Red Hat Single Sign-On 7.5

Release Notes

For Use with Red Hat Single Sign-On 7.5

Last Updated: 2021-09-22

Red Hat Single Sign-On 7.5 Release Notes

For Use with Red Hat Single Sign-On 7.5

Legal Notice

Abstract

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

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

CHAPTER 1. RED HAT SINGLE SIGN-ON 7.5.0.GA

1.1. OVERVIEW

Red Hat is proud to announce the release of version 7.5 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.

NOTE

Red Hat Single Sign-On for IBM Z and IBM Power Systems is supported only in the OpenShift environment. Bare metal installations on IBM Z and IBM Power Systems are not supported.

The following notes apply to the RH-SSO 7.5 release.

1.2. NEW OR IMPROVED FEATURES

1.2.1. Financial-grade API, FAPI CIBA, and Open Banking Brasil

The Red Hat Single Sign-On server provides support for the Financial-grade API (FAPI). Red Hat Single Sign-On is compliant with the OpenID Connect Client Initiated Backchannel Authentication (CIBA) and OpenBanking Brasil. Support also exists for CIBA ping mode.

To ensure that the Red Hat Single Sign-On server validates your client to be more secure and FAPI compliant, you can configure FAPI client policies. These policies ensure security best practices such as SSL requirements for clients and secure redirect URI. For more details, see the FAPI section of Securing Applications and Services Guide.

1.2.2. New Account Console

The Account Console, previously called the User Account Service, has been revised and is now the default Account Console in Red Hat Single Sign-On. However, if you have a custom theme for the User Account Service, that console remains the default console for this release. Therefore, you have time to update your custom theme to the new Account Console.

The new console uses GZip to optimize the download of artifacts.

1.2.3. Upgrade login theme to PatternFly 4

The Red Hat Single Sign-On login theme components have been upgraded to PatternFly 4. PatternFly 3 runs simultaneously with the new version, so PatternFly 3 components can coexist.

Also, the login theme provides a better user experience and you can define icons for your custom Identity providers. For details, see the Server Developer Guide.

1.2.4. Users can delete their own accounts

You can allow users in a given realm to delete their own account through the Account Console. This capability is enabled by the **Delete Account** action in the Admin Console.

1.2.5. Identity brokering sync-mode

With Identity Brokering Sync Mode, you can now control if user profiles are updated on the first login or on every login from an external Identity Provider. You can also override this behavior on individual mappers.

1.2.6. Client Session Timeout for OpenID Connect / OAuth 2.0

Typically, an SSO session lasts for days or even months, but individual client sessions should ideally be much shorter. You can now configure a separate timeout for individual clients and a default for all clients within a realm.

You can also configure a client offline session timeout, which determines the maximum time before an offline token is expired and invalidated.

1.2.7. OAuth 2.0 Token Revocation (RFC 7009)

For applications that use Red Hat Single Sign-On as an OAuth 2.0 Authorization Server, you can now revoke refresh tokens through the token revocation endpoint.

1.2.8. OAuth 2.0 Device Authorization Grant (RFC 8628)

Support for OAuth 2.0 Device Authorization Grant is now available.

1.2.9. OpenID Connect Back-channel logout

Support for OpenID Connect Back-Channel Logout is now available.

1.2.10. Improvements to offline sessions

Offline session preloading has been improved, providing faster performance.

1.2.11. Additional improvements

1.2.11.1. Custom claims for AccessTokenResponse

You can now add custom claims to the AccessTokenResponse. This is a generic enhancement but it supports a healthcare provider standard that is part of US regulations.

1.2.11.2. Support PKCE for identity brokering

Red Hat Single Sign-On can now leverage PKCE when brokering to an external OpenID Connect Identity Provider.

1.2.11.3. Improvements to User Profile SPI and support for declarative configuration

The user Profile SPI has been improved to better facilitate management of user profiles. These improvements include support for configuring user profiles through the Admin Console. For more details, see the Server Administration Guide

1.2.11.4. SAML Artifact binding in server to client communication

Red Hat Single Sign-On now supports communication with clients using SAML *Artifact* binding. A new

Force Artifact Binding option is available in the client configuration. It forces communication with the client using artifact messages. For more details, see Server Administration Guide. Note, that with this version, Red Hat Single Sign-On SAML client adapter does NOT support Artifact binding.

1.2.11.5. Default roles processing improvement

Default roles are now internally stored as new composite roles, which are typically named **default-roles-<realmName>**. Previously realm roles and client default roles were directly assigned to new users and to users who were imported through Identity Brokering. However, now the composite role is assigned to them and other default roles are assigned as effective roles. This change improves performance of default roles processing, especially with a larger number of clients. It is no longer necessary to go through all clients.

1.2.11.6. Not email password policy

You can use a Not Email policy to disallow a password to be the same as the email address.

1.2.11.7. Support for a redirect-uri for any port with http://127.0.0.1

http://localhost is used as a callback when an HTTP server is started on a random port. The best practice is to use http://127.0.0.1 instead of localhost.

1.2.12. Other improvements

- Support for invoking Application Initiated Actions added to Red Hat Single Sign-On JavaScript adapter.
- Support for AES 192 and AES 256 algorithms used for signed and encrypted ID tokens.
- Support for OAuth2 Client Credentials grant without refresh token and without user session.
- Support for send access tokens to the OAuth2 Revocation endpoint.
- Support for configuring a maximum number of active authentication sessions. The default value is set to 300 authentication sessions (browser tabs) per browser session.
- Support for LDAPv3 password modify operation, including the Admin Console ability to request metadata from the configured LDAP server to see if it supports LDAPv3 password modify operations.
- Namespace support for LDAP group mapper. You can map groups from LDAP under a specified branch (namespace) of the Red Hat Single Sign-On groups tree. Previously groups from LDAP were always added as the top level groups in Red Hat Single Sign-On
- Support for specification of AuthnContext section in authentication requests issued by a SAML identity provider has been added.
- Performance improvements to fetching resources and policies during evaluation
- A new Identity Provider Mapper, **OIDC Advanced attribute to role mapper**, was added as a counterpart to the SAML mapper, Advanced Claim to Role Mapper. The new mapper supports regex for attribute values and multiple attribute values.

1.3. EXISTING TECHNOLOGY PREVIEW FEATURES

The following features continue to be in a Technology Preview status:

- Cross-site data replication
- RH-SSO Operator
- Token exchange
- Fine-grained authorization permissions
- W3C Web Authentication (WebAuthn)

1.4. REMOVED OR DEPRECATED FEATURES

These features have a change in status:

- RH-SSO 7.5 does not support installation on Red Hat Enterprise Linux 6 (RHEL 6). RHEL 6 entered the ELS phase of its lifecycle on November 30, 2020. Customers should deploy their RH-SSO 7.5 upgrades on RHEL 7 or 8 versions.
- Installation from an RPM is deprecated. RH-SSO will continue to deliver RPMs for the life of the 7.x product, but will not deliver RPMs with the next major version. The product will continue to support installation from a ZIP file and installation on OpenShift.
- Authorization Services Drools Policy was removed at RH-SSO 7.4.
- Upload of scripts through admin rest endpoints/console is deprecated. It will be removed at a future release.

1.5. FIXED ISSUES

More than 3,700 issues were fixed between RH-SSO 7.4 and 7.5.0. For details, see RHSSO 7.5.0 Fixed Issues.

1.6. KNOWN ISSUES

This release includes the following known issues:

- KEYCLOAK-18115 - Attempt to edit attribute denied in RHSSO 7.4.6
- KEYCLOAK-18338 - Attempt to update user account with configured SSSD leads to Internal Server Error
- KEYCLOAK-18994 - deleteExpiredClientSessions very slow on MariaDB

1.7. SUPPORTED CONFIGURATIONS

The set of supported features and configurations for RH-SSO Server 7.5 is available on the Customer Portal.

1.8. COMPONENT VERSIONS

The list of supported component versions for RH-SSO 7.5 is available on the Customer Portal.

1.9. RED HAT SINGLE SIGN-ON METERING LABELS FOR RED HAT OPENSHIFT

You can add metering labels to your Red Hat Single Sign-On pods and check Red Hat subscription details with the OpenShift Metering Operator.

NOTE

Do not add metering labels to any pods that an operator deploys and manages.

Red Hat Single Sign-On can use the following metering labels:

- **com.redhat.component-name: Red Hat Single Sign-On**
- **com.redhat.component-type: application**
- **com.redhat.component-version: 7.5**
- **com.redhat.product-name: "Red_Hat_Runtimes"**
- **com.redhat.product-version: 2020/Q2**

Additional resources

- Configuring and using Metering in OpenShift Container Platform