



Red Hat Single Sign-On 7.4

スタートガイド

Red Hat Single Sign-On 7.4 向け

Red Hat Single Sign-On 7.4 スタートガイド

Red Hat Single Sign-On 7.4 向け

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

法律上の通知

Copyright © 2021 | You need to change the HOLDER entity in the en-US/Getting_Started_Guide.ent file |.

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.

概要

本ガイドは、実稼働環境で使用する前に Red Hat Single Sign-On を使用して評価するのに役立ちます。これには、スタンドアロンモードで Red Hat Single Sign-On サーバーをインストールし、ユーザーおよびアプリケーションを管理するためのアカウントおよびレルムを作成し、JBoss EAP サーバーアプリケーションのセキュリティーを保護する手順が含まれます。

目次

多様性を受け入れるオープンソースの強化	3
第1章 RED HAT SINGLE SIGN-ON のサンプルインスタンスのインストール	4
1.1. RED HAT SINGLE SIGN-ON サーバーのインストール	4
1.2. RED HAT SINGLE SIGN-ON サーバーの起動	4
1.3. 管理アカウントの作成	5
1.4. 管理コンソールへのログイン	6
第2章 レルムおよびユーザーの作成	8
2.1. レルムとユーザー	8
2.2. レルムの作成	8
2.3. ユーザーの作成	9
2.4. アカウントコンソールへのログイン	11
第3章 サンプルアプリケーションのセキュリティー保護	13
3.1. RED HAT SINGLE SIGN-ON が使用するポートの調整	13
3.2. JBOSS EAP クライアントアダプターのインストール	14
3.3. JBOSS EAP アプリケーションの登録	15
3.4. JBOSS EAP インスタンスの変更	17
3.5. アプリケーションをセキュアにするためのサンプルコードのインストール	17

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、[弊社](#) の CTO、Chris Wright の [メッセージ](#) を参照してください。

第1章 RED HAT SINGLE SIGN-ON のサンプルインスタンスのインストール

本セクションでは、スタンドアロンモードで Red Hat Single Sign-On サーバーをインストールして起動し、初期管理ユーザーを設定し、Red Hat Single Sign-On 管理コンソールにログインする方法を説明します。

関連情報

このインストールは、Red Hat Single Sign-On の使用を目的としています。実稼働環境と、すべての製品機能の完全な詳細については、[Red Hat Single Sign-On](#) ドキュメントの他のガイドを参照してください。

1.1. RED HAT SINGLE SIGN-ON サーバーのインストール

Red Hat Single Sign-On のインスタンス例では、この手順ではスタンドアロンモードでインストールが関係します。サーバーのダウンロード ZIP ファイルには、Red Hat Single Sign-On サーバーを実行するためのスクリプトとバイナリーが含まれています。サーバーを Linux または Windows にインストールできます。

手順

1. [Red Hat カスタマーポータル](#) に移動します。
2. Red Hat Single Sign-On サーバー (**rh-sso-7.4.0.zip**) をダウンロードします。
3. 選択したディレクトリーにファイルを配置します。
4. unzip などの適切な **unzip** ユーティリティーまたは Expand-Archive を使用して ZIP ファイルを展開します。

Linux/Unix

```
$ unzip rhssso-7.4.0.zip
```

Windows

```
> Expand-Archive -Path 'C:\Downloads\rhssso-7.4.0.zip' -DestinationPath 'C:\Downloads'
```

1.2. RED HAT SINGLE SIGN-ON サーバーの起動

インストールしたシステムでサーバーを起動します。

前提条件

- Red Hat Single Sign-On サーバーのインストール時にエラーはありません。

手順

1. サーバーディストリビューションの **bin** ディレクトリーに移動します。
2. ブートスクリプト **standalone** を実行します。

Linux/Unix

```
$ cd bin  
$ ./standalone.sh
```

Windows

```
> ...\bin\standalone.bat
```

1.3. 管理アカウントの作成

Red Hat Single Sign-On を使用する前に、Red Hat Single Sign-On 管理コンソールにログインするために使用する管理者アカウントを作成する必要があります。

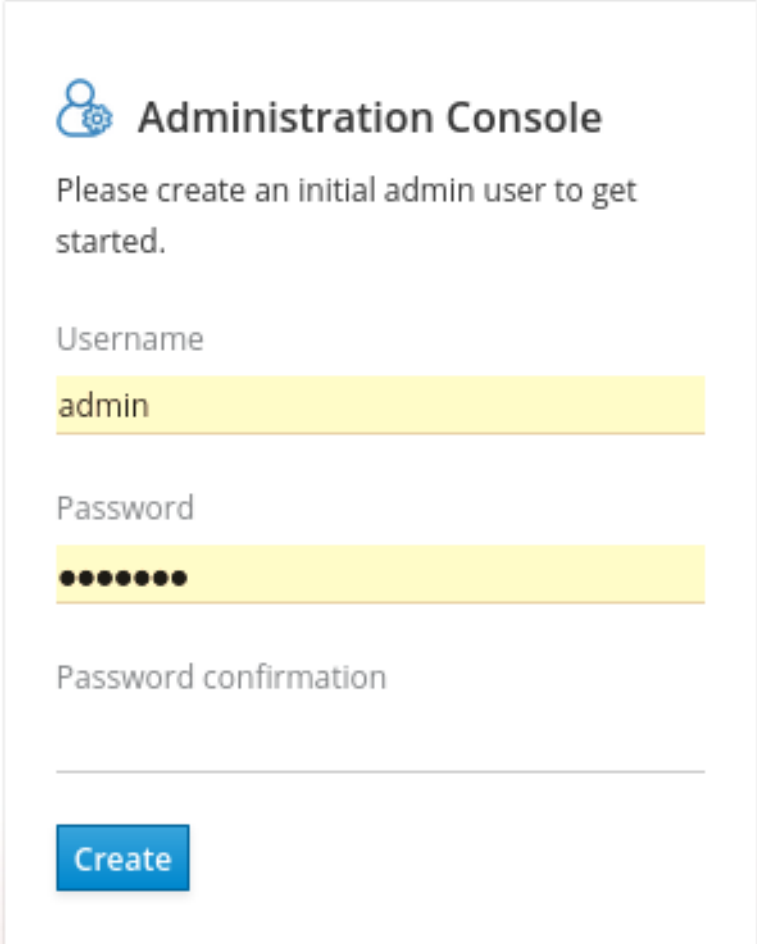
前提条件


- Red Hat Single Sign-On サーバーを起動した場合、エラーはありません。

手順

1. Web ブラウザーで <http://localhost:8080/auth> を開きます。
Welcome ページが開き、サーバーが実行していることを確認します。

Welcome ページ



 **Administration Console**

Please create an initial admin user to get started.

Username
admin

Password
●●●●●●

Password confirmation

Create

2. ユーザー名とパスワードを入力して、最初の管理ユーザーを作成します。

1.4. 管理コンソールへのログイン

初期管理者アカウントを作成したら、管理コンソールにログインすることができます。このコンソールで、Red Hat Single Sign-On が保護されるようにユーザーを追加し、アプリケーションを登録します。

前提条件

- 管理コンソールの管理者アカウントがある。

手順

1. **Welcome** ページの **Administration Console** リンクをクリックします。または、<http://localhost:8080/auth/admin/> (コンソール URL) に直接アクセスします。



注記

管理コンソールは通常、Red Hat Single Sign-On ドキュメントの管理コンソールと呼ばれます。

2. **Welcome** ページで作成したユーザー名とパスワードを入力して、**管理コンソール** を開きます。

管理コンソールのログイン画面

Username or email

admin

Password

●●●●●●

Remember me

Log In

管理コンソールの初期画面が表示されます。

管理コンソール

The screenshot shows the 'Master' realm configuration page in the Red Hat Single Sign-On administration console. The left sidebar contains a navigation menu with 'Realm Settings' selected. The main content area shows the 'General' tab with the following configuration:

- Name:** master
- Display name:** master
- HTML Display name:** master realm
- Frontend URL:** (empty)
- Enabled:** ON
- User-Managed Access:** OFF
- Endpoints:** OpenID Endpoint Configuration, SAML 2.0 Identity Provider Metadata

Buttons for 'Save' and 'Cancel' are located at the bottom of the form.

次のステップ

管理コンソールにログインできるようになったので、管理者がユーザーを作成できるレルムの作成を開始でき、アプリケーションへのアクセス権限を付与できます。詳細は、「[レルムおよびユーザーの作成](#)」を参照してください。

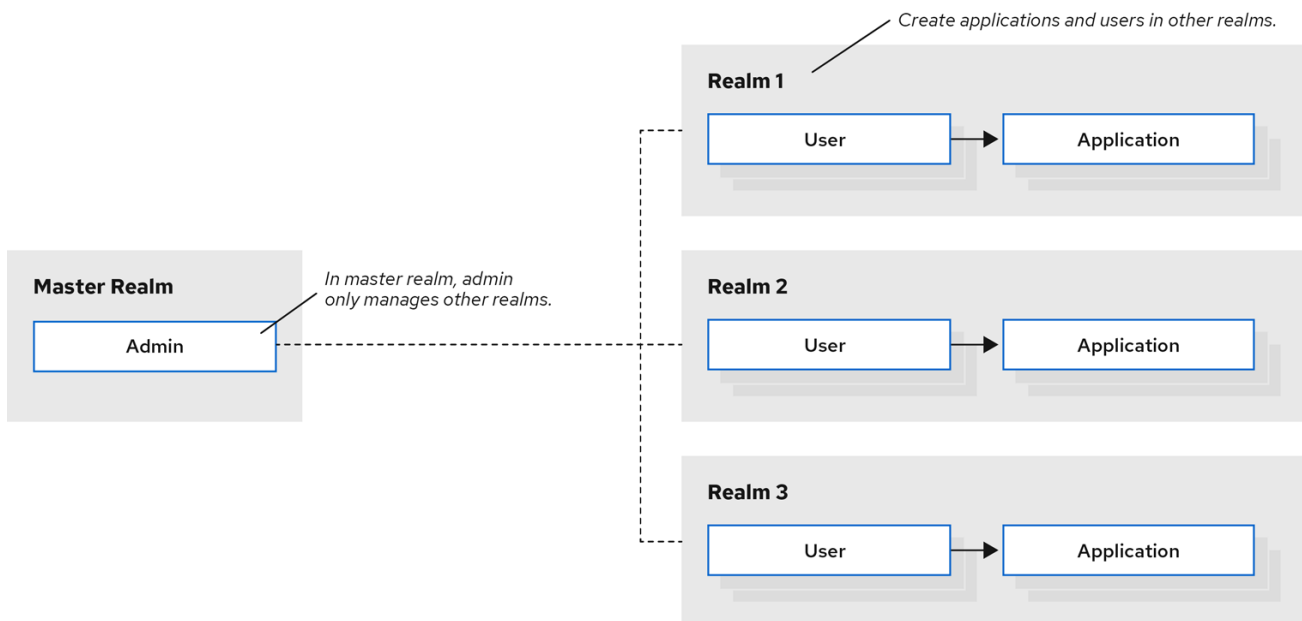
第2章 レalmおよびユーザーの作成

Red Hat Single Sign-On 管理コンソールの最初の使い方は、レalmを作成し、そのレalmでユーザーを作成します。そのユーザーを使用して、新しいレalmにログインし、すべてのユーザーがアクセス可能な組み込みアカウントコンソールにアクセスします。

2.1. レalmとユーザー

管理コンソールにログインすると、レalmで作業します。このレalmは、オブジェクトを管理するスペースになります。以下のレalmには2つのタイプがあります。

- **Master レalm** - このレalmは、Red Hat Single Sign-On の初回起動時に作成されました。これには、初回ログイン時に作成した管理者アカウントが含まれます。このレalmを使用して他のレalmのみを作成します。
- **他のレalm** - これらのレalmは、マスターレalmで管理者により作成されます。これらのレalmでは、管理者はユーザーとアプリケーションを作成します。アプリケーションはユーザーが所有します。



RHSSO_44_0919

2.2. レalmの作成

マスターレalmの管理者として、管理者がユーザーおよびアプリケーションを作成するレalmを作成します。

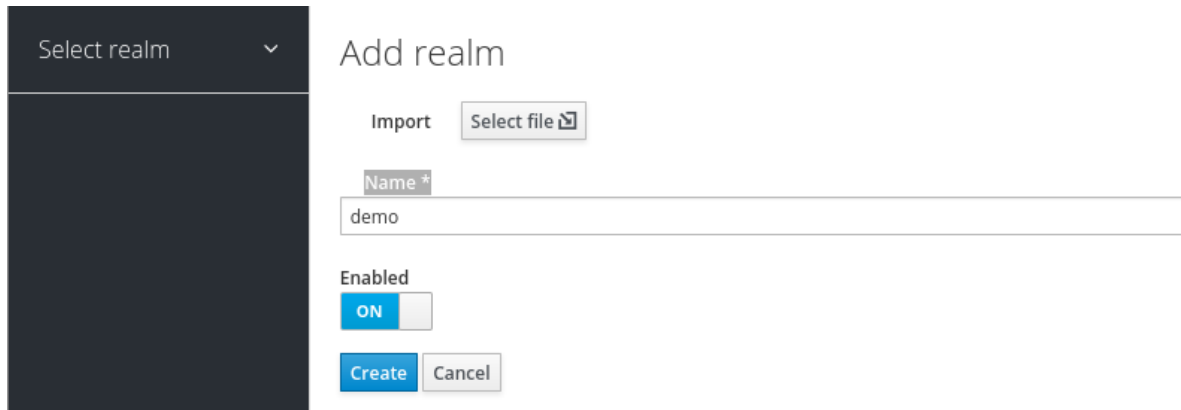
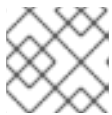
前提条件

- Red Hat Single Sign-On がインストールされている。
- 管理コンソールの初期管理者アカウントがある。

手順

1. <http://localhost:8080/auth/admin/> にアクセスし、管理者アカウントを使用して Red Hat Single Sign-On 管理コンソールにログインします。
2. マスターメニューから、**Add Realm** をクリックします。マスターレalmにログインすると、このメニューには他のすべてのレalmが一覧表示されます。
3. **Name** フィールドに **demo** と入力します。

新しいレalm

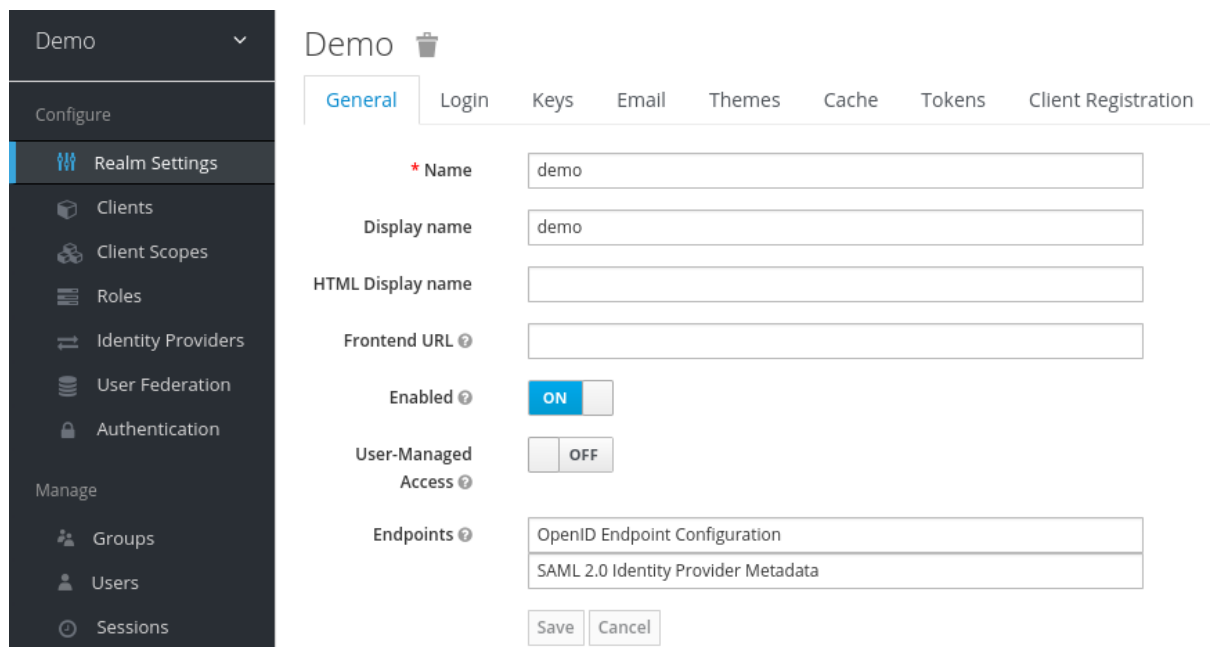



注記

レalm名は大文字と小文字を区別するため、使用するケースを書き留めます。

4. **Create** をクリックします。
レalmを **demo** に設定し、メインの管理コンソールページが開きます。

demo レalm



5. **Select realm** ドロップダウンリストでエントリをクリックして、**master** レalmと、作成したレalmの管理を切り替えます。

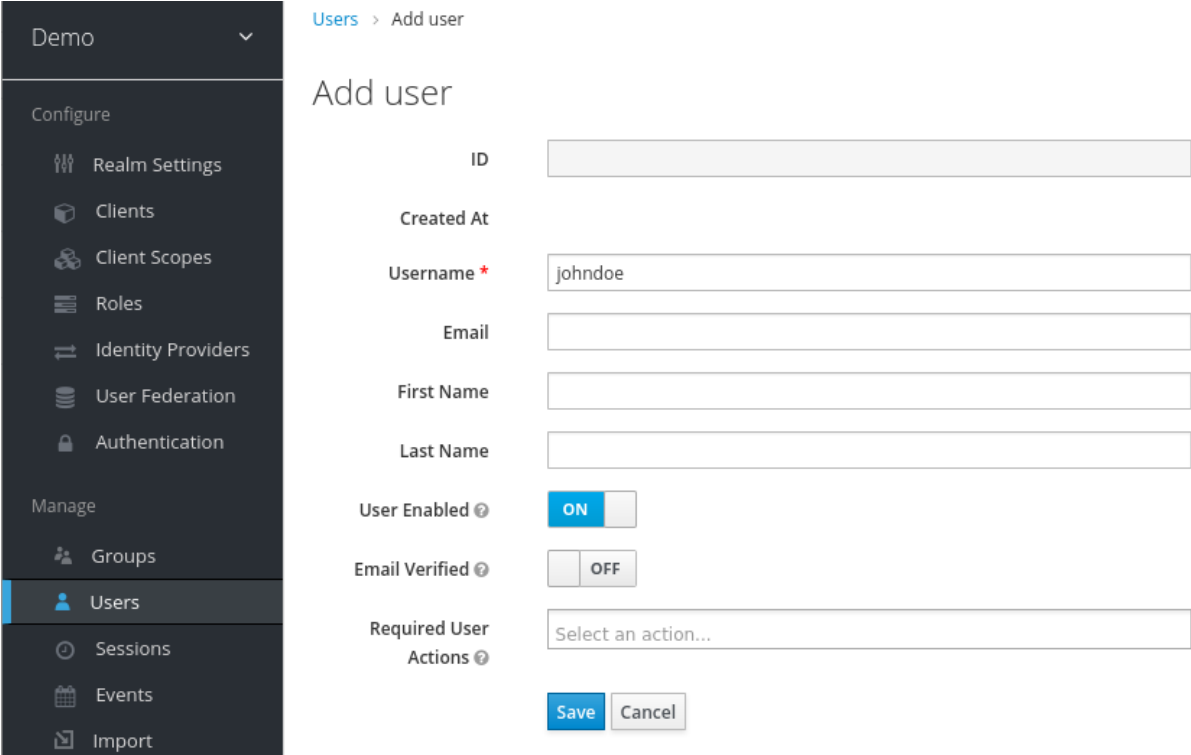
2.3. ユーザーの作成

demo レalmでは、新規ユーザーと、その新しいユーザーの一時パスワードを作成します。

手順

1. メニューから **Users** をクリックしてユーザー一覧ページを開きます。
2. 空のユーザー一覧の右側で、**Add User** をクリックして Add user ページを開きます。
3. **Username** フィールドに名前を入力します。
これは唯一の必須フィールドです。

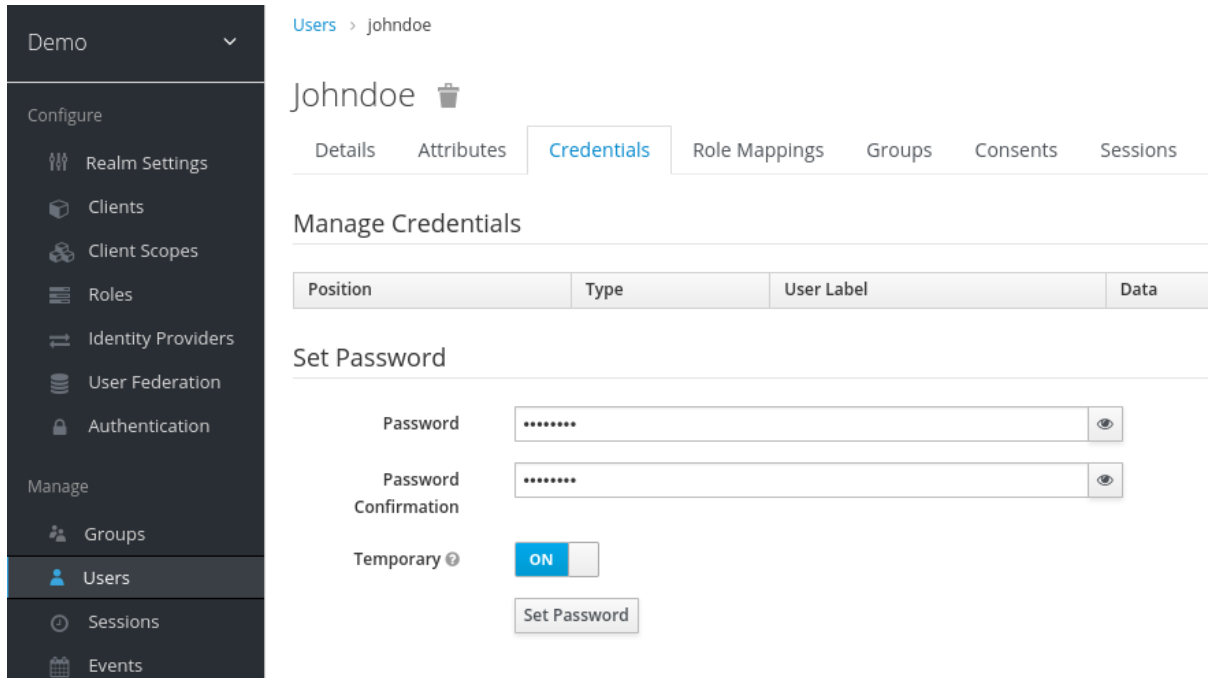
Add user ページ




The screenshot displays the 'Add user' page. On the left is a dark sidebar menu with 'Users' highlighted. The main content area shows the 'Add user' form. The 'Username' field is pre-filled with 'johndoe'. The 'User Enabled' toggle is set to 'ON', and 'Email Verified' is set to 'OFF'. The 'Required User Actions' dropdown is set to 'Select an action...'. 'Save' and 'Cancel' buttons are located at the bottom of the form.

4. **Email Verified** スイッチを **On** に切り替え、**Save** をクリックします。
新規ユーザーの管理ページが開きます。
5. **Credentials** タブをクリックして、新規ユーザーの一時パスワードを設定します。
6. 新規パスワードを入力して確認します。
7. **Set Password** をクリックして、指定した新しいパスワードにユーザーパスワードを設定します。

認証情報ページの管理



Users > johndoe

Johndoe 

Details Attributes **Credentials** Role Mappings Groups Consents Sessions

Manage Credentials

Position	Type	User Label	Data
----------	------	------------	------

Set Password

Password

Password Confirmation

Temporary



注記

このパスワードは一時的なもので、ユーザーは初回ログイン時にパスワードを変更する必要があります。永続的なパスワードを作成する場合は、**Temporary** スイッチを **Off** に切り替え、**Set Password** をクリックします。

2.4. アカウントコンソールへのログイン

レルムのすべてのユーザーは、アカウントコンソールにアクセスできます。このコンソールを使用してプロフィール情報を更新し、認証情報を変更します。作成したレルムのそのユーザーでログインをテストすることができます。

手順

1. ユーザーメニューを開き、**Sign Out** を選択して管理コンソールからログアウトします。
2. <http://localhost:8080/auth/realms/demo/account> にアクセスし、作成したユーザーとして **demo** レルムにログインします。
3. 新しいパスワードを入力するように求められたら、記憶できるパスワードを入力します。

パスワードの更新



You need to change your password to activate your account.

New Password

Confirm password

Submit

このユーザーにアカウントコンソールが開きます。

アカウントコンソール

- Account >
- Password
- Authenticator
- Sessions
- Applications

Edit Account

* Required fields

Username	<input type="text" value="johndoe"/>
Email *	<input type="text" value="johndoe@virgernetworks.com"/>
First name *	<input type="text" value="John"/>
Last name *	<input type="text" value="Doe"/>

Cancel

Save

- このページを使用してテストする値で必須フィールドに入力します。

次のステップ

これで、JBoss EAP で実行されるサンプルアプリケーションをセキュアにする最終手順ができました。「[サンプルアプリケーションのセキュリティー保護](#)」を参照してください。

第3章 サンプルアプリケーションのセキュリティー保護

これで、管理者アカウント、レルム、およびユーザーが、Red Hat Single Sign-On を使用してサンプル JBoss EAP サブレットアプリケーションをセキュアにできるようになりました。JBoss EAP クライアントアダプターをインストールし、管理コンソールでアプリケーションを登録し、JBoss EAP インスタンスを変更して Red Hat Single Sign-On と連携し、一部のサンプルコードと Red Hat Single Sign-On を使用してアプリケーションのセキュリティーを保護します。

前提条件

- JBoss EAP とポートが競合しないように、Red Hat Single Sign-On によって使用されるポートを調整する必要があります。

3.1. RED HAT SINGLE SIGN-ON が使用するポートの調整

本書の手順は、Red Hat Single Sign-On サーバーと同じマシン上で JBoss EAP の実行に適用されます。このような場合、JBoss EAP は Red Hat Single Sign-On とバンドルされていますが、JBoss EAP をアプリケーションコンテナとして使用することはできません。サブレットアプリケーションに対して別の JBoss EAP インスタンスを実行する必要があります。

ポートの競合を回避するには、Red Hat Single Sign-On および JBoss EAP を実行するには、異なるポートが必要です。

前提条件

- 管理コンソールの管理者アカウントがある。
- デモレルムが作成されている。
- デモレルムでユーザーが作成されている。

手順

1. [Red Hat カスタマーポータル](#) から JBoss EAP 7.3 をダウンロードします。
2. ダウンロードした JBoss EAP を展開します。

```
$ unzip <filename>.zip
```

3. Red Hat Single Sign-On の root ディレクトリーに移動します。
4. **jboss.socket.binding.port-offset** システムプロパティーの値を指定して、Red Hat Single Sign-On サーバーを起動します。この値は、Red Hat Single Sign-On サーバーにより開かれる全ポートのベース値に追加されます。この例では、100 が値です。

Linux/Unix

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

Windows

```
> ...\bin\standalone.bat -Djboss.socket.binding.port-offset=100
```

Windows Powershell

```
> ...\bin\standalone.bat -D"jboss.socket.binding.port-offset=100"
```

- Red Hat Single Sign-On サーバーが稼働していることを確認します。<http://localhost:8180/auth/admin/> にアクセスします。管理コンソールを開くと、JBoss EAP が Red Hat Single Sign-On と動作できるようにするクライアントアダプターをインストールすることができます。

3.2. JBOSS EAP クライアントアダプターのインストール

JBoss EAP と Red Hat Single Sign-On を同じマシンにインストールする場合、JBoss EAP ではいくつかの変更が必要になります。この変更を加えるには、Red Hat Single Sign-On クライアントアダプターをインストールします。

前提条件

- JBoss EAP がインストールされている。
- このファイルをカスタマイズする場合は `../standalone/configuration/standalone.xml` ファイルのバックアップを作成します。

手順

- [Red Hat カスタマーポータル](#) から、**Client Adapter for EAP 7**をダウンロードします。
- JBoss EAP のルートディレクトリーに移動します。
- ダウンロードしたクライアントアダプターをこのディレクトリーに展開します。たとえば、以下のようになります。

```
$ unzip <filename>.zip
```

- bin ディレクトリーに移動します。

```
$ cd bin
```

- プラットフォームに適したスクリプトを実行します。



注記

file not found エラーが発生した場合は、前の手順で **unzip** を使用していたことを確認してください。この抽出方法は、正しい場所にファイルをインストールします。

Linux/Unix

```
$ ./jboss-cli.sh --file=adapter-elytron-install-offline.cli
```

Windows

```
> jboss-cli.bat --file=adapter-elytron-install-offline.cli
```



注記

このスクリプトを使用すると、`.../standalone/configuration/standalone.xml` ファイルに必要な編集が行われます。

- アプリケーションサーバーを起動します。

Linux/Unix

```
$ ./standalone.sh
```

Windows

```
> ...\standalone.bat
```

3.3. JBOSS EAP アプリケーションの登録

Red Hat Single Sign-On 管理コンソールでクライアントを定義し、登録できるようになりました。

前提条件

- JBoss EAP と連携するクライアントアダプターがインストールされている。

手順

- 管理者アカウントで管理コンソール (<http://localhost:8180/auth/admin/>) にログインします。
- 左上のドロップダウンリストで、**Demo** レalmを選択します。
- 左側のメニューで **Clients** をクリックし、クライアントページを開きます。

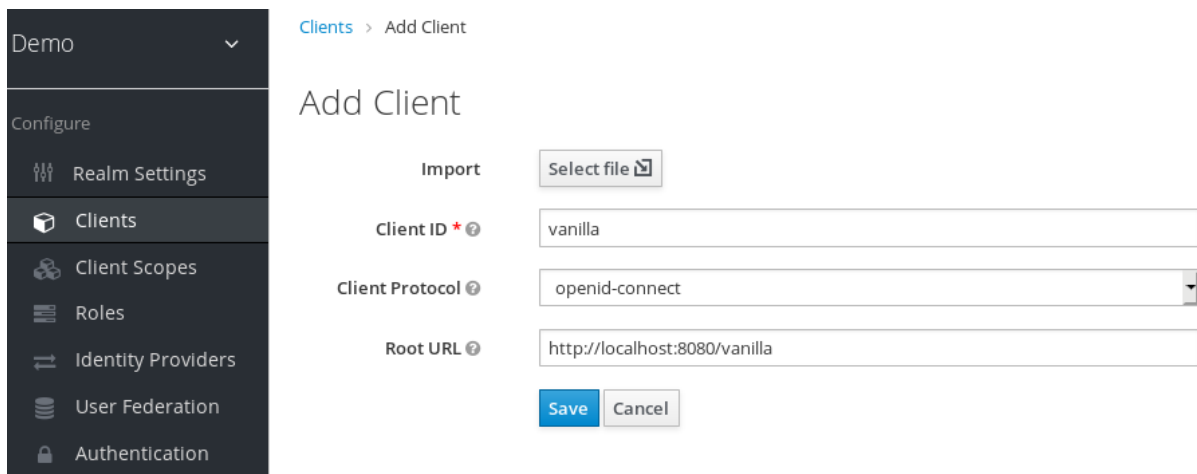
クライアント

The screenshot shows the 'Clients' page in the Red Hat Single Sign-On management console. The left sidebar is set to 'Demo' and 'Clients' is selected. The main content area shows a table of existing clients with columns for Client ID, Enabled, Base URL, and Actions (Edit, Export, Delete). A 'Create' button is visible in the top right corner of the table area.

Client ID	Enabled	Base URL	Actions		
account	True	http://localhost:8080/auth/realms/demo/account/	Edit	Export	Delete
account-console	True	http://localhost:8080/auth/realms/demo/account/	Edit	Export	Delete
admin-cli	True	Not defined	Edit	Export	Delete
broker	True	Not defined	Edit	Export	Delete
realm-management	True	Not defined	Edit	Export	Delete
security-admin-console	True	http://localhost:8080/auth/admin/demo/console/	Edit	Export	Delete

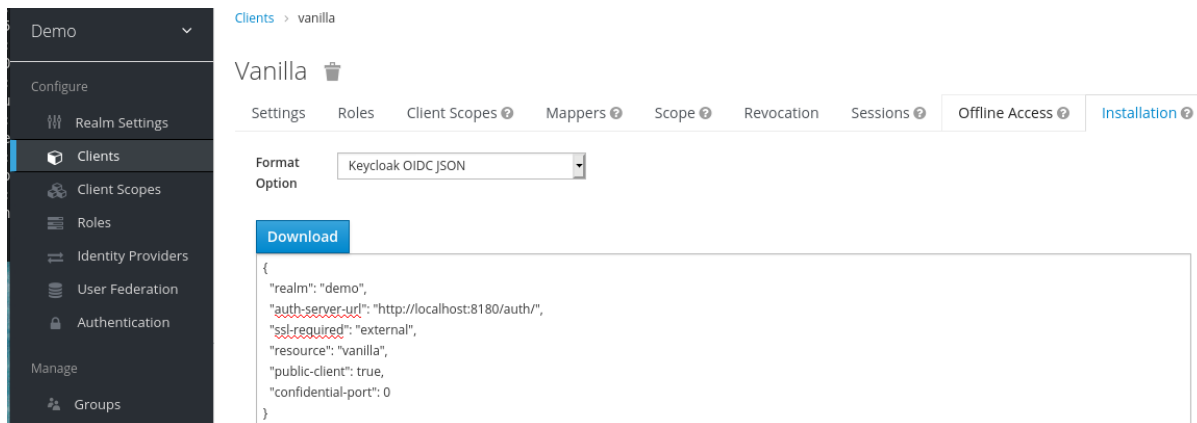
- 右側の **Create** をクリックします。
- クライアントの追加ダイアログで、以下のようにフィールドを完了して、**vanilla** という名前のクライアントを作成します。

クライアントの追加



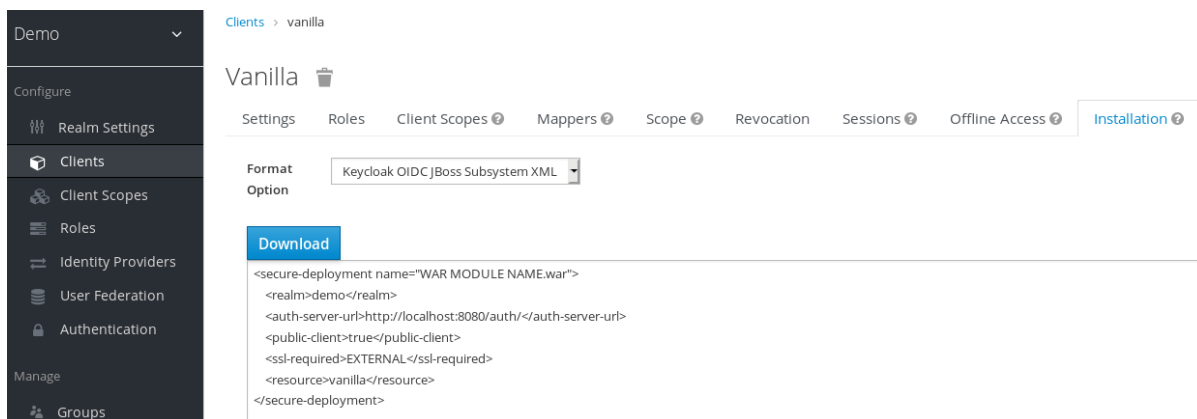
6. **Save** をクリックします。
7. 表示される **Vanilla** クライアントページで、**Installation** タブをクリックします。
8. **Keycloak OIDC JSON** を選択して、後で必要なファイルを生成します。

Keycloak.json ファイル



9. **Download** をクリックして、後で確認できる場所に **Keycloak.json** を保存します。
10. **Keycloak OIDC JBoss Subsystem XML** を選択して XML テンプレートを生成します。

テンプレート XML



11. **Download** をクリックして、次の手順で使用するコピーを保存します。これには JBoss EAP の設定が含まれます。

3.4. JBOSS EAP インスタンスの変更

JBoss EAP サブレットアプリケーションは、Red Hat Single Sign-On によってセキュア化される前に追加の設定を必要とします。

前提条件

- demo レルムに、vanilla という名前のクライアントが作成されている。
- このクライアントのテンプレート XML ファイルを保存している。

手順

1. JBoss EAP ルートディレクトリーの **standalone/configuration** ディレクトリーに移動します。
2. **standalone.xml** ファイルを開き、以下のテキストを検索します。

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1"/>
```

3. 次に示すように、XML エントリーを自己終了から開始タグと終了タグのペアを使用するように変更します。

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
</subsystem>
```

4. 以下の例のように、XML テンプレートの内容を **<subsystem>** 要素内に貼り付けます。

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
  <secure-deployment name="WAR MODULE NAME.war">
    <realm>demo</realm>
    <auth-server-url>http://localhost:8180/auth</auth-server-url>
    <public-client>true</public-client>
    <ssl-required>EXTERNAL</ssl-required>
    <resource>vanilla</resource>
  </secure-deployment>
</subsystem>
```

5. **WAR MODULE NAME.war** を **vanilla.war** に変更します。

```
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
  <secure-deployment name="vanilla.war">
    ...
  </subsystem>
```

6. アプリケーションサーバーを再起動します。

3.5. アプリケーションをセキュアにするためのサンプルコードのインストール

最後の手順は、<https://github.com/redhat-developer/redhat-ssso-quickstarts> リポジトリから一部のサンプルコードをインストールして、このアプリケーションのセキュリティーを保護する方法を説明します。クイックスタートは、最新の Red Hat Single Sign-On リリースと連携します。

サンプルコードは **app-profile-jee-vanilla** クイックスタートです。これは、WAR を変更せずに Basic 認証でセキュア化された JavaEE アプリケーションを変更する方法を実証します。Red Hat Single Sign-On クライアントアダプターサブシステムは認証方法を変更し、設定を挿入します。

前提条件

以下がマシンにインストールされ、PATH で利用できる。

- Java JDK 8
- Apache Maven 3.1.1 以降
- Git

keycloak.json ファイルがある。

手順

1. JBoss EAP アプリケーションサーバーが起動していることを確認します。
2. 以下のコマンドを使用して、コードをダウンロードし、ディレクトリーを変更します。

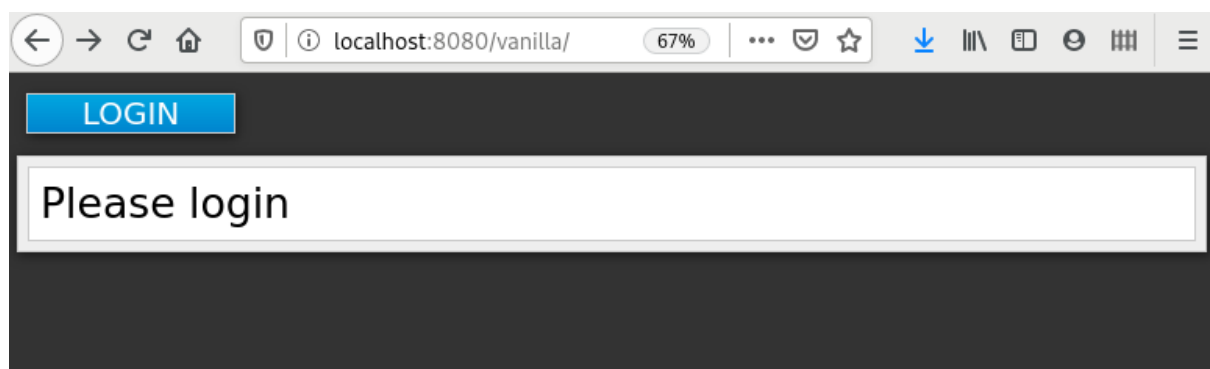
```
$ git clone https://github.com/redhat-developer/redhat-ssso-quickstarts
$ cd redhat-ssso-quickstarts/app-profile-jee-vanilla/config
```

3. **keycloak.json** ファイルを現在のディレクトリーにコピーします。
4. **app-profile-jee-vanilla** ディレクトリーに移動します。
5. 以下のコマンドを使用してコードをインストールします。

```
$ mvn clean wildfly:deploy
```

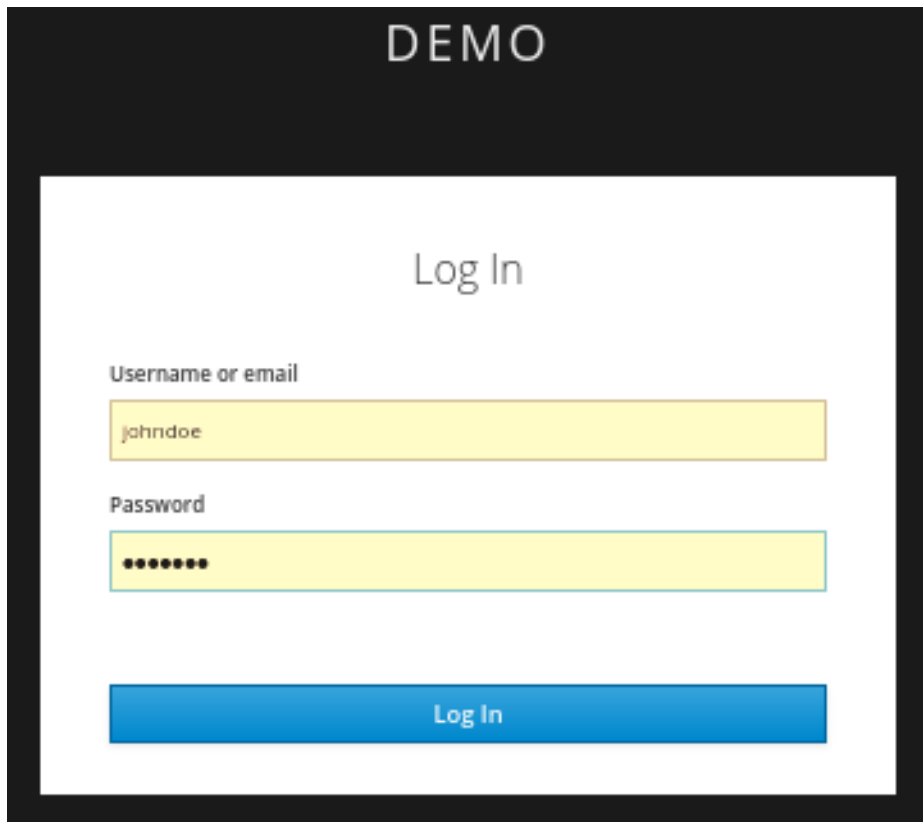
6. アプリケーションのインストールが正常に完了したことを確認します。ログインページが表示される <http://localhost:8080/vanilla> に移動します。

成功を確認するログインページ



7. demo レルムで作成したアカウントを使用してログインします。

demo レルムへのログインページ



DEMO

Log In

Username or email

johndoe


Password

••••••••

Log In

Red Hat Single Sign-On の使用が成功したことを示すメッセージが表示され、サンプル JBoss EAP アプリケーションを保護します。おめでとうございます。

完全な成功



LOGOUT

You are logged in!
Principal f1fb36db-29cd-4b6d-812b-edc82b31cbbd