Red Hat Single Sign-On 7.6

Release Notes

For Use with Red Hat Single Sign-On 7.6

Last Updated: 2024-09-19

Red Hat Single Sign-On 7.6 Release Notes

For Use with Red Hat Single Sign-On 7.6

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 7.6.0.GA

1.1. OVERVIEW

Red Hat is proud to announce the release of version 7.6 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 7.6 release.

1.2. NEW OR IMPROVED FEATURES

1.2.1. Step-up authentication

Red Hat Single Sign-On now supports Step-up authentication. For more details, see the Server Administration Guide.

1.2.2. Client secret rotation

Red Hat Single Sign-On now supports Client Secret Rotation through customer policies. This feature is now available as a preview feature and allows that confidential clients can be provided with realm policies allowing the use up to two secrets simultaneously.

For more details, see the Server Administration Guide.

1.2.3. Recovery Codes

Recovery Codes as another way to do two-factor authentication is now available as a preview feature.

1.2.4. OpenID Connect Logout Improvements

Some fixes and improvements were made to make sure that Red Hat Single Sign-On is now fully compliant with all the OpenID Connect logout specifications:

- OpenID Connect RP-Initiated Logout 1.0
- OpenID Connect Front-Channel Logout 1.0
- OpenID Connect Back-Channel Logout 1.0
- OpenID Connect Session Management 1.0

For more details, see the Server Administration Guide.

1.2.5. WebAuthn improvements

WebAuthn is no longer a Technical Preview feature. It is now fully supported.

Also, Red Hat Single Sign-On now supports WebAuthn id-less authentication. This feature allows that WebAuthn Security Key will identify the user during authentication as long as the security key supports Resident Keys. For more details, see the Server Administration Guide.

1.2.6. Session limits

Red Hat Single Sign-On now supports limits on the number of sessions a user can have. Limits can be placed at the realm level or at the client level.

For more details, see the Server Administration Guide.

1.2.7. SAML ECP Profile is disabled by default

To mitigate the risk of abusing SAML ECP Profile, Red Hat Single Sign-On now blocks this flow for all SAML clients that do not allow it explicitly. The profile can be enabled using *Allow ECP Flow* flag within client configuration, see Server Administration Guide.

1.3. IMPROVEMENTS IN LDAP AND KERBEROS INTEGRATION

From RH-SSO 7.6.9, Red Hat Single Sign-On supports multiple LDAP providers in a realm, which support Kerberos integration with the same Kerberos realm. When an LDAP provider is not able to find the user which was authenticated through Kerberos/SPNEGO, Red Hat Single Sign-On ties to fallback to the next LDAP provider. Red Hat Single Sign-On has also better support for the case when single LDAP provider supports multiple Kerberos realms, which are in trust with each other.

1.3.1. Other improvements

- Account console alignments with latest PatternFly release.
- Support for encrypted User Info endpoint response.
- Support for the algorithm RSA-OAEP with A256GCM used for encryption keys.
- Support for login with GitHub Enterprise server.

1.4. EXISTING TECHNOLOGY PREVIEW FEATURES

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

- Token exchange
- Fine-grained authorization permissions

1.5. REMOVED OR DEPRECATED FEATURES

These features have a change in status:

- Cross-site replication, which was introduced as a Technology Preview feature in Red Hat Single Sign-On 7.2, is no longer available as a supported feature in any Red Hat SSO 7.x release including the latest RH-SSO 7.6 release. Red Hat does not recommend any customer

implement or use this feature in their environment because it is not supported. Also, support exceptions for this feature are no longer considered or accepted.
A new solution for cross-site replication is being discussed and tentatively considered for a future release of Red Hat build of Keycloak (RHBK), which is the product that will be introduced instead of Red Hat SSO 8. More details will be available soon.

- The **podDisruptionBudget** field in the Keycloak CR is deprecated and will be ignored when the Operator is deployed on OpenShift 4.12 and higher. As a workaround, see the Upgrading Guide.
- The deprecated **upload-script** feature has been removed.
- Support for Red Hat Single Sign-On (RH-SSO) on Red Hat Enterprise Linux 6 (RHEL 6) is deprecated and the 7.6 release of RH-SSO will not be supported on RHEL 6. RHEL 6 entered the ELS phase of its lifecycle on November 30, 2020 and the Red Hat JBoss Enterprise Application Platform (EAP) that RH-SSO depends upon will drop support for RHEL 6 with the EAP 7.4 release. Customers should deploy their RH-SSO 7.6 upgrades on RHEL 7 or 8 versions.
- The Spring Boot Adapter is deprecated and will not be included in the 8.0 and higher versions of RH-SSO. This adapter will be maintained during the lifecycle of RH-SSO 7.x. Users are urged to migrate to Spring Security to integrate their Spring Boot applications with RH-SSO.
- Installation from an RPM is deprecated. Red Hat Single Sign-On 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.
- Red Hat Single Sign-On for OpenShift on Eclipse OpenJ9 is deprecated. However, Red Hat Single Sign-On on OpenShift will now support all platforms (x86, IBM Z, and IBM Power Systems) as documented in the Red Hat Single Sign-On for OpenShift Guide . For more details on this change, see Java Change in PPC and s390x OpenShift Images .
- Authorization Services Drools Policy has been removed.

1.6. FIXED ISSUES

For details on the issues fixed between RH-SSO 7.5 and 7.6.0, see RHSSO 7.6.0 Fixed Issues.

After 7.6.0 release we also introduced a patch release for the Red Hat Single Sign-On Operator to fix a critical issue that prevented the upgrade from 7.5.2 to 7.6.0 using the Operator. See the Upgrading Guide for more details and caveats.

1.7. KNOWN ISSUES

This release includes the following known issues:

- KEYCLOAK-18115 - Attempt to edit attribute denied in RHSSO 7.4.6

1.8. CVES

At this release, the following CVEs are fixed:

- CVE-2024-8883 Vulnerable redirect URI validation results in Open Redirect
- CVE-2024-8698 Improper verification of SAML responses leading to privilege escalation in Red Hat Single Sign-On

- CVE-2024-7341 Session fixation in elytron SAML adapters for better protection against a possible Cookie hijacking.
- CVE-2024-5967 Leak of configured LDAP bind credentials through the Admin Console. There is the possibility to change the hostURL to the attacker's machine with the appropriate permission.
- CVE-2024-4629 An attacker could potentially bypass brute force protection by launching multiple login attempts in parallel.
- CVE-2024-4540, an important security issue affecting some OIDC confidential clients using PAR (Pushed authorization request). In case you use OIDC confidential clients together with PAR and you use client authentication based on **client_id** and **client_secret** sent as parameters in the HTTP request body (method **client_secret_post** specified in the OIDC specification), it is highly encouraged to rotate the client secrets of your clients after upgrading to this version.

1.9. SUPPORTED CONFIGURATIONS

The set of supported features and configurations for RH-SSO Server 7.6 is available on the Customer Portal.

1.10. COMPONENT VERSIONS

The list of supported component versions for RH-SSO 7.6 is available on the Customer Portal.

1.11. 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: 7.6**
- **com.redhat.product-name: "Red_Hat_Runtimes"**
- **com.redhat.product-version: 2020/Q2**

Additional resources

- Configuring and using Metering in OpenShift Container Platform