Red Hat Single Sign-On 7.1 Release Notes

For Use with Red Hat Single Sign-On 7.1

Red Hat Customer Content Services

Red Hat Single Sign-On 7.1 Release Notes

For Use with Red Hat Single Sign-On 7.1

Legal Notice

Abstract

These release notes contain important information related to Red Hat Single Sign-On 7.1

Table of Contents

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.

CHAPTER 2. FEATURE OVERVIEW

2.1. OPENID CONNECT CERTIFICATION

The Keycloak version included in Red Hat Single Sign-On (RH-SSO) 7.1 conforms to the 5 OpenID Connect profiles: Basic, Implicit, Hybrid, Config, and Dynamic. Certification was achieved in Keycloak v2.3 (http://openid.net/certification/). Future RH-SSO 7.x versions will remain compatible with these profiles, unless documented otherwise.

2.2. CLIENT ADAPTER FOR RED HAT JBOSS FUSE

RH-SSO 7.1 features a new client adapter for Red Hat JBoss Fuse, which enables securing of web application archives (WARs), servlets, Apache routes and Apache CXF endpoints deployed on JBoss Fuse, in both the Apache Karaf and Red Hat JBoss Enterprise Application Platform (JBoss EAP).

2.3. NODE.JS CLIENT ADAPTER

RH-SSO 7.1 includes a new Node.js client adapter, which enables use of RH-SSO 7.1 Server for authentication and web single sign-on for Node.js applications.

2.4. EXTERNALIZED AUTHORIZATION SERVICE

RH-SSO 7.1 introduces a new authorization service feature-set, based on the User Managed Access (UMA) specification. This enables RH-SSO 7.1 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.

2.5. USER STORAGE SPI

RH-SSO 7.1 features a new User Storage SPI that you can use to implement your own custom user storage federation provider, such as a relational or NoSQL database, to enable federation of users from any user store.

2.6. SSSD INTEGRATION

RH-SSO 7.1 adds an integration with System Security Services Daemon (SSSD) in Red Hat Enterprise Linux (RHEL) 7.3. This enables use of SSSD as a user federation provider in front of a Microsoft Active Directory forest.

2.7. CLIENT REGISTRATION CLI

RH SSO 7.1 introduces a command-line interface (CLI) for developers to register client applications on RH-SSO Server.

2.8. RPM DISTRIBUTION

RH-SSO 7.1 introduces a new RPM distribution for Red Hat Enterprise Linux 6 and 7. The RH-SSO Server is provided in its own channel; the client adapters for JBoss EAP 6 and 7 are provided in their respective JBoss EAP x86_64 channels. The JBoss Fuse and Node.js client adapters are not available as RPMs.

CHAPTER 3. SUPPORTED CONFIGURATIONS

3.1. SUPPORTED CONFIGURATIONS

The set of supported features and configurations for RH-SSO Server 7.1 is available on the Customer Portal.

CHAPTER 4. COMPONENT VERSIONS

4.1. COMPONENT VERSIONS

The list of supported component versions for Red Hat Single Sign-On 7.1 is available on the Customer Portal.

CHAPTER 5. KNOWN ISSUES

5.1. KNOWN ISSUES

1. (7.1.z) SAML encrypted assertion with newlines fails during parsing
2. No proper way to set JDBC_PING
3. Client's logout handling gets stuck between HTTP-POST and HTTP-Redirect
4. (7.1.z) SAML logouts are not invalidating the sessions for all logged-in applications
5. SAML isPassive not working with 7.0 adapter
6. Fuse adapter: Login to Hawt.io with user without admin role
7. "Add user federation provider" form doesn't validate "Custom User LDAP Filter" field
8. Disabling Authorization for a client deletes all authorization data
9. searchForUserByUserAttribute does not filter users by realm
10. Deleting a client with existing sessions/offline_tokens leads to Internal Server Errors
11. MAX_LIFESPAN cache policy does not evict objects
12. NPE when requesting .well-known URI for which no provider exists
13. Unexpected error when creating client with existing client ID
14. Kerberos flow is executed even when no Kerberos provider is present
15. keycloak-nodejs-auth-utils chokes on TLS errors instead of catching them
16. NPE fix for HttpMethod
17. Wrong message when a temporarily disabled user requests password reset
18. TypeError: this.reject is not a function
19. Import of huge certificates fails
20. Periodic sync of User Storage Provider SPI does not work
21. Access token appears to be valid even though session has expired in the background
22. Error when session expired and ajax request execute in Keycloak
23. SAML IdP only imports one key from metadata
24. Export/Import clients functionality not working as expected
25. Unhandled ReadOnlyException in Account Management when updating user from read-only store
26. Cannot import realm, which contains user-based authorization policy
27. UserRemovedEvent not triggered when userStorage provider is removed
28. Removing userSessions is very slow when removing many sessions

29. SAML federation link fails to work with read-only LDAP user