BlackBerry Web Services OAuth

Implementation Guide

12.17

Contents

Using OAuth authentication for the BlackBerry Web Services REST APIs

Version 12.12 of the BlackBerry Web Services REST APIs introduce support for OAuth, an industry standard identity verification and authentication process. For more information about OAuth, visit https://openid.net/connect/.

OAuth for the BlackBerry Web Services REST APIs is supported for BlackBerry UEM Cloud and BlackBerry UEM version 12.12 and later. The OAuth implementation leverages BlackBerry Enterprise Identity for authentication using OAuth2 and supports the following grant types:

- client_credentials grant type for simple scripts and unattended automation use cases
- authorization_code grant type for advanced apps using UEM administrator user credentials

The supported authentication types depend on the type of app and the UEM environment:

App type	Description	Supported OAuth grant types
Enterprise app	An enteprise app is developed and distributed internally within an organization. The app developer can configure the app to require user authentication or to function as a simple utility that can run unattended.	• authorization_code • client_credentials
Third-party app in a customer's on-premises environment	A third-party app is created by a third-party developer and deployed in an organization's on-premises domain.	• authorization_code
Third-party app in a cloud environment	A third-party app is created by a third-party developer and deployed in a third-party cloud domain.	• authorization_code

This guide is intended for app developers, but some tasks must be completed by a UEM administrator and BlackBerry Online Account administrator. Contact the UEM administrator in your organization, or the UEM administrator in the organization that you are developing the app for, to coordinate and complete the necessary administrator tasks.

Prerequisites for using OAuth with the BlackBerry Web Services REST APIs

- You or a BlackBerry UEM administrator require a BlackBerry Online Account that is associated with the organization's UEM domain.
- If you are a third-party developer creating an app for an organization that uses UEM, you require a BlackBerry Online Account.
- Note that the BlackBerry Web Services REST APIs use the following default ports:
  - UEM (on-premises): 18084
  - UEM Cloud: 443

- Note the following discovery document URI for BlackBerry Enterprise Identity: https://idp.blackberry.com/op/tenant/{tenantId}/.well-known/openid-configuration. You will use this URI for tenant-specific authentication and access for the app.

OAuth sample apps

BlackBerry provides the following sample apps that demonstrate how to use the BlackBerry Web Services REST APIs with OAuth. The samples are available as a downloadable .zip package. The package includes a readme file that explains each sample in detail.

The instructions in this document refer to these sample apps to clarify certain details or steps.

Java samples

Sample name	Description
SampleWithAuthorizationCodeAndClientSecret.java	A sample app that uses the authorization_code grant type and a client secret
SampleWithClientCredsAndClientSecret.java	A sample app that uses the client_credentials grant type and a client secret
SampleWithClientCredsAndPrivateKey.java	A sample app that uses the client_credentials grant type and a private key

PowerShell samples

Sample name	Description
SampleWithAuthorizationCodeAndClientSecret.ps1	A sample script that uses the authorization_code grant type and a client secret
SampleWithAuthorizationCodeAndClientSecretRefreshT	A sample script that uses the authorization_code grant type and a client secret with a refresh token
SampleWithClientCredsAndClientSecret.ps1	A sample script that uses the client_credentials grant type and a client secret
SampleWithClientCredsAndPrivateKey.ps1	A sample script that uses the client_credentials grant type and a private key

Postman REST client samples

Sample name	Description
AuthorizationCodeGrant.postman_environment.json	A Postman environment settings sample that demonstrates the authorization_code grant type variables

Sample name	Description
ClientCredentialsGrant.postman_environment.json	A Postman environment settings sample that demonstrates the client_credentials grant type variables
PublicRestApiSamples.postman_collection.json	A Postman sample that uses the environment settings described above to use authorization_code and client_credentials when invoking the BlackBerry Web Services REST APIs

Use cases for implementing OAuth for the BlackBerry Web Services REST APIs

Based on your use case and how you want your app to use OAuth with the BlackBerry Web Services REST APIs, follow the instructions in the appropriate section of this guide:

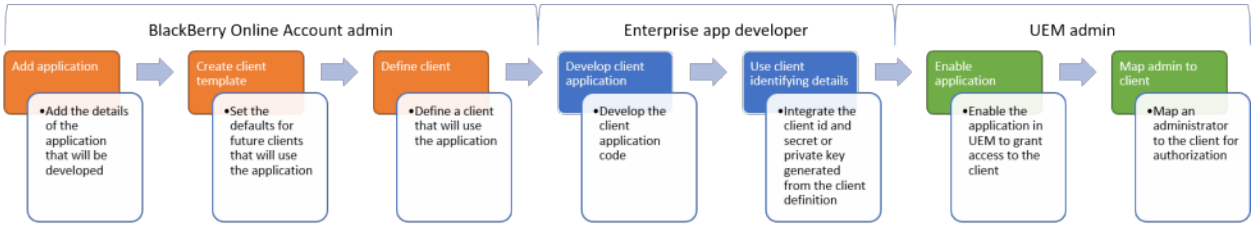
- Using the OAuth client credentials grant type with an enterprise app
- Using the OAuth authorization code grant type with an enterprise app
- Using OAuth with a third-party app in an on-premises environment
- Using OAuth with a third-party app in a cloud environment

Using the OAuth client credentials grant type with an enterprise app

Follow the instructions in this section if you are developing an app that will be distributed within your organization and you want to use the OAuth client credentials grant type for a simple utility that can run unattended. Apps of this type typically do not have browser capabilities.

You can download the package of sample apps to review and execute samples that demonstrate this use case. The applicable samples are referenced throughout this section.

The following diagram summarizes the tasks involved, and who is responsible for completing them:



Configure the app resources in BlackBerry Online Account

This task must be completed by someone (you or the UEM administrator) that has access to the BlackBerry Online Account that is associated with the UEM domain. You or the UEM administrator use the BlackBerry Online Account to:

- Add the details of the app (name, description, entitlement ID, version, capabilities)
- Create a client template that defines the default settings for all clients that belong to the app
- Use the client template to define the app client and generate a unique client ID (and if applicable, client secret) that the app can use to connect to UEM and invoke the REST APIs

For all tasks that involve the use of BlackBerry Online Account, see the BlackBerry Online Account User Guide for complete instructions.

Before you begin: If an administrator will complete this task, review the steps below and give the administrator the necessary information that they will need to specify (name, entitlement ID, entitlement version, preferred token endpoint authentication method, and so on).

1. Log in to BlackBerry Online Account and navigate to your organization.
2. On the menu bar, click **Applications**. On the **Organization** tab, click **Add Application**.
3. Specify the app details. In the **Capabilities** section, select the **BlackBerry Platform APIs** check box only (unless you are making changes to an existing app that uses other capabilities). For example:
   - **Name**: BB Sample Client Credentials App
   - **Entitlement ID**: com.domain.bb.sample.cc
   - **Entitlement version**: 1.0.0.0
   - **Capabilities**: BlackBerry Platform APIs
4. Click **Add Application**.
5. On the **BlackBerry Platform APIs** tab for the app, on the **Template** tab, click **Add Template**.
6. Specify the template details. Select the following options:
   - **Redirect URLs**: https://localhost:9443/cb

- **Type**: web
- **Grant Type**: client_credentials
- **Response Types**: none
- **Token Endpoint Auth Method**
  - To generate a client secret code, click client_secret_basic.
  - To require the generation of a public/private key pair (you will register the public key when you define the client in step 8 and on), click private_key_jwt.
- **API Scopes**: Mobile Device Management

The SampleWithClientCredsAndClientSecret.java sample demonstrates the use of the client_secret_basic token endpoint authentication method. The SampleWithClientCredsAndPrivateKey.java sample demonstrates the private_key_jwt method and passes a private key when executed.

7. Click **Register**.
8. On the **BlackBerry Platform APIs** tab for the app, on the **Client** tab, click **Add Client**.
9. Specify the required information.
   Example for SampleWithClientCredsAndClientSecret.java
   - **Client Name**: BlackBerry Sample Client Credentials Client
   - **Tenants**: Select the UEM tenants that the client app will contact to invoke the REST APIs.

   Example for SampleWithClientCredsAndPrivateKey.java
   - **Client Name**: BlackBerry Sample Client Credentials Client
   - **Id Token Signed Response Alg**: RS256
   - **Token Endpoint Auth Signing Alg**: RS256
   - **Public Key**: Add the public key in PKCS#8 format
   - **Tenants**: Select the UEM tenants that the client app will contact to invoke the REST APIs.
10. Click **Register**.

The client ID (and if applicable, the client secret) is generated. The client app will use the client ID and either a client secret or private key (depending on the configuration) to connect to the BlackBerry Web Services REST APIs.

After you finish: Develop the client app.

Develop the client app

After you or a UEM administrator configure the app resources in BlackBerry Online Account, you can develop the client app that will invoke the BlackBerry Web Services REST APIs using OAuth. You can use any programming language that supports OAuth.

Download and review the sample apps to see examples of OAuth implementation. For example, SampleWithClientCredsAndClientSecret.java demonstrates how the client ID and client secret are passed on the command line to BlackBerry Enterprise Identity for authentication. BlackBerry Enterprise Identity provides a service token with a 10 minute expiry.

Note the following requirements for the app:

- You must configure the client app to use the client ID and client secret (if you selected client_secret_basic token endpoint authentication) or the client ID and and a private key (if you selected private_key_jwt). This information must be stored securely.
- The authentication scope for requesting tokens from BlackBerry Enterprise Identity and invoking the REST APIs is **MDMBWS.All**.

- The app must be able to handle a change in BlackBerry Enterprise Identity keys at any time. To avoid a load spike in key rollover and some failure scenarios, design the app to do the following:
  - Cache a local copy of the BlackBerry Enterprise Identity public key set on a periodic basis (max 24 hours).
  - When validating the BlackBerry Enterprise Identity token signature, find the correct key by searching the local key set copy using the key id (kid) identified in the JWT header.
  - If the kid cannot be found in the local key set copy, and if the last copy is older than a configurable amount of time (minimum 30 mins), load the key set directly from BlackBerry Enterprise Identity. This covers emergency key rolling within the 24 hour period and throttles key set requests sent to BlackBerry Enterprise Identity in failure scenarios.
- If the app uses private_key_jwt token endpoint authentication and can roll its keys, BlackBerry Enterprise Identity requires the app to follow the key rolling recommendations in the OpenID Connect spec.

When you are ready to deploy the app to users, coordinate with the UEM administrator to enable the app in UEM.

Enable and authorize the app in UEM

The UEM administrator must complete the steps below to authorize the client app with BlackBerry Enterprise Identity (the token issuer) and BlackBerry UEM (the provider of the BlackBerry Web Services REST APIs).

Before you begin:

- Configure the app resources in BlackBerry Online Account
- Develop the client app

1. In the UEM management console, on the menu bar, click **Settings > BlackBerry Enterprise Identity > Services**.
2. In the **OpenID Connect** apps table, click **+**.
3. Click the app name that was added in BlackBerry Online Account.
4. Complete the prompts and add the app.
5. Click **Settings > Administrators > Web service clients**.
6. Select the client in the table.
7. Select an administrator user to map to the client app.

After you finish: Compile and run the app to verify that it can invoke the BlackBerry Web Services REST APIs.

If you've used one of the sample apps to complete the tasks in this section, you can compile and run the sample app with the following arguments:

SampleWithClientCredsAndClientSecret.java

```
-c <arg>     Client id

-cs <arg>    Client secret

-t <arg>     Tenant id

-uem <arg>   UEM endpoint
```

SampleWithClientCredsAndPrivateKey.java

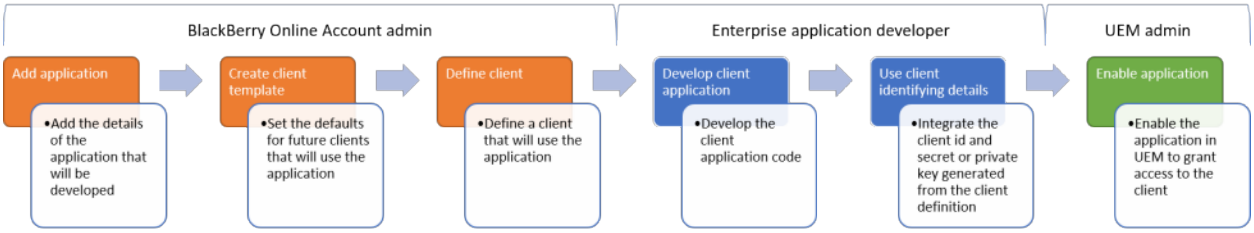
```
-c <arg>     Client id

-pk <arg>    Path to the private key pem file

-t <arg>     Tenant id

-uem <arg>   UEM endpoint
```

Using the OAuth authorization code grant type with an enterprise app

Follow the instructions in this section if you are developing an app that will be distributed within your organization and you want to use the OAuth authorization code grant type and the credentials of a UEM administrator account to authenticate users with BlackBerry Enterprise Identity. Apps of this type have browser capabilities.

You can download the package of sample apps to review and execute samples that demonstrate this use case. The applicable samples are referenced throughout this section.

The following diagram summarizes the tasks involved, and who is responsible for completing them:



Configure the app resources in BlackBerry Online Account

This task must be completed by someone (you or the UEM administrator) that has access to the BlackBerry Online Account that is associated with the UEM domain. You or the UEM administrator use the BlackBerry Online Account to:

- Add the details of the app (name, description, entitlement ID, version, capabilities)
- Create a client template that defines the default settings for all clients that belong to the app
- Use the client template to define the app client and generate a unique client ID (and if applicable, client secret) that the app can use to connect to UEM and invoke the REST APIs

For all tasks that involve the use of BlackBerry Online Account, see the BlackBerry Online Account User Guide for complete instructions.

Before you begin: If an administrator will complete this task, review the steps below and give the administrator the necessary information that they will need to specify (name, entitlement ID, entitlement version, preferred token endpoint authentication method, and so on).

1. Log in to BlackBerry Online Account and navigate to your organization.
2. On the menu bar, click **Applications**. On the **Organization** tab, click **Add Application**.
3. Specify the app details. In the **Capabilities** section, select the **BlackBerry Platform APIs** check box only (unless you are making changes to an existing app that uses other capabilities). For example:
   - **Name**: BB Sample Authorization Code App
   - **Entitlement ID**: com.domain.bb.sample.ua
   - **Entitlement version**: 1.0.0.0
   - **Type**: Application
   - **Capabilities**: BlackBerry Platform APIs
4. Click **Add Application**.
5. On the **BlackBerry Platform APIs** tab for the app, on the **Template** tab, click **Add Template**.
6. Specify the template details. Specify or select the following options:

- **Redirect URLs**: the app web page address that BlackBerry Enterprise Identity will invoke as a browser redirect for user authentication (for example, https://localhost:9443/cb)
- **Type**: web
- **Grant Type**: authorization_code
- **Response Types**: code
- **Token Endpoint Auth Method**
  - To generate a client secret code, click client_secret_basic.
  - To require the generation of a public/private key pair (you will register the public key when you define the client in step 8 and on), click private_key_jwt.
- **API Scopes**: Mobile Device Management

The SampleWithAuthorizationCodeAndClientSecret.java sample demonstrates the use of the client_secret_basic token endpoint authentication method.

7. Click **Register**.
8. On the **BlackBerry Platform APIs** tab for the app, on the **Client** tab, click **Add Client**.
9. Specify the required information.
   Example for SampleWithAuthorizationCodeAndClientSecret.java
   - **Client Name**: BB Sample Authorization Code Client
   - **Tenants**: Select the UEM tenants that the client app will contact to invoke the REST APIs.
10. Click **Register**.

The client ID (and if applicable, the client secret) is generated. The client app will use the client ID and either a client secret or private key (depending on the configuration) to connect to the BlackBerry Web Services REST APIs.

After you finish: Develop the client app.

Develop the client app

After you or a UEM administrator configure the app resources in BlackBerry Online Account, you can develop the client app that will invoke the BlackBerry Web Services REST APIs using OAuth. You can use any programming language that supports OAuth.

Download and review the sample apps to see examples of OAuth implementation.

- The SampleWithAuthorizationCodeAndClientSecret.java sample demonstrates how the client ID and client secret are passed on the command line to BlackBerry Enterprise Identity to receive an access token for authentication (the token expiry period is 15 minutes).
- The SampleWithAuthorizationCodeAndClientSecretRefreshToken.ps1 PowerShell sample demonstrates how BlackBerry Enterprise Identity can provide an optional refresh token that can be used to request a new access token on expiry. The refresh token expiry is 1 year, and it must be stored securely. A new refresh token is provided with a new access token.

Note the following requirements for the app:

- You must configure the client app to use the client ID and client secret (if you selected client_secret_basic token endpoint authentication) or the client ID and and a private key (if you selected private_key_jwt). This information must be stored securely.
- The app must support browser-based user authorization and redirects from BlackBerry Enterprise Identity.
- To receive an access token from BlackBerry Enterprise Identity, the end user must provide the credentials of a UEM administrator when they are prompted.

- If you want the app to continue working in unattended mode after initial authentication, the app can use a refresh token to get a new access token on its expiry. As long as the app continues to use the refresh token, it can run in unattended mode perpetually.
- The authentication scope for requesting tokens from BlackBerry Enterprise Identity and invoking the REST APIs is **openid MDMBWS.All**. If you want to use refresh tokens, use **openid offline_access MDMBWS.All** .
- The app must be able to handle a change in BlackBerry Enterprise Identity keys at any time. To avoid a load spike in key rollover and some failure scenarios, design the app to do the following:
  - Cache a local copy of the BlackBerry Enterprise Identity public key set on a periodic basis (max 24 hours).
  - When validating the BlackBerry Enterprise Identity token signature, find the correct key by searching the local key set copy using the key id (kid) identified in the JWT header.
  - If the kid cannot be found in the local key set copy, and if the last copy is older than a configurable amount of time (minimum 30 mins), load the key set directly from BlackBerry Enterprise Identity. This covers emergency key rolling within the 24 hour period and throttles key set requests sent to BlackBerry Enterprise Identity in failure scenarios.
- If the app uses private_key_jwt token endpoint authentication and can roll its keys, BlackBerry Enterprise Identity requires the app to follow the key rolling recommendations in the OpenID Connect spec.

When you are ready to deploy the app to users, coordinate with the UEM administrator to enable the app in UEM.

Enable the app in UEM

The UEM administrator must complete the steps below to authorize the client app with BlackBerry Enterprise Identity (the token issuer) and BlackBerry UEM (the provider of the BlackBerry Web Services REST APIs).

Before you begin:

- Configure the app resources in BlackBerry Online Account
- Develop the client app

1. In the UEM management console, on the menu bar, click **Settings > BlackBerry Enterprise Identity > Services**.
2. In the **OpenID Connect** apps table, click **+**.
3. Click the app name that was added in BlackBerry Online Account.
4. Complete the prompts and add the app.

After you finish:

- If any changes are made to the client template or app clients defined in BlackBerry Online Account, the UEM administrator must repeat this task.
- Compile and run the app to verify that it can invoke the BlackBerry Web Services REST APIs.

If you've used one of the sample apps to complete the tasks in this section, you can compile and run the sample app with the following arguments:

SampleWithAuthorizationCodeAndClientSecret.java

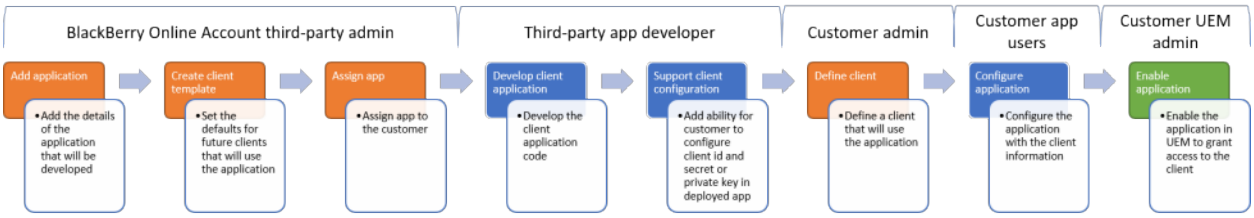
```
-c <arg>     Client id

-cs <arg>    Client secret

-t <arg>     Tenant id

-uem <arg>   UEM endpoint
```

Using OAuth with a third-party app in an on-premises environment

Follow the instructions in this section if you are a third-party developer creating an app that will be distributed to a customer's on-premises domain or to a dedicated hosted domain. You must have an ISV organization type in BlackBerry Online Account to complete the steps in this section. BlackBerry strongly recommends using the authorization code grant type for this use case.

You can download the package of sample apps to review and execute samples that demonstrate this use case. The applicable samples are referenced throughout this section.

The following diagram summarizes the tasks involved, and who is responsible for completing them:



Configure the app resources in BlackBerry Online Account

Complete this task in your BlackBerry Online Account to:

- Add the details of the app (name, description, entitlement ID, version, capabilities)
- Create a client template that defines the default settings for all clients that belong to the app; your customer will use this template to define an app client
- Entitle the app to your customer so they can define an app client

For all tasks that involve the use of BlackBerry Online Account, see the BlackBerry Online Account User Guide for complete instructions.

1. Log in to BlackBerry Online Account and navigate to your organization.
2. On the menu bar, click **Applications**. On the **Organization** tab, click **Add Application**.
3. Specify the app details. In the **Capabilities** section, select the **BlackBerry Platform APIs** check box only (unless you are making changes to an existing app that uses other capabilities). For example:
   - **Name**: BB Sample 3rd Party OnPrem App
   - **Entitlement ID**: com.domain.bb.sample.ua
   - **Entitlement version**: 1.0.0.0
   - **Type**: Application or Solutions
   - **Capabilities**: BlackBerry Platform APIs
4. Click **Add Application**.
5. On the **BlackBerry Platform APIs** tab for the app, on the **Template** tab, click **Add Template**.
6. Specify the template details. Specify or select the following options:
   - **Redirect URLs**: the app web page address that BlackBerry Enterprise Identity will invoke as a browser redirect for user authentication (for example, https://localhost:9443/cb)
   - **Type**: web
   - **Grant Type**: recommend authorization_code or authorization_code,refresh_token

- **Response Types**: code
- **Token Endpoint Auth Method**
  - To generate a client secret code, click client_secret_basic. The code is generated when your customer defines the app client.
  - To require the generation of a public/private key pair (the public key is registered when the customer defines the app client), click private_key_jwt.
- **Application Scope**: Organization (this allows your customer to define the app client in their BlackBerry Online Account)
- **API Scopes**: Mobile Device Management

The SampleWithAuthorizationCodeAndClientSecretRefreshToken.ps sample demonstrates the use of the authorization_code grant type with the use of a refresh token that can be used to request a new access token from BlackBerry Enterprise Identity on expiry. The refresh token expiry is 1 year, and it must be stored securely. A new refresh token is provided with a new access token.

7. Click **Register**.
8. On the menu, click **Manage Customers**.
9. Click a customer.
10. In the **Publishing Status** column, click the **UNPUBLISHED** check box to entitle the app to your customer.

After you finish: Develop the client app.

Develop the client app

After you configure the app resources in BlackBerry Online Account, you can develop the app that will invoke the BlackBerry Web Services REST APIs using OAuth. You can use any programming language that supports OAuth.

Download and review the sample apps to see examples of OAuth implementation. The SampleWithAuthorizationCodeAndClientSecretRefreshToken.ps sample demonstrates the use of the authorization_code grant type with a refresh token that can be used to request a new access token from BlackBerry Enterprise Identity on expiry. The refresh token expiry is 1 year, and it must be stored securely. A new refresh token is provided with a new access token.

Note the following requirements for the app:

- Structure the app so that customer can configure the app to use the client ID and client secret (if you selected client_secret_basic token endpoint authentication) or the client ID and a private key (if you selected private_key_jwt). This information must be stored securely.
- The app must support browser-based user authorization and redirects from BlackBerry Enterprise Identity.
- To receive an access token from BlackBerry Enterprise Identity, the customer's end users must provide the credentials of a UEM administrator when they are prompted.
- If you want the app to continue working in unattended mode after initial authentication, the app can use a refresh token to get a new access token on its expiry. As long as the app continues to use the refresh token, it can run in unattended mode perpetually.
- The authentication scope for requesting tokens from BlackBerry Enterprise Identity and invoking the REST APIs is **openid MDMBWS.All**. If you want to use refresh tokens, use **openid offline_access MDMBWS.All** .
- The app must be able to handle a change in BlackBerry Enterprise Identity keys at any time. To avoid a load spike in key rollover and some failure scenarios, design the app to do the following:
  - Cache a local copy of the BlackBerry Enterprise Identity public key set on a periodic basis (max 24 hours).
  - When validating the BlackBerry Enterprise Identity token signature, find the correct key by searching the local key set copy using the key id (kid) identified in the JWT header.

    - If the kid cannot be found in the local key set copy, and if the last copy is older than a configurable amount of time (minimum 30 mins), load the key set directly from BlackBerry Enterprise Identity. This covers emergency key rolling within the 24 hour period and throttles key set requests sent to BlackBerry Enterprise Identity in failure scenarios.
- If the app uses private_key_jwt token endpoint authentication and can roll its keys, BlackBerry Enterprise Identity requires the app to follow the key rolling recommendations in the OpenID Connect spec.

When the app is ready to deploy to the customer's users, coordinate with the UEM administrator to define the app client and enable the app in UEM. Provide any information that app users will need to configure and use the app.

Define the app client

Your customer's UEM administrator must complete this task using the BlackBerry Online Account that is associated with the organization's UEM domain.

Before you begin: The third-party developer must configure the app resources in BlackBerry Online Account, develop the client app, and provide the information required to define the client.

1. Log in to the BlackBerry Online Account that is associated with the organization's UEM domain.
2. On the menu, click **Applications.** On the **Marketplace** tab, edit the third-party app that was entitled to your organization.
3. Click **Add Client**.
4. Specify the required information provided by the third-party developer.

   Example for SampleWithAuthorizationCodeAndClientSecretRefreshToken.ps

   - **Client Name**: BB Sample 3rd Pary OnPrem Client
   - **Tenants**: Select the UEM tenants that the client app will contact to invoke the REST APIs.
5. Click **Register**.

The client ID (and if applicable, the client secret) is generated. The client app will use the client ID and either a client secret or private key (depending on the configuration set by the third-party developer) to connect to the BlackBerry Web Services REST APIs.

After you finish:

- Refer to the developers instructions for how app users can configure the app to use the client ID and client secret (for client_secret_basic token endpoint authentication) or the client ID and a private key (for private_key_jwt token endpoint authentication).
- The UEM administrator enables the app in UEM.

Enable the app in UEM

The customer's UEM administrator must complete the steps below to authorize the client app with BlackBerry Enterprise Identity (the token issuer) and BlackBerry UEM (the provider of the BlackBerry Web Services REST APIs).

Before you begin:

- The third-party developer must configure the app resources in BlackBerry Online Account and develop the client app.
- The UEM administrator must define the app client.

1. In the UEM management console, on the menu bar, click **Settings > BlackBerry Enterprise Identity > Services**.

2. In the **OpenID Connect** apps table, click **+**.
3. Click the app name that was added in BlackBerry Online Account.
4. Complete the prompts and add the app.

After you finish:

- If any changes are made to the client template or app clients defined in BlackBerry Online Account, the UEM administrator must repeat this task.
- Compile and run the app to verify that it can invoke the BlackBerry Web Services REST APIs.

If you've used the SampleWithAuthorizationCodeAndClientSecretRefreshToken.ps sample, you can edit the PowerShell script to configure and execute it:

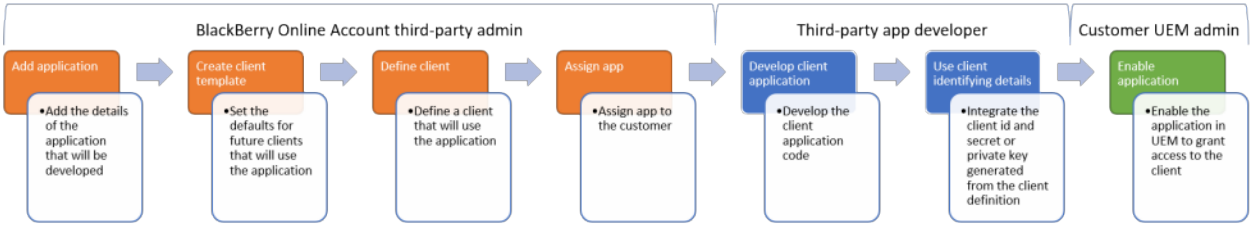
```
.\SampleWithAuthorizationCodeAndClientSecretRefreshToken
```

Using OAuth with a third-party app in a cloud environment

Follow the instructions in this section if you are a third-party developer creating an app that will be used by a customer in your cloud domain. You must have an ISV organization type in BlackBerry Online Account to complete the steps in this section. BlackBerry strongly recommends using the authorization code grant type for this use case.

You can download the package of sample apps to review and execute samples that demonstrate this use case. The applicable samples are referenced throughout this section.

The following diagram summarizes the tasks involved, and who is responsible for completing them:



Configure the app resources in BlackBerry Online Account

Complete this task in your BlackBerry Online Account to:

- Add the details of the app (name, description, entitlement ID, version, capabilities)
- Create a client template that defines the default settings for all clients that belong to the app
- Use the client template to define the app client and generate a unique client ID (and if applicable, client secret) that the app can use to connect to UEM and invoke the REST APIs
- Entitle the app to your customer

For all tasks that involve the use of BlackBerry Online Account, see the BlackBerry Online Account User Guide for complete instructions.

1. Log in to BlackBerry Online Account.
2. On the menu bar, click **Applications**. On the **Organization** tab, click **Add Application**.
3. Specify the app details. In the **Capabilities** section, select the **BlackBerry Platform APIs** check box only (unless you are making changes to an existing app that uses other capabilities). For example:
   - **Name**: BB Sample 3rd Party Cloud App
   - **Entitlement ID**: com.domain.bb.sample.ua
   - **Entitlement version**: 1.0.0.0
   - **Type**: Application or Solutions
   - **Capabilities**: BlackBerry Platform APIs
4. Click **Add Application**.
5. On the **BlackBerry Platform APIs** tab for the app, on the **Template** tab, click **Add Template**.
6. Specify the template details. Specify or select the following options:
   - **Redirect URLs**: the app web page address that BlackBerry Enterprise Identity will invoke as a browser redirect for user authentication (for example, https://localhost:9443/cb)
   - **Type**: web

- **Grant Type**: recommend authorization_code or authorization_code,refresh_token
- **Response Types**: code
- **Token Endpoint Auth Method**
  - To generate a client secret code, click client_secret_basic.
  - To require the generation of a public/private key pair, click private_key_jwt.
- **Application Scope**: Global (this option prevents your customer from creating additional app clients in the organization's BlackBerry Online Account; your customer will use the app client that you define)
- **API Scopes**: Mobile Device Management

The SampleWithAuthorizationCodeAndClientSecretRefreshToken.ps sample demonstrates the use of the authorization_code grant type with the use of a refresh token that can be used to request a new access token from BlackBerry Enterprise Identity on expiry. The refresh token expiry is 1 year, and it must be stored securely. A new refresh token is provided with a new access token.

7. Click **Register**.
8. On the **BlackBerry Platform APIs** tab for the app, on the **Client** tab, click **Add Client**.
9. Specify the required information.
10. Click **Register**.

    The client ID (and if applicable, the client secret) is generated. The client app will use the client ID and either a client secret or private key (depending on the configuration) to connect to the BlackBerry Web Services REST APIs.
11. On the menu, click **Manage Customers**.
12. Click a customer.
13. In the **Publishing Status** column, click the **UNPUBLISHED** check box to entitle the app to your customer.

After you finish: Develop the client app.

Develop the client app

After you configure the app resources in BlackBerry Online Account, you can develop the client app that will invoke the BlackBerry Web Services REST APIs using OAuth. You can use any programming language that supports OAuth.

Download and review the sample apps to see examples of OAuth implementation. The SampleWithAuthorizationCodeAndClientSecretRefreshToken.ps sample demonstrates the use of the authorization_code grant type with a refresh token that can be used to request a new access token from BlackBerry Enterprise Identity on expiry. The refresh token expiry is 1 year, and it must be stored securely. A new refresh token is provided with a new access token.

Note the following requirements for the app:

- You must configure the client app to use the client ID and client secret (if you selected client_secret_basic token endpoint authentication) or the client ID and and a private key (if you selected private_key_jwt). This information must be stored securely.
- The app must support browser-based user authorization and redirects from BlackBerry Enterprise Identity.
- To receive an access token from BlackBerry Enterprise Identity, the end user must provide the credentials of a UEM administrator when they are prompted.
- If you want the app to continue working in unattended mode after initial authentication, the app can use a refresh token to get a new access token on its expiry. As long as the app continues to use the refresh token, it can run in unattended mode perpetually.
- The authentication scope for requesting tokens from BlackBerry Enterprise Identity and invoking the REST APIs is **openid MDMBWS.All**. If you want to use refresh tokens, use **openid offline_access MDMBWS.All** .

- The app must be able to handle a change in BlackBerry Enterprise Identity keys at any time. To avoid a load spike in key rollover and some failure scenarios, design the app to do the following:
  - Cache a local copy of the BlackBerry Enterprise Identity public key set on a periodic basis (max 24 hours).
  - When validating the BlackBerry Enterprise Identity token signature, find the correct key by searching the local key set copy using the key id (kid) identified in the JWT header.
  - If the kid cannot be found in the local key set copy, and if the last copy is older than a configurable amount of time (minimum 30 mins), load the key set directly from BlackBerry Enterprise Identity. This covers emergency key rolling within the 24 hour period and throttles key set requests sent to BlackBerry Enterprise Identity in failure scenarios.
- If the app uses private_key_jwt token endpoint authentication and can roll its keys, BlackBerry Enterprise Identity requires the app to follow the key rolling recommendations in the OpenID Connect spec.

When the app is ready to deploy to the customer's users, coordinate with the UEM administrator to enable the app in UEM.

Enable the app in UEM

The customer's UEM administrator must complete the steps below to authorize the client app with BlackBerry Enterprise Identity (the token issuer) and BlackBerry UEM (the provider of the BlackBerry Web Services REST APIs).

Before you begin: The developer must configure the app resources in BlackBerry Online Account and develop the client app.

1. In the UEM management console, on the menu bar, click **Settings > BlackBerry Enterprise Identity > Services**.
2. In the **OpenID Connect** apps table, click **+**.
3. Click the app name that was added in BlackBerry Online Account.
4. Complete the prompts and add the app.

After you finish:

- If any changes are made to the client template or app clients defined in BlackBerry Online Account, the UEM administrator must repeat this task.
- Compile and run the app to verify that it can invoke the BlackBerry Web Services REST APIs.

If you've used the SampleWithAuthorizationCodeAndClientSecretRefreshToken.ps sample, you can edit the PowerShell script to configure and execute it:

```
.\SampleWithAuthorizationCodeAndClientSecretRefreshToken
```

Legal notice

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada