# **Practical Exercise: Onboarding a Standard Web Application**

Training Objective

Learn how to configure a service provider for the sample application by setting up inbound authentication.

Business Scenario

PizzaShack needs developer squads to share applications they manage to avoid duplication and encourage reuse of applications and APIs.

High-Level Steps

* Create an application on the API Developer Portal
* Generate OAuth Keys
* Configure Service Provider
* Configure Role-Based Authentication

Detailed Instructions

1. Create an application on the API Developer Portal.
2. Follow the below steps to configure the new application

# **Registering a service provider**

You can connect your application with Identity Server and control how users log into your app. This guide provides instructions on how to add and configure a [service provider](https://is.docs.wso2.com/en/6.1.0/guides/applications/service-provider-overview) to Identity Server through the management console.

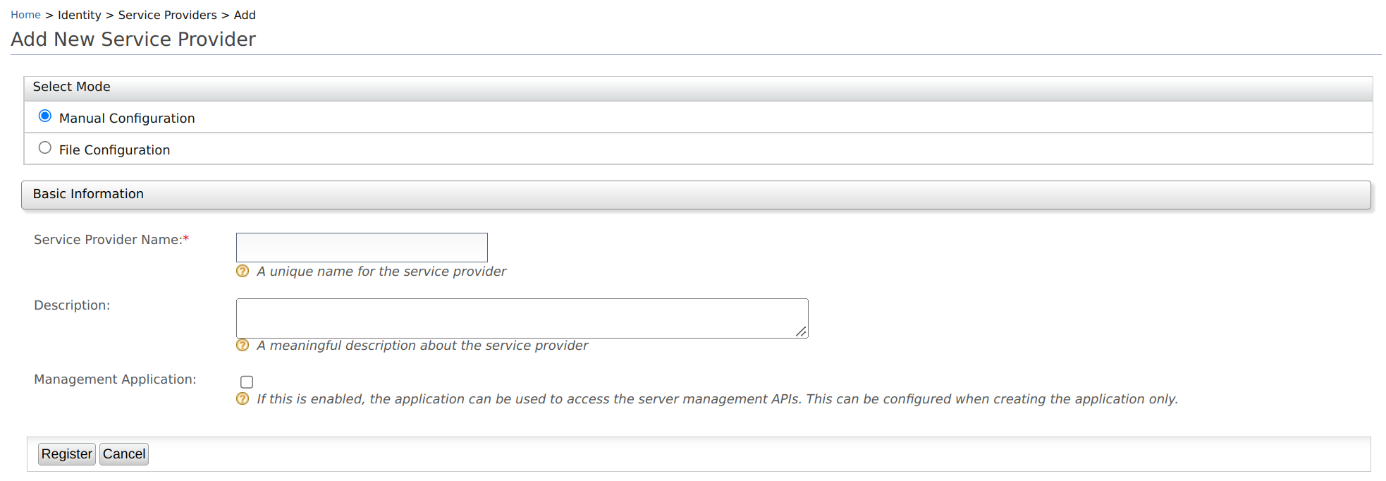
For more information on how the service provider fits into the WSO2 IS architecture, see [Architecture](https://is.docs.wso2.com/en/6.1.0/references/architecture/architecture).

## **Register a service provider**

To add a new service provider on WSO2 Identity Server:

1. On WSO2 IS Management Console, go to **Main > Identity > Service Providers > Add**.
2. Select **Manual Configuration**, and enter the following details:

| Field | Description |
| --- | --- |
| Service Provider Name | A name for your service provider. This field is required to register an SP. |
| Description | A short description of the service provider |
| Management Application | Select this checkbox if the application is used to access the management APIs. |



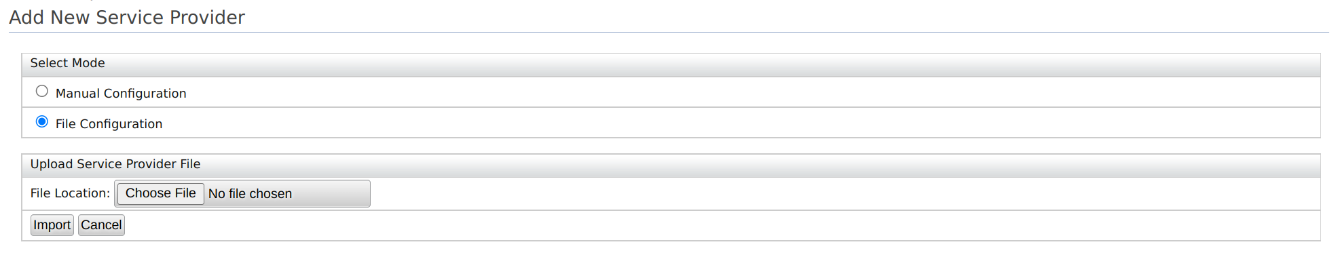
1. Modify validation for service provider name
2. Click **Register** to complete the registration.

**Info**

You can also [import a service provider](https://is.docs.wso2.com/en/latest/guides/applications/register-sp/#import-a-service-provider) using the **File configuration** option.

## **Import a service provider**

To import a service provider:

1. On WSO2 IS Management Console, go to **Main > Identity > Service Providers > Add**.
2. Select **File Configuration**, and upload the **.XML** file. 
3. Click **Import** to add the service provider using the XML file.

## **Service provider configurations**

You can find the basic configurations of a service provider under **Service Providers** section of the selected application.

| Field | Description |
| --- | --- |
| Select SP Certificate Type | A certificate is used to validate requests from the SP. You can either **Use SP JWKS endpoint** or **Upload SP certificate**. |
| JWKS URI | If you have selected **Use SP JWKS endpoint** in the above field, this field will appear. You need to add the JWKS endpoint URI in this field. |
| Application Certificate | If you have selected **Upload SP certificate** in the above field, paste the public certificate into the given text area or upload the certificate file in **PEM** format. Learn more about [public certificates for service providers](https://is.docs.wso2.com/en/latest/guides/applications/register-sp/#public-certificates-for-service-providers). |
| SaaS Application | Enable this to allow users to allow tenants to log in to the application. Disabling this allows only users of the current tenant (the tenant you use to configure the SP) to login into the application. |
| Discoverable Application | Enable this to make the application discoverable to users. |
| Access URL | Access URL for the Service Provider. |
| Logo URL | Add a link to the logo for your application here. |
| Logout Return URL or regex | The URL that the users will be redirected to during a direct IdP logout |
| Management Application | The selection you made for Management Application during the application creation will be shown here. This cannot be updated. WSO2 Identity Server exposes all the management capabilities as [REST APIs](https://is.docs.wso2.com/en/6.1.0/apis/overview/). These APIs are protected by OAuth2 access tokens and other API authentication mechanisms. The applications that are marked as management applications can only be used to access these management APIs in the OAuth2 flow. This can only be configured when creating the application. |

### **Public certificates for service providers**

A certificate is used to validate the signatures of the signed requests received from the application (service provider) to WSO2 IS.

#### Usage of the certificate

The certificate is used in the following scenarios:

* To validate the signature of the SAML2 authentication requests and the SAML2 logout requests sent by the service provider during [SAML SSO flows](https://is.docs.wso2.com/en/6.1.0/guides/login/sso-for-saml).
* When [passing OIDC authentication request parameters](https://is.docs.wso2.com/en/6.1.0/guides/login/oidc-parameters-in-auth-request) the certificate is used to:
  + Encrypt the id\_token sent to the service provider in the OIDC Authentication Response.
  + Validate the signed Request Object sent in the OAuth2/OIDC Authorization Request.

#### Obtain the PEM encoded certificate

WSO2 IS expects the certificate to be in PEM format.

To obtain the PEM content of a certificate in a JKS file:

1. Export the certificate from the key store using the following command.

keytool -export -keystore <keystore-path> -alias <alias-of-the-certificate> -file <path-of-the-expected-certificate-file>

Example: keytool -export -keystore wso2carbon.jks -alias wso2carbon -file wso2carbon.crt

1. The exported certificate will be in binary format. Convert this binary encoded certificate to a PEM-coded certificate using the following command.

openssl x509 -inform der -in <path-of-binary-certificate> -out <path-of-expected-pem-content>

Example: openssl x509 -inform der -in wso2carbon.crt -out wso2carbon.pem

#### What happens if you don't add the certificate

If the **Application Certificate** field is left blank, as WSO2 IS is backward compatible and follows the previous implementation to locate the certificates in the key store.

* For a SAML SSO flow, the certificate alias mentioned in SAML inbound authentication configuration will be used when the certificate is not updated via the management console.
* For an OIDC request object signature validation, the certificate will be retrieved from the default key store, an alias to the consumer key of the auth application.

# **Configure Role-Based Adaptive Authentication**

This page guides you through configuring role-based adaptive authentication for a sample web application.

## **Scenario**

Consider a scenario with two user roles, admin and manager. For users assigned to these roles, the login flow in applications should be stepped up with TOTP as follows:

1. Basic authentication (username and password)
2. TOTP or Security Key/Biometrics (FIDO)

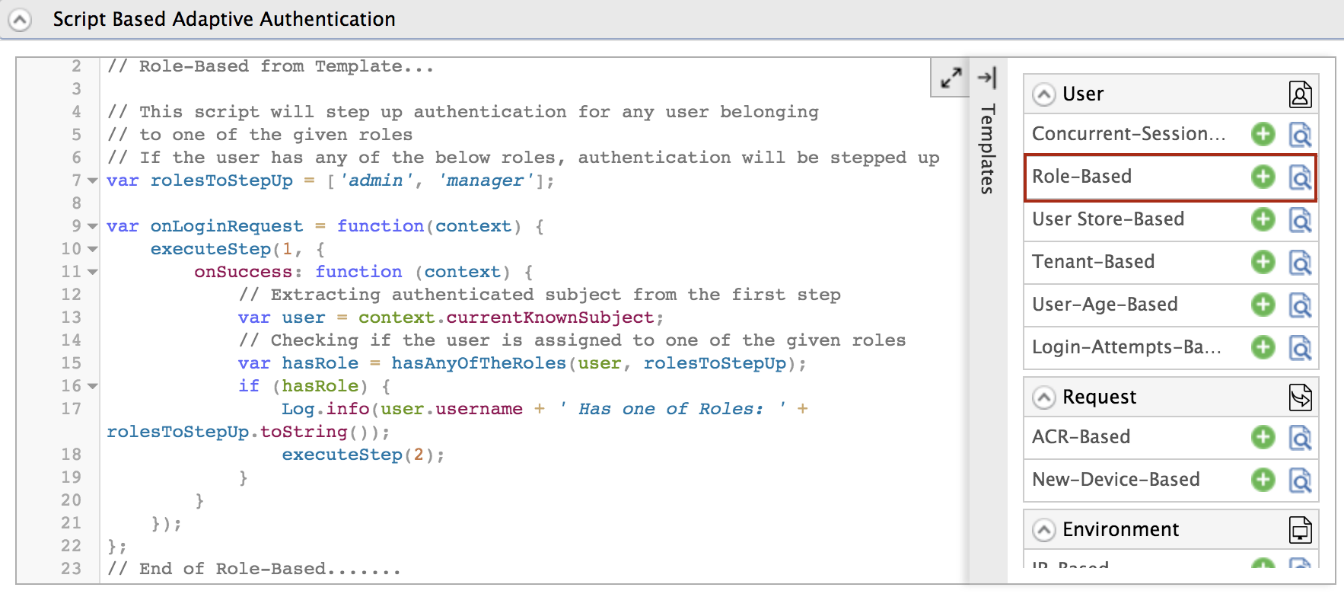
## **Prerequisites**

* See the [general prerequisites](https://is.docs.wso2.com/en/6.1.0/guides/adaptive-auth/configure-adaptive-auth/#prerequisites-for-adaptive-authentication) for all adaptive authenticaiton scenarios.
* You need to [set up the sample](https://is.docs.wso2.com/en/6.1.0/guides/adaptive-auth/adaptive-auth-overview/#set-up-the-sample) application.
* You need to [add a user](https://is.docs.wso2.com/en/6.1.0/guides/identity-lifecycles/admin-creation-workflow/) named Alex with login permissions. Do not assign any roles to this user.

## **Configure role-based authentication**

To configure role-based authentication:

1. On the management console, go to **Main** > **Identity** > **Service Providers** > **List**.
2. Click **Edit** on the saml2-web-app-pickup-dispatch.com service provider.
3. Expand the **Local and Outbound Authentication Configuration** section and click **Advanced Configuration**.
4. You will be redirected to **Advanced Configuration**, expand **Script Based Conditional Authentication**.
5. In the **Templates** section, click on the **+** corresponding to **Role-Based** template.



1. Click **Ok** to add the authentication script. The authentication script and authentication steps will be configured.

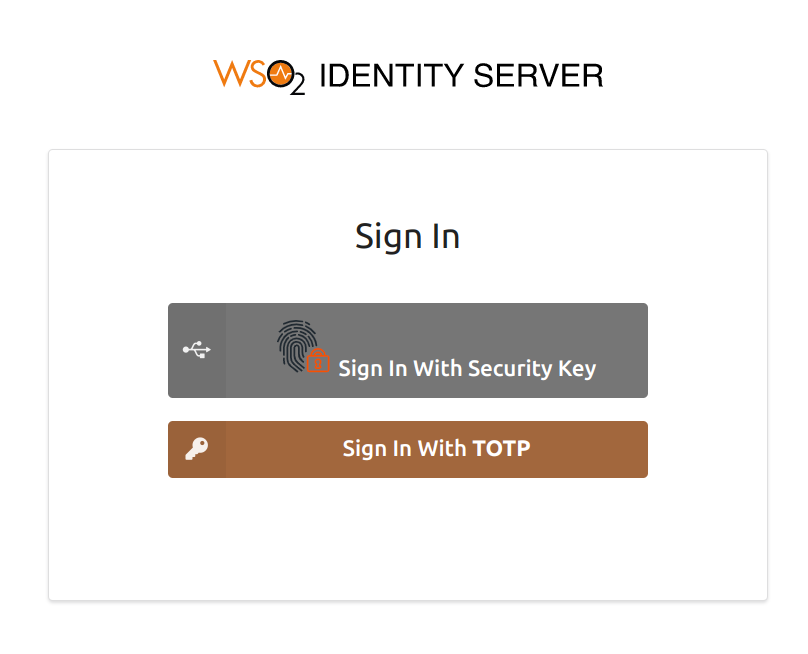
**Info**

By default, TOTP and Security Key/Biometrics (FIDO) will be added as the second authentication step. You can update this with any authentication method.

1. Click **Update** to save your configurations.

## **Try it out**

1. Access the following sample Pickup Dispatch application URL: http://localhost.com:8080/saml2-web-app-pickup-dispatch.com
2. Click **Login** and enter your admin account credentials.
3. You will be prompted to enter your TOTP or Security Key/Biometrics (FIDO) code. Enter any code and click **Sign In**.



1. Log out of the application and log in again as Alex.
2. Alex will be able to log in to the application after the successful completion of basic authentication.

Expected Outcome

As a result of this exercise, only certain users will be able to authenticate to the newly added application.