



Red Hat Single Sign-On 7.0 Release Notes

Release Notes

Red Hat Customer Content
Services

Red Hat Single Sign-On 7.0 Release Notes

Release Notes

Legal Notice

Copyright © 2017 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

These release notes contain important information related to Red Hat Single Sign-On 7.0

Table of Contents

CHAPTER 1. OVERVIEW	3
1.1. OVERVIEW	3
CHAPTER 2. FEATURE OVERVIEW	4
2.1. SINGLE SIGN-ON(SSO) SERVER	4
2.2. CLIENT ADAPTERS FOR JBOSS EAP	4
2.3. MOD_AUTH_MELLON CERTIFICATION	4
2.4. CLIENT ADAPTER FOR JBOSS FUSE	4
2.5. USER FEDERATION	4
2.6. SPNEGO-BASED KERBEROS	4
2.7. IDENTITY BROKERING	4
2.8. ADMINISTRATION USER INTERFACE (UI) AND REST APIS	4
CHAPTER 3. SUPPORTED CONFIGURATIONS	5
3.1. SUPPORTED CONFIGURATIONS	5
CHAPTER 4. COMPONENT VERSIONS	6
4.1. COMPONENT VERSIONS	6
CHAPTER 5. KNOWN ISSUES	7
5.1. KNOWN ISSUES	7

CHAPTER 1. OVERVIEW

1.1. OVERVIEW

The single sign-on (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, mediating with your enterprise user directory or 3rd-party Identity Provider for identity information and your applications via standards-based tokens.

CHAPTER 2. FEATURE OVERVIEW

2.1. SINGLE SIGN-ON(SSO) SERVER

Red Hat Single Sign-On (RH-SSO) 7.0 includes a standalone SSO server, which serves as a Security Assertion Markup Language (SAML) 2.0 or OpenID Connect-based Identity Provider.

2.2. CLIENT ADAPTERS FOR JBOSS EAP

RH-SSO 7.0 includes client adapters for Red Hat JBoss Enterprise Application Platform (EAP) 6.4 and 7.0. The designated adapters enable JBoss EAP to act as SAML Service Provider or OpenID Connect-based Resource Server, interfacing with standalone RH-SSO Server.

2.3. MOD_AUTH_MELLON CERTIFICATION

RH-SSO 7.0 Server is supported as a SAML 2.0 Identity Provider integrated with the mod_auth_mellon module in Red Hat Enterprise Linux (RHEL) 7.2 acting as SAML 2.0 Service Provider.

2.4. CLIENT ADAPTER FOR JBOSS FUSE

The Maven repository for RH-SSO 7.0 includes a client adapter for Red Hat JBoss Fuse 6.2 as a Technology Preview feature.

2.5. USER FEDERATION

RH-SSO 7.0 is tested with a variety of LDAP servers, Microsoft Active Directory, and RHEL Identity Management (IdM) as one or more federated sources of enterprise user information. For more details on supported integrations, please refer to <https://access.redhat.com/articles/2342861>

2.6. SPNEGO-BASED KERBEROS

RH-SSO 7.0 Server supports SPNEGO integration with Microsoft Active Directory and RHEL Identity Management (IdM), which have been configured to use Kerberos.

2.7. IDENTITY BROKERING

RH-SSO 7.0 integrates with 3rd party SSO Providers and social login providers, such as Facebook, Google, Twitter, for user authentication.

2.8. ADMINISTRATION USER INTERFACE (UI) AND REST APIS

RH-SSO supports an Administration UI as well as REST APIs for a variety of user management, role mapping, client registration, user federation, and identity brokering operations.

CHAPTER 3. SUPPORTED CONFIGURATIONS

3.1. SUPPORTED CONFIGURATIONS

For supported hardware and software configurations and integrations, see the Red Hat Single Sign-On Supported Configurations reference on the Customer Portal at <https://access.redhat.com/articles/2342861>

CHAPTER 4. COMPONENT VERSIONS

4.1. COMPONENT VERSIONS

The full list of component versions used in Red Hat Single Sign-On 7.0 is available at the Customer Portal at <https://access.redhat.com/articles/2342881>

CHAPTER 5. KNOWN ISSUES

5.1. KNOWN ISSUES

1. "Add user federation provider" form doesn't validate "Custom User LDAP Filter" field
2. The "tree lines" menu doesn't work
3. Unstable Admin Console when opening multiple browser tabs
4. Confirm before changing OTP Policy
5. Unable to add an Authenticator app without scanning QR
6. Broken Authenticator Setup with smaller resolutions
7. Composite roles does not work with SAML
8. RESET_PASSWORD_ERROR and UPDATE_PASSWORD_ERROR events not fired
9. Upload-certificate admin endpoint does not nullify private keys
10. Roles assigned to groups are not recognized when users access admin console
11. Kerberos authenticator changed from REQUIRED to ALTERNATIVE during userFederationProvider update
12. Dropdown menu in navigation bar doesn't work with small screens
13. Internal Server Error thrown when Update User API is invoked w/o 'username' parameter
14. IBM DB2 fails if JPA criteria query sets just firstResult but not maxResults
15. Download adapter config from admin console for "signed JWT" clients
16. NPE when accessing Account with invalid clientId set as ?referrer, and additional referrer_uri set
17. SAML ECP Profile Flow is empty
18. OutdatedTopologyException when creating realm during cluster node failback/startup