



Red Hat Process Automation Manager 7.8

Integrating Red Hat Process Automation Manager with Red Hat Single Sign-On

Red Hat Process Automation Manager 7.8 Integrating Red Hat Process Automation Manager with Red Hat Single Sign-On

Red Hat Customer Content Services
brms-docs@redhat.com

Legal Notice

Copyright © 2020 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, the Red Hat 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 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 document describes how to integrate Red Hat Single Sign-On with Red Hat Process Automation Manager to provide a single secure authentication method.

Table of Contents

PREFACE	3
CHAPTER 1. INTEGRATION OPTIONS	4
CHAPTER 2. INSTALLING AND CONFIGURING RH-SSO	5
CHAPTER 3. RED HAT PROCESS AUTOMATION MANAGER ROLES AND USERS	6
3.1. ADDING RED HAT PROCESS AUTOMATION MANAGER USERS	7
CHAPTER 4. AUTHENTICATING BUSINESS CENTRAL THROUGH RH-SSO	8
4.1. CREATING THE BUSINESS CENTRAL CLIENT FOR RH-SSO	8
4.2. INSTALLING THE RH-SSO CLIENT ADAPTER FOR BUSINESS CENTRAL	9
4.3. SECURING BUSINESS CENTRAL FILE SYSTEM SERVICES USING RH-SSO	12
CHAPTER 5. AUTHENTICATING KIE SERVER THROUGH RH-SSO	15
5.1. CREATING THE KIE SERVER CLIENT ON RH-SSO	15
5.2. INSTALLING AND CONFIGURING KIE SERVER WITH THE CLIENT ADAPTER	16
5.3. KIE SERVER TOKEN-BASED AUTHENTICATION	18
CHAPTER 6. AUTHENTICATING THIRD-PARTY CLIENTS THROUGH RH-SSO	20
6.1. BASIC AUTHENTICATION	20
6.2. TOKEN-BASED AUTHENTICATION	20
APPENDIX A. VERSIONING INFORMATION	22

PREFACE

As a system administrator, you can integrate Red Hat Single Sign-On with Red Hat Process Automation Manager to secure your Red Hat Process Automation Manager browser applications with a single authentication method.

Prerequisites

- Red Hat Process Automation Manager is installed on Red Hat JBoss EAP 7.3. For information, see [Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP 7.3](#) .

CHAPTER 1. INTEGRATION OPTIONS

Red Hat Single Sign-On (RH-SSO) is a single sign-on solution that you can use to secure your browser applications with your REST web services and Git access.

When you integrate Red Hat Process Automation Manager with RH-SSO, you create an SSO and identity management (IDM) environment for Red Hat Process Automation Manager. The session management feature of RH-SSO enables you to use a single authentication for different Red Hat Process Automation Manager environments on the internet.

The following chapters describe how you can integrate RH-SSO with Red Hat Process Automation Manager:

- **Chapter 4, *Authenticating Business Central through RH-SSO***
To authenticate Red Hat Process Automation Manager through an RH-SSO server, you must secure both the Red Hat Process Automation Manager web client (Business Central) and remote services through RH-SSO. This integration enables you to connect to Red Hat Process Automation Manager through RH-SSO using either Business Central or a remote service consumer.
- **Chapter 5, *Authenticating KIE Server through RH-SSO***
To authenticate KIE Server through an RH-SSO server, you must secure the remote services provided by KIE Server. Doing this enables any remote Red Hat Process Automation Manager service consumer (user or a service) to authenticate through RH-SSO. Note that KIE Server does not have a web interface.
- **Chapter 6, *Authenticating third-party clients through RH-SSO***
If Business Central or KIE Server are using RH-SSO, third-party clients must authenticate themselves using RH-SSO. After authentication, they can consume the remote service endpoints provided by Business Central and KIE Server, such as the REST API or remote file system services.

To facilitate LDAP integration with Red Hat Process Automation Manager, consider using RH-SSO with LDAP. For information, see the "LDAP and Active Directory" chapter of the [Red Hat Single Sign-On Server Administration Guide](#).

CHAPTER 2. INSTALLING AND CONFIGURING RH-SSO

A realm is a security policy domain defined for a web or application server. Security realms are used to restrict access for different application resources. You should create a new realm whether your RH-SSO instance is private or shared with other products. You can keep the master realm as a place for super administrators to create and manage the realms in your system. If you are integrating with an RH-SSO instance that is shared with other product installations to achieve single sign-on with those applications, all of those applications must use the same realm. To create an RH-SSO realm, download, install, and configure RH-SSO 7.4.



NOTE

If Business Central and KIE Server are installed on different servers, complete this procedure on both servers.

Procedure

1. Navigate to the [Software Downloads](#) page in the Red Hat Customer Portal (login required), and select the product and version from the drop-down options:
 - **Product:** Red Hat Single Sign-On
 - **Version:** 7.4
2. Download **Red Hat Single Sign-on 7.4.0 Server(rh-sso-7.4.0.zip)** and apply the latest patches.
3. To install and configure a basic RH-SSO standalone server, follow the instructions in the "Installing and Booting" chapter of the [Red Hat Single Sign On Getting Started Guide](#) . For advanced settings for production environments, see the [Red Hat Single Sign On Server Administration Guide](#).



NOTE

If you want to run both RH-SSO and Red Hat Process Automation Manager servers on the same system, ensure that you avoid port conflicts. by doing one of the following:

- Update the ***RHSSO_HOME/standalone/configuration/standalone-full.xml*** file and set a port offset to 100. For example:

```
<socket-binding-group name="standard-sockets" default-interface="public" port-offset="${jboss.socket.binding.port-offset:100}">
```

- Use an environment variable to run the server:

```
bin/standalone.sh -Djboss.socket.binding.port-offset=100
```

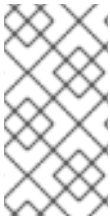
CHAPTER 3. RED HAT PROCESS AUTOMATION MANAGER ROLES AND USERS

To access Business Central or KIE Server, you must create users and assign them appropriate roles before the servers are started.

The Business Central and KIE Server use Java Authentication and Authorization Service (JAAS) login module to authenticate the users. If both Business Central and KIE Server are running on a single instance, then they share the same JAAS subject and security domain. Therefore, a user, who is authenticated for Business Central can also access KIE Server.

However, if Business Central and KIE Server are running on different instances, then the JAAS login module is triggered for both individually. Therefore, a user, who is authenticated for Business Central, needs to be authenticated separately to access the KIE Server (for example, to view or manage process definitions in Business Central). In case, the user is not authenticated on the KIE Server, then 401 error is logged in the log file, displaying **Invalid credentials to load data from remote server. Contact your system administrator.** message in Business Central.

This section describes available Red Hat Process Automation Manager user roles.



NOTE

The **admin**, **analyst**, **developer**, **manager**, **process-admin**, **user**, and **rest-all** roles are reserved for Business Central. The **kie-server** role is reserved for KIE Server. For this reason, the available roles can differ depending on whether Business Central, KIE Server, or both are installed.

- **admin:** Users with the **admin** role are the Business Central administrators. They can manage users and create, clone, and manage the repositories. They have full access to make required changes in the application. Users with the **admin** role have access to all areas within Red Hat Process Automation Manager.
- **analyst:** Users with the **analyst** role have access to all high-level features. They can model and execute their projects. However, these users cannot add contributors to spaces or delete spaces in the **Design → Projects** view. Access to the **Deploy → Execution Servers** view, which is intended for administrators, is not available to users with the **analyst** role. However, the **Deploy** button is available to these users when they access the Library perspective.
- **developer:** Users with the **developer** role have access to almost all features and can manage rules, models, process flows, forms, and dashboards. They can manage the asset repository, they can create, build, and deploy projects, and they can use Red Hat CodeReady Studio to view processes. Only certain administrative functions such as creating and cloning a new repository are hidden from users with the **developer** role.
- **manager:** Users with the **manager** role can view reports. These users are usually interested in statistics about the business processes and their performance, business indicators, and other business-related reporting. A user with this role has access only to process and task reports.
- **process-admin:** Users with the **process-admin** role are business process administrators. They have full access to business processes, business tasks, and execution errors. These users can also view business reports and have access to the Task Inbox list.
- **user:** Users with the **user** role can work on the Task Inbox list, which contains business tasks that are part of currently running processes. Users with this role can view process and task reports and manage processes.

- **rest-all**: Users with the **rest-all** role can access Business Central REST capabilities.
- **kie-server**: Users with the **kie-server** role can access KIE Server (KIE Server) REST capabilities. This role is mandatory for users to have access to **Manage** and **Track** views in Business Central.

3.1. ADDING RED HAT PROCESS AUTOMATION MANAGER USERS

Before you can use RH-SSO to authenticate Business Central or KIE Server, you must add users to the realm that you created. To add new users and assign them a role to access Red Hat Process Automation Manager, complete the following steps:

1. Log in to the RH-SSO Admin Console and open the realm that you want to add a user to.
2. Click the **Users** menu item under the **Manage** section.
An empty user list appears on the **Users** page.
3. Click the **Add User** button on the empty user list to start creating your new user.
The **Add User** page opens.
4. On the **Add User** page, enter the user information and click **Save**.
5. Click the **Credentials** tab and create a password.
6. Assign the new user one of the roles that allows access to Red Hat Process Automation Manager. For example, assign the **admin** role to access Business Central or assign the **kie-server** role to access KIE Server.



NOTE

For projects that deploy from Business Central on OpenShift, create an RH-SSO user called **mavenuser** without any role assigned, then add this user to the **BUSINESS_CENTRAL_MAVEN_USERNAME** and **BUSINESS_CENTRAL_MAVEN_PASSWORD** in your OpenShift template.

7. Define the roles as realm roles in the **Realm Roles** tab under the **Roles** section.
8. Click the **Role Mappings** tab on the **Users** page to assign roles.

CHAPTER 4. AUTHENTICATING BUSINESS CENTRAL THROUGH RH-SSO

This chapter describes how to authenticate Business Central through RH-SSO. It includes the following sections:

- [Section 4.1, "Creating the Business Central client for RH-SSO"](#)
- [Section 4.2, "Installing the RH-SSO client adapter for Business Central"](#)
- [Section 4.3, "Securing Business Central file system services using RH-SSO"](#)

Prerequisites

- Business Central is installed in a Red Hat JBoss EAP 7.3 server, as described in [Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP 7.3](#).
- RH-SSO is installed as described in [Chapter 2, Installing and configuring RH-SSO](#).
- Business Central users have been added to RH-SSO as described in [Section 3.1, "Adding Red Hat Process Automation Manager users"](#).



NOTE

Except for [Section 4.1, "Creating the Business Central client for RH-SSO"](#), this section is intended for standalone installations. If you are integrating RH-SSO and Red Hat Process Automation Manager on Red Hat OpenShift Container Platform, complete only the steps in [Section 4.1, "Creating the Business Central client for RH-SSO"](#) and then deploy the Red Hat Process Automation Manager environment on Red Hat OpenShift Container Platform. For information about deploying Red Hat Process Automation Manager on Red Hat OpenShift Container Platform, see the relevant document on the [Red Hat Customer Portal](#).

4.1. CREATING THE BUSINESS CENTRAL CLIENT FOR RH-SSO

After the RH-SSO server starts, use the RH-SSO Admin Console to create the Business Central client for RH-SSO.

Procedure

1. Enter **`http://localhost:8180/auth/admin`** in a web browser to open the RH-SSO Admin Console and log in using the admin credentials that you created while installing RH-SSO.



NOTE

If you are configuring RH-SSO with Red Hat OpenShift Container Platform, enter the URL that is exposed by the RH-SSO routes. Your OpenShift administrator can provide this URL if necessary.

When you login for the first time, you can set up the initial user on the new user registration form.

2. In the RH-SSO Admin Console, click the **Realm Settings** menu item.

3. On the **Realm Settings** page, click **Add Realm**.
The **Add realm** page opens.
4. On the **Add realm** page, provide a name for the realm and click **Create**.
5. Click the **Clients** menu item and click **Create**.
The **Add Client** page opens.
6. On the **Add Client** page, provide the required information to create a new client for your realm.
For example:
 - **Client ID:** kie
 - **Client protocol:** openid-connect
 - **Root URL:** **`http://localhost:8080/business-central`**



NOTE

If you are configuring RH-SSO with Red Hat OpenShift Container Platform, enter the URL that is exposed by the KIE Server routes. Your OpenShift administrator can provide this URL if necessary.

7. Click **Save** to save your changes.
After you create a new client, its **Access Type** is set to **public** by default. Change it to **confidential**.

The RH-SSO server is now configured with a realm with a client for Business Central applications and running and listening for HTTP connections at **localhost:8180**. This realm provides different users, roles, and sessions for Business Central applications.

4.2. INSTALLING THE RH-SSO CLIENT ADAPTER FOR BUSINESS CENTRAL

After you install RH-SSO, you must install the RH-SSO client adapter for Red Hat JBoss EAP and configure it for Business Central.

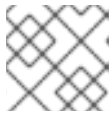
Prerequisites

- Business Central is installed in a Red Hat JBoss EAP 7.3 instance, as described in [as described in *Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP 7.3*](#).
- RH-SSO is installed as described in [Chapter 2, *Installing and configuring RH-SSO*](#).
- A user with the **admin** role has been added to RH-SSO as described in [Section 3.1, “Adding Red Hat Process Automation Manager users”](#).

Procedure

1. Navigate to the [Software Downloads](#) page in the Red Hat Customer Portal (login required), and select the product and version from the drop-down options:
 - **Product:** Red Hat Single Sign-On
 - **Version:** 7.4

2. Download **Red Hat Single Sign-on 7.4 Client Adapter for JBoss EAP** ([rh-sso-7.4.0-eap7-adapter.zip](#) or the latest version).
3. Extract and install the adapter zip file. For installation instructions, see the "JBoss EAP Adapter" section of the [Red Hat Single Sign On Securing Applications and Services Guide](#) .



NOTE

Install the adapter with the **-Dserver.config=standalone-full.xml** property.

4. Navigate to the **EAP_HOME/standalone/configuration** directory in your Red Hat JBoss EAP installation and open the **standalone-full.xml** file in a text editor.
5. Add the system properties listed in the following example to **<system-properties>**:

```
<system-properties>
  <property name="org.jbpm.workbench.kie_server.keycloak" value="true"/>
  <property name="org.uberfire.ext.security.management.api.userManagementServices"
value="KCAdapterUserManagementService"/>
  <property name="org.uberfire.ext.security.management.keycloak.authServer"
value="http://localhost:8180/auth"/>
</system-properties>
```

6. Add the RH-SSO subsystem configuration. For example:

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
  <secure-deployment name="business-central.war">
    <realm>demo</realm>
    <realm-public-
key>MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrVrCuTtArbgaZzL1hvh0xtL5mc
7o0NqPVnYXkLVgcwiC3BjLGw1tGEGoJaXDUSaRilobm53JBhjx33UNv+5z/UMG4kytBWxheNV
KnL6GgqINabMaFiPLPCF8kAgKnsi79NMo+n6KnSY8YeUmec/p2vjO2NjsSAVcWEQMVhJ31L
wIDAQAB</realm-public-key>
    <auth-server-url>http://localhost:8180/auth</auth-server-url>
    <ssl-required>external</ssl-required>
    <enable-basic-auth>true</enable-basic-auth>
    <resource>kie</resource>
    <credential name="secret">759514d0-dbb1-46ba-b7e7-ff76e63c6891</credential>
    <principal-attribute>preferred_username</principal-attribute>
  </secure-deployment>
</subsystem>
```

In this example:

- **secure-deployment name** is the name of your application's WAR file.
- **realm** is the name of the realm that you created for the applications to use.
- **realm-public-key** is the public key of the realm you created. You can find the key in the **Keys** tab in the **Realm settings** page of the realm you created in the RH-SSO Admin Console. If you do not provide a value for **realm-public-key**, the server retrieves it automatically.
- **auth-server-url** is the URL for the RH-SSO authentication server.

- **enable-basic-auth** is the setting to enable basic authentication mechanism, so that the clients can use both token-based and basic authentication approaches to perform the requests.
- **resource** is the name for the client that you created.
- **credential name** is the secret key for the client you created. You can find the key in the **Credentials** tab on the **Clients** page of the RH-SSO Admin Console.
- **principal-attribute** is the login name of the user. If you do not provide this value, your User Id is displayed in the application instead of your user name.



NOTE

The RH-SSO server converts the user names to lower case. Therefore, after integration with RH-SSO, your user name will appear in lower case in Red Hat Process Automation Manager. If you have user names in upper case hard coded in business processes, the application might not be able to identify the upper case user.

7. The Elytron subsystem provides a built-in policy provider based on JACC specification. To enable the JACC manually in the **standalone.xml** or in the file where Elytron is installed, do any of the following tasks:

- To create the policy provider, enter the following commands in the management command-line interface (CLI) of Red Hat JBoss EAP:

```
/subsystem=elytron/policy=jacc:add(jacc-policy={})
/subsystem=undertow/application-security-domain=other:remove
/subsystem=undertow/application-security-domain=other:add(http-authentication-
factory=keycloak-http-authentication,enable-jacc=true)
```

For more information about management CLI of Red Hat JBoss EAP, see the [Management CLI Guide](#).

- Navigate to the **EAP_HOME/standalone/configuration** directory in your Red Hat JBoss EAP installation. Locate the Elytron and undertow subsystem configurations in the **standalone.xml** and **standalone-full.xml** files and enable JACC. For example:

```
<subsystem xmlns="urn:wildfly:elytron:4.0" ...>
.....
  <policy name="jacc"><jacc-policy/></policy>
</subsystem>
```

```
<subsystem xmlns="urn:jboss:domain:undertow:7.0" ...>
.....
  <application-security-domains>
    <application-security-domain name="other" http-authentication-factory="keycloak-http-
authentication" enable-jacc="true"/>
  </application-security-domains>
</subsystem>
```

8. Navigate to **EAP_HOME/bin/** and enter the following command to start the Red Hat JBoss EAP server:



```
./standalone.sh -c standalone-full.xml
```



NOTE

You can also configure the RH-SSO adapter for Business Central by updating your application's WAR file to use the RH-SSO security subsystem. However, Red Hat recommends that you configure the adapter through the RH-SSO subsystem. Doing this updates the Red Hat JBoss EAP configuration instead of applying the configuration on each WAR file.


4.3. SECURING BUSINESS CENTRAL FILE SYSTEM SERVICES USING RH-SSO






To consume other remote services such as file systems (for example, a remote GIT service), you must specify the correct RH-SSO login module.


Procedure


1. Generate a JSON configuration file:
 - a. Navigate to the **RH-SSO Admin Console** located at <http://localhost:8180/auth/admin>.
 - b. Click **Clients**.
 - c. Create a new client with the following settings:
 - Set **Client ID** as **kie-git**.
 - Set **Access Type** as **confidential**.
 - Disable the **Standard Flow Enabled** option.
 - Enable the **Direct Access Grants Enabled** option.


Clients > kie-git


Kie-git 


Settings Credentials Roles Mappers  Scope  Revocation Sessions  Offline Access  Clustering Installation 


Client ID  kie-git


Name 


Description 


Enabled  ON


Consent Required  OFF


Client Protocol  openid-connect


Client Template 


Access Type  confidential


Standard Flow Enabled  OFF

Direct Access Grants Enabled  ON

Service Accounts Enabled  OFF

Root URL 

Base URL 

Admin URL 

- d. Click **Save**.
 - e. Click the **Installation** tab at the top of the client configuration screen and choose **Keycloak OIDC JSON** as a **Format Option**.
 - f. Click **Download**.
2. Move the downloaded JSON file to an accessible directory in the server's file system or add it to the application class path.
 3. Specify the correct RH-SSO login module in the ***EAP_HOME/standalone/configuration/standalone-full.xml*** file. By default, the security domain in Red Hat Process Automation Manager is set to **other**. Replace the default values of the **login-module** in this security domain with the values in the following example:

```
<security-domain name="other" cache-type="default">
  <authentication>
    <login-module code="org.keycloak.adapters.jaas.DirectAccessGrantsLoginModule"
flag="required">
      <module-option name="keycloak-config-file" value="$EAP_HOME/kie-git.json"/>
    </login-module>
  </authentication>
</security-domain>
```

4. The JSON file specified in the **module-option** element contains a client used for securing the remote services. Replace the ***\$EAP_HOME/kie-git.json*** value of the **module-option** element with the absolute path or the class path (***classpath:/EXAMPLE_PATH/kie-git.json***) to this JSON configuration file.

At this point, all users authenticated through the RH-SSO server can clone internal GIT repositories. In the following command, change **USER_NAME** to a RH-SSO user, for example **admin**:

■

```
git clone ssh://USER_NAME@localhost:8001/system
```

CHAPTER 5. AUTHENTICATING KIE SERVER THROUGH RH-SSO

KIE Server provides a REST API for third-party clients. If you integrate KIE Server with RH-SSO, you can delegate third-party client identity management to the RH-SSO server.

After you create a realm client for Red Hat Process Automation Manager and set up the RH-SSO client adapter for Red Hat JBoss EAP, you can set up RH-SSO authentication for KIE Server.

Prerequisites

- RH-SSO is installed as described in [Chapter 2, *Installing and configuring RH-SSO*](#).
- At least one user with the **kie-server** role has been added to RH-SSO as described in [Section 3.1, *Adding Red Hat Process Automation Manager users*](#).
- KIE Server is installed in a Red Hat JBoss EAP 7.3 instance, as described in [Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP 7.3](#).

This chapter contains the following sections:

- [Section 5.1, *Creating the KIE Server client on RH-SSO*](#)
- [Section 5.2, *Installing and configuring KIE Server with the client adapter*](#)
- [Section 5.3, *KIE Server token-based authentication*](#)



NOTE

Except for [Section 5.1, *Creating the KIE Server client on RH-SSO*](#), this section is intended for standalone installations. If you are integrating RH-SSO and Red Hat Process Automation Manager on Red Hat OpenShift Container Platform, complete the steps in [Section 5.1, *Creating the KIE Server client on RH-SSO*](#) and then deploy the Red Hat Process Automation Manager environment on Red Hat OpenShift Container Platform. For information about deploying Red Hat Process Automation Manager on Red Hat OpenShift Container Platform, see the relevant document on the [Red Hat Customer Portal](#).

5.1. CREATING THE KIE SERVER CLIENT ON RH-SSO

Use the RH-SSO Admin Console to create a KIE Server client in an existing realm.

Prerequisites

- KIE Server is installed in a Red Hat JBoss EAP 7.3 server, as described in [Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP 7.3](#).
- RH-SSO is installed as described in [Chapter 2, *Installing and configuring RH-SSO*](#).
- At least one user with the **kie-server** role has been added to RH-SSO as described in [Section 3.1, *Adding Red Hat Process Automation Manager users*](#).

Procedure

1. In the RH-SSO Admin Console, open the security realm that you created in [Chapter 2, Installing and configuring RH-SSO](#).
2. Click **Clients** and click **Create**.
The **Add Client** page opens.
3. On the **Add Client** page, provide the required information to create a KIE Server client for your realm, then click **Save**. For example:
 - **Client ID:** `kie-execution-server`
 - **Root URL:** `http://localhost:8080/kie-server`
 - **Client protocol:** `openid-connect`



NOTE

If you are configuring RH-SSO with Red Hat OpenShift Container Platform, enter the URL that is exposed by the KIE Server routes. Your OpenShift administrator can provide this URL if necessary.

4. The new client **Access Type** is set to **public** by default. Change it to **confidential** and click **Save** again.
5. Navigate to the **Credentials** tab and copy the secret key. The secret key is required to configure the `kie-execution-server` client.

5.2. INSTALLING AND CONFIGURING KIE SERVER WITH THE CLIENT ADAPTER

After you install RH-SSO, you must install the RH-SSO client adapter for Red Hat JBoss EAP and configure it for KIE Server.

Prerequisites

- KIE Server is installed in a Red Hat JBoss EAP 7.3 server, as described in [Installing and configuring Red Hat Process Automation Manager on Red Hat JBoss EAP 7.3](#).
- RH-SSO is installed as described in [Chapter 2, Installing and configuring RH-SSO](#).
- At least one user with the `kie-server` role has been added to RH-SSO as described in [Section 3.1, "Adding Red Hat Process Automation Manager users"](#).



NOTE

If you deployed KIE Server to a different application server than Business Central, install and configure RH-SSO on your second server as well.

Procedure

1. Navigate to the [Software Downloads](#) page in the Red Hat Customer Portal (login required), and select the product and version from the drop-down options:
 - **Product:** Red Hat Single Sign-On

- **Version:** 7.4
2. Download **Red Hat Single Sign-on 7.4 Client Adapter for JBoss EAP** ([rh-sso-7.4.0-eap7-adapter.zip](#) or the latest version).
 3. Extract and install the adapter zip file. For installation instructions, see the "JBoss EAP Adapter" section of the [Red Hat Single Sign On Securing Applications and Services Guide](#) .
 4. Go to **EAP_HOME/standalone/configuration** and open the **standalone-full.xml** file.
 5. Delete the **<single-sign-on/>** element from both of the files.
 6. Navigate to **EAP_HOME/standalone/configuration** directory in your Red Hat JBoss EAP installation and edit the **standalone-full.xml** file to add the RH-SSO subsystem configuration. For example:
 7. Navigate to **EAP_HOME/standalone/configuration** in your Red Hat JBoss EAP installation and edit the **standalone-full.xml** file to add the RH-SSO subsystem configuration. For example:

```

<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
  <secure-deployment name="kie-server.war">
    <realm>demo</realm>
    <realm-public-
key>MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrVrCuTtArbgaZzL1hvh0xtL5mc
7o0NqPVnYXkLVgcwiC3BjLGw1tGEGoJaXDuSaRIlobm53JBhjx33UNv+5z/UMG4kytBWxheNV
KnL6GgqINabMaFiPLPCF8kAgKnsi79NMo+n6KnSY8YeUmec/p2vjO2NjsSAVcWEQMvhJ31L
wIDAQAB</realm-public-key>
    <auth-server-url>http://localhost:8180/auth</auth-server-url>
    <ssl-required>external</ssl-required>
    <resource>kie-execution-server</resource>
    <enable-basic-auth>true</enable-basic-auth>
    <credential name="secret">03c2b267-7f64-4647-8566-572be673f5fa</credential>
    <principal-attribute>preferred_username</principal-attribute>
  </secure-deployment>
</subsystem>

<system-properties>
  <property name="org.kie.server.sync.deploy" value="false"/>
</system-properties>

```

In this example:

- **secure-deployment name** is the name of your application WAR file.
- **realm** is the name of the realm that you created for the applications to use.
- **realm-public-key** is the public key of the realm you created. You can find the key in the **Keys** tab in the **Realm settings** page of the realm you created in the RH-SSO Admin Console. If you do not provide a value for this public key, the server retrieves it automatically.
- **auth-server-url** is the URL for the RH-SSO authentication server.
- **resource** is the name for the server client that you created.

- **enable-basic-auth** is the setting to enable basic authentication mechanism, so that the clients can use both token-based and basic authentication approaches to perform the requests.
 - **credential name** is the secret key of the server client you created. You can find the key in the **Credentials** tab on the **Clients** page of the RH-SSO Admin Console.
 - **principal-attribute** is the login name of the user. If you do not provide this value, your User Id is displayed in the application instead of your user name.
8. Save your configuration changes.
 9. Use the following command to restart the Red Hat JBoss EAP server and run KIE Server.

```
EXEC_SERVER_HOME/bin/standalone.sh -c standalone-full.xml -Dorg.kie.server.id=<ID> -
Dorg.kie.server.user=<USER> -Dorg.kie.server.pwd=<PWD> -Dorg.kie.server.location=
<LOCATION_URL> -Dorg.kie.server.controller=<CONTROLLER_URL> -
Dorg.kie.server.controller.user=<CONTROLLER_USER> -Dorg.kie.server.controller.pwd=
<CONTROLLER_PASSWORD>
```

For example:

```
EXEC_SERVER_HOME/bin/standalone.sh -c standalone-full.xml -
Dorg.kie.server.id=kieserver1 -Dorg.kie.server.user=kieserver -
Dorg.kie.server.pwd=password -Dorg.kie.server.location=http://localhost:8080/kie-
server/services/rest/server -Dorg.kie.server.controller=http://localhost:8080/business-
central/rest/controller -Dorg.kie.server.controller.user=kiecontroller -
Dorg.kie.server.controller.pwd=password
```

10. When KIE Server is running, enter the following command to check the server status, where **<KIE_SERVER_USER>** is a user with the **kie-server** role and **<PASSWORD>** is the password for that user:

```
curl http://<KIE_SERVER_USER>:<PASSWORD>@localhost:8080/kie-
server/services/rest/server/
```

5.3. KIE SERVER TOKEN-BASED AUTHENTICATION

You can also use token-based authentication for communication between Red Hat Process Automation Manager and KIE Server. You can use the complete token as a system property of your application server, instead of the user name and password, for your applications. However, you must ensure that the token will not expire while the applications are interacting because the token is not automatically refreshed. To get the token, see [Section 6.2, "Token-based authentication"](#).

Procedure

1. To configure Business Central to manage KIE Server using tokens:
 - a. Set the **org.kie.server.token** property.
 - b. Make sure that the **org.kie.server.user** and **org.kie.server.pwd** properties are not set. Red Hat Process Automation Manager will then use the **Authorization: Bearer \$TOKEN** authentication method.
2. To use the REST API using the token-based authentication:

- a. Set the **org.kie.server.controller.token** property.
- b. Make sure that the **org.kie.server.controller.user** and **org.kie.server.controller.pwd** properties are not set.



NOTE

Because KIE Server is unable to refresh the token, use a high-lifespan token. A token's lifespan must not exceed January 19 2038. Check with your security best practices to see whether this is a suitable solution for your environment.

CHAPTER 6. AUTHENTICATING THIRD-PARTY CLIENTS THROUGH RH-SSO

To use the different remote services provided by Business Central or by KIE Server, your client, such as curl, wget, web browser, or a custom REST client, must authenticate through the RH-SSO server and have a valid token to perform the requests. To use the remote services, the authenticated user must have the following roles:

- **rest-all** for using Business Central remote services.
- **kie-server** for using the KIE Server remote services.

Use the RH-SSO Admin Console to create these roles and assign them to the users that will consume the remote services.

Your client can authenticate through RH-SSO using one of these options:

- Basic authentication, if it is supported by the client
- Token-based authentication

6.1. BASIC AUTHENTICATION

If you enabled basic authentication in the RH-SSO client adapter configuration for both Business Central and KIE Server, you can avoid the token grant and refresh calls and call the services as shown in the following examples:

- For web based remote repositories endpoint:

```
curl http://admin:password@localhost:8080/business-central/rest/repositories
```

- For KIE Server:

```
curl http://admin:password@localhost:8080/kie-server/services/rest/server/
```

6.2. TOKEN-BASED AUTHENTICATION

If you want a more secure option of authentication, you can consume the remote services from both Business Central and KIE Server by using a granted token provided by RH-SSO.

Procedure

1. In the RH-SSO Admin Console, click the **Clients** menu item and click **Create** to create a new client.
The **Add Client** page opens.
2. On the **Add Client** page, provide the required information to create a new client for your realm.
For example:
 - **Client ID:** kie-remote
 - **Client protocol:** openid-connect
3. Click **Save** to save your changes.

4. Change the token settings in **Realm Settings**:
 - a. In the RH-SSO Admin Console, click the **Realm Settings** menu item.
 - b. Click the **Tokens** tab.
 - c. Change the value for **Access Token Lifespan** to **15** minutes.
This gives you enough time to get a token and invoke the service before it expires.
 - d. Click **Save** to save your changes.
5. After a public client for your remote clients is created, you can now obtain the token by making an HTTP request to the RH-SSO server's token endpoint using:

```
RESULT=`curl --data "grant_type=password&client_id=kie-remote&username=admin&password=password" http://localhost:8180/auth/realms/demo/protocol/openid-connect/token`
```

The user in this command is a Business Central RH-SSO user. For more information, see [Section 3.1, "Adding Red Hat Process Automation Manager users"](#).

6. To view the token obtained from the RH-SSO server, use the following command:

```
TOKEN=`echo $RESULT | sed 's/.*access_token:"//g' | sed 's/".*//g`
```

You can now use this token to authorize the remote calls. For example, if you want to check the internal Red Hat Process Automation Manager repositories, use the token as shown below:

```
curl -H "Authorization: bearer $TOKEN" http://localhost:8080/business-central/rest/repositories
```

APPENDIX A. VERSIONING INFORMATION

Documentation last updated on Wednesday, July 29, 2020.