



Red Hat Single Sign-On 7.0 Administration and Configuration Guide

Administration and Configuration Guide

Red Hat Customer Content
Services

Red Hat Single Sign-On 7.0 Administration and Configuration Guide

Administration and Configuration Guide

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

This guide provides the basic information to help users get started with Red Hat Single Sign-On 7.0 .

Table of Contents

CHAPTER 1. USER MANAGEMENT	3
1.1. LOGIN TO THE ADMINISTRATION CONSOLE	3
1.2. ADD USER	3
1.3. ENABLE AND DISABLE USER	3
1.4. MODIFY THE ROLES OF AN EXISTING USER	3
1.5. RESET USER PASSWORD	4
1.6. ENABLE ONE-TIME-PASSWORD	4
1.7. ACCESS USER HISTORY	4
1.8. UNLOCK USER ACCOUNT	4

CHAPTER 1. USER MANAGEMENT

1.1. LOGIN TO THE ADMINISTRATION CONSOLE

To access the administration console, you need to start the Red Hat Single Sign-On Server. Once the server is running successfully and you can access the landing page at <http://localhost:8080/>

To login to the administration console,

1. Click **Administration Console** link on the landing page.
2. Enter the registered user name and password.
3. Click **Log in**

You will be redirected to the Master Realm in the Administration Console.

1.2. ADD USER

To add a new user to the Red Hat Single Sign-On using the script, follow these steps:

1. On the command line, go to the bin directory of Red Hat Single Sign-On.
2. Run the command "add-user", for example, "add-user.sh --user test --password test123".
3. If the user is added successfully, you will get a confirmation on the commandline.
4. To list the user in the console, restart the RH-SSO server.

1.3. ENABLE AND DISABLE USER

To disable and enable an existing user, follow these steps.

1. Login to the **Administration Console**.
2. Click **Users** → **View all users**.
3. Select the appropriate user and click **Edit**
4. In the **Details** section, Turn Off **User Enabled**.

Similarly to enable user you can Turn ON the **User Enabled** option.

1.4. MODIFY THE ROLES OF AN EXISTING USER

To modify or assign the roles of an existing user follow these steps:

1. Login to the **Administration Console**.

2. Click **Users** → **View all users**.
3. Select the appropriate user, click **Edit**.
4. Click **Role Mapping**.
5. To assign a new role to the user, select the role from the **Available Roles** list and click **Add Selected**.

1.5. RESET USER PASSWORD

You can reset the user password by using the **Forgot Password** link on administration console.

To reset the password,

1. On the **Administration Console** log in page, Click **Forgot Password**.
2. Enter your registered EmailID or Username.
3. Follow the link in your email to reset your password.

1.6. ENABLE ONE-TIME-PASSWORD

To enable One Time Password (OTP), follow these steps:

1. Login to the **Administration Console**.
2. On the top right hand side of the panel, click the username.
3. Click **Manage Account** and click **Authenticator**.
4. Follow the steps shown on the panel.
5. Enter OTP and click **Save**.

1.7. ACCESS USER HISTORY

To access the history of all the session from a user including the IP address and the login and logout time, follow these steps.

1. Login to the **Administration Console**
2. Click **Users** and click **View all users**.
3. Click **Edit** for the Username for which you want to view to session history.
4. Click **Sessions**.

You can see the IP address of the user, the list of clients accessed by the user, and the access time including the login time.

1.8. UNLOCK USER ACCOUNT

The user account can be automatically locked after too many login attempts. To unlock a user account, the administrator can follow these steps:

1. Login to the **Administration Console**.
2. Click **Users, View all users**.
3. Click **Unlock Users**.