comments on a technology preview feature.

2.1. CLUSTERED DATABASE SUPPORT

RH-SSO is now supported on Oracle RAC and MySQL/Galera clusters.

2.2. NO-IMPORT LDAP OPTION

No-import LDAP reduces the load on the RH-SSO database. User data is not imported into the RH-SSO database, and all user data requests are forwarded to LDAP. Initial import of the data and ongoing synchronization are eliminated.

2.3. BLACKLISTED PASSWORD POLICY

Administrators can now provide a list of blacklisted passwords, ensuring that end users cannot select specific banned passwords.

2.4. X.509 USER AUTHENTICATION

Browser and Direct Grant authentication flows now support user authentication via X.509 Certificates.

2.5. NEW ADAPTERS

Adapters for Spring Boot applications and Servlet based applications are now available and generally supported.

An adapter for Elytron, the new security subsystem for Red Hat JBoss EAP is generally available. The adapter enables SSO with the EAP Administrative console and the management CLI.

2.6. ADDITIONAL SOCIAL LOGINS

Social login with GitLab, BitBucket, OpenShift, and PayPal have been added to the list of social login providers supported by RH-SSO.

2.7. CROSS-DATACENTER REPLICATION MODE

Cross-Datacenter Replication mode allows you to run RH-SSO in a cluster across multiple data centers, most typically using data center sites that are in different geographic regions. When using this mode, each data center will have its own cluster of Red Hat Single Sign-On servers.

This functionality is in technology preview and should not be used in production environments.

2.8. TOKEN EXCHANGE

Token exchange is the process of using a token to obtain an entirely different token. A client may want to invoke on a less trusted application so it may want to downgrade the current token it has. A client may want to exchange a {project_token} for a token stored for a linked social provider account. You may want to trust external tokens minted by other RH-SSO realms or foreign IDPs. A client may have a need to impersonate a user.

Token exchange in RH-SSO is a very loose implementation of the OAuth Token Exchange specification at the IETF. We have extended it a little, ignored some of it, and loosely interpreted other parts of the specification. It is a simple grant type invocation on a realm's OpenID Connect token endpoint.

This functionality is in technology preview and should not be used in production environments.

2.9. FINE-GRAINED PERMISSIONS FOR ADMIN ENDPOINTS/CONSOLE

Sometimes roles like manage-realm or manage-users do not give you the ability to specify permissions with the level of control you may desire and you want to create restricted admin accounts that have more precise permissions. RH-SSO allows you to define and assign restricted access policies for managing a realm, such as managing only one specific client or the users of a specific group.

Note that:

- Fine-grained permissions are only available within dedicated admin consoles and admins defined within those realms. You cannot define cross-realm fine grained permissions.
- Fine-grained permissions are used to grant additional permissions. You cannot override the default behavior of the built in admin roles.

This functionality is in technology preview and should not be used in production environments.

2.10. AUTHORIZATION SERVICES REMAINS IN TECH PREVIEW

RH-SSO 7.1 introduced a new authorization service feature-set, based on the User Managed Access (UMA) specification. This enables RH-SSO Server to act as a Policy Administration Point (PAP), Policy Decision Point (PDP), or Policy Information Point (PIP), separating the authorization logic from the application.

This functionality is in technology preview and should not be used in production environments, as we plan to update to to UMA 2.0.

CHAPTER 3. SUPPORTED CONFIGURATIONS

3.1. SUPPORTED CONFIGURATIONS

The set of supported features and configurations for RH-SSO Server 7.2 is available on the Customer Portal.

CHAPTER 4. COMPONENT VERSIONS

4.1. COMPONENT VERSIONS

The list of supported component versions for RH-SSO 7.2 is available on the Customer Portal.

CHAPTER 5. KNOWN ISSUES

5.1. KNOWN ISSUES

The following are known issues for this release.

- KEYCLOAK-4976 - AbstractUserAdapterFederatedStorage.setSingleAttribute(,) causing deadlocks on MSSQL
- KEYCLOAK-5411 - MSSQL client creation deadlocks
- KEYCLOAK-6142 - Manual configuration page for the OTP doesn't reflect HOTP
- KEYCLOAK-6171 and KEYCLOAK-6286 - Node.js and Java adapters for RH-SSO 7.1 don't remove "session_state" from URL after login to RH-SSO 7.2 The issue should only affect users who were logged in but inactive before an RH-SSO upgrade who then find themselves logged out after the RHSSO upgrade is complete when they attempt to use that same session. The workaround is that the users must log in again.
- KEYCLOAK-6309 - Eap6 SAML filter fails while downloading keys from Keycloak server when SSL is enabled Two workarounds are available. You may either use bouncy castle version 1.52 instead of 1.56 OR you may start EAP6 with the argument `**-Dcom.sun.net.ssl.enableECC=false**.
- KEYCLOAK-6451 - Adapter RPMs have an obsolete dependency, meaning that any customer who previously installed adapters using RPMs that executes **`yum update`** will find the package updated. The workaround is to exclude the adapter package from yum update.
- When a resource permission is created with no associated policies and you try to update the permission, the Save button is not enabled in the Resource Permission UI when adding new policies to the permission.
- Authorization services client does not support JDK7 At the moment, this means you must use Java 8 if you want to try the new authorization services, which are currently in technology preview.

CHAPTER 6. FIXED ISSUES

6.1. FIXED ISSUES

Nearly 1,000 issues were resolved in this release.

- https://issues.jboss.org/issues/?filter=12334077