BlackBerry 2FA

Administration Guide

Contents

About BlackBerry 2FA

BlackBerry 2FA protects access to your organization's critical resources using two-factor authentication. The product uses a password that users enter and a secure prompt on their mobile device each time they attempt to access resources. BlackBerry 2FA also supports the use of standards-based One-Time Password (OTP) tokens.

You manage BlackBerry 2FA users from the BlackBerry UEM Cloud or BlackBerry UEM management console. You can also use BlackBerry 2FA on devices that aren't managed by BlackBerry UEM Cloud or BlackBerry UEM. BlackBerry 2FA supports iOS and Android devices that have only a BlackBerry Dynamics container, devices managed by third-party MDM systems, or unmanaged devices.

You can use BlackBerry 2FA to protect a wide variety of systems, including VPNs, RADIUS-compatible systems, custom applications using a REST API, and SAML-compliant cloud services when they are used in conjunction with BlackBerry Enterprise Identity.

Configuring BlackBerry 2FA for use with mobile devices is straightforward. The first authentication factor, the password, can be a user's directory or container password. The second authentication factor, the device prompt, requires an app on the device that triggers a secure validation of the device. For iOS and Android devices, BlackBerry 2FA is included in the BlackBerry UEM Client. They are either installed during activation or you must have users install them. For managed BlackBerry 10 devices, you must deploy a separate BlackBerry 2FA app or have users install it.

Configuring BlackBerry 2FA for users without mobile devices is also straightforward. Standards-based OTP tokens are registered in the BlackBerry UEM console and issued to users. The first authentication factor is the user's directory password, and the second authentication factor is a dynamic code that appears on the token's screen. For more information, see the Administration content for BlackBerry 2FA.

The BlackBerry 2FA server is an optional component that is deployed when the product is used in conjunction with RADIUS-based systems like most VPNs, or it is used with apps calling the product's REST API. The BlackBerry 2FA server is not required in deployments that use only Enterprise Identity, but it can be deployed in cases where you want to use two-factor authentication for both cloud services and the other supported systems. For more information, see the BlackBerry 2FA server compatibility matrix content, BlackBerry 2FA server installation and upgrade content, and the BlackBerry 2FA server configuration content.

Architecture: BlackBerry 2FA
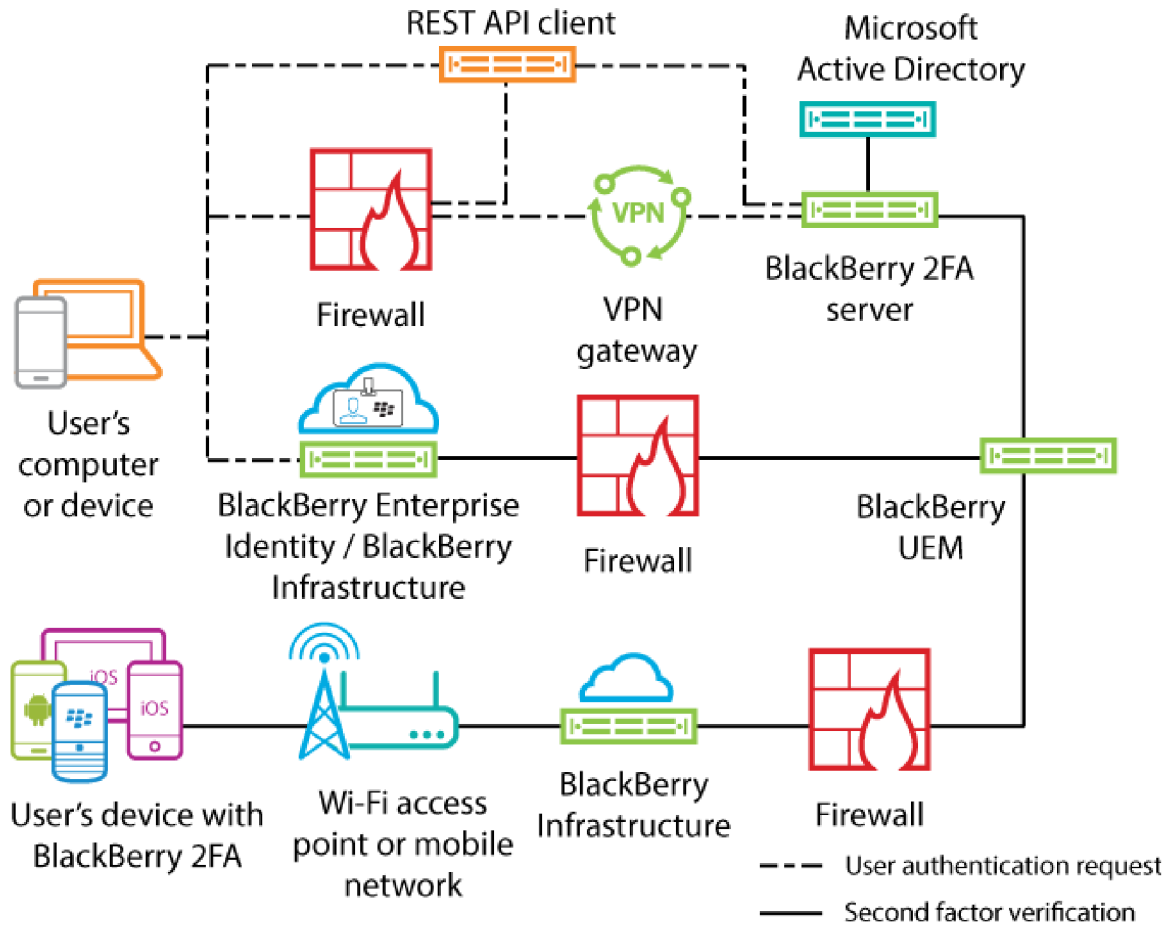
Component	Description
User's computer or device	A user's computer or device is any computer or device, from inside or outside a firewall, that is used to connect to a resource that requires two-factor authentication.
BlackBerry 2FA server	The BlackBerry 2FA server connects to BlackBerry UEM to find the devices associated with a user and to send authentication requests to the BlackBerry 2FA app that's installed on devices.
VPN gateway (optional)	The VPN gateway is a computer that accepts VPN connections to your organization's network. **Note:** This feature requires the BlackBerry 2FA server.
REST API client (optional)	The REST API client is a customer-defined, on-premises service that authenticates users who access it through the BlackBerry 2FA server's REST API. **Note:** This feature requires the BlackBerry 2FA server.

Component	Description
BlackBerry Enterprise Identity (optional)	BlackBerry Enterprise Identity provides single sign-on (SSO) to cloud services, such as Box, Salesforce, and G Suite. Enterprise Identity connects directly to the BlackBerry 2FA service in BlackBerry UEM or BlackBerry UEM Cloud.
BES12, or BlackBerry UEM, BlackBerry UEM Cloud	BlackBerry UEM also manages BlackBerry 2FA user configuration through the BlackBerry 2FA profile and the use of one-time password (OTP) tokens.
User's device with BlackBerry 2FA	For iOS and Android devices, BlackBerry 2FA is included in the BlackBerry UEM Client. For BlackBerry 10 devices, users install the BlackBerry 2FA app.

Authentication requests through BlackBerry UEM
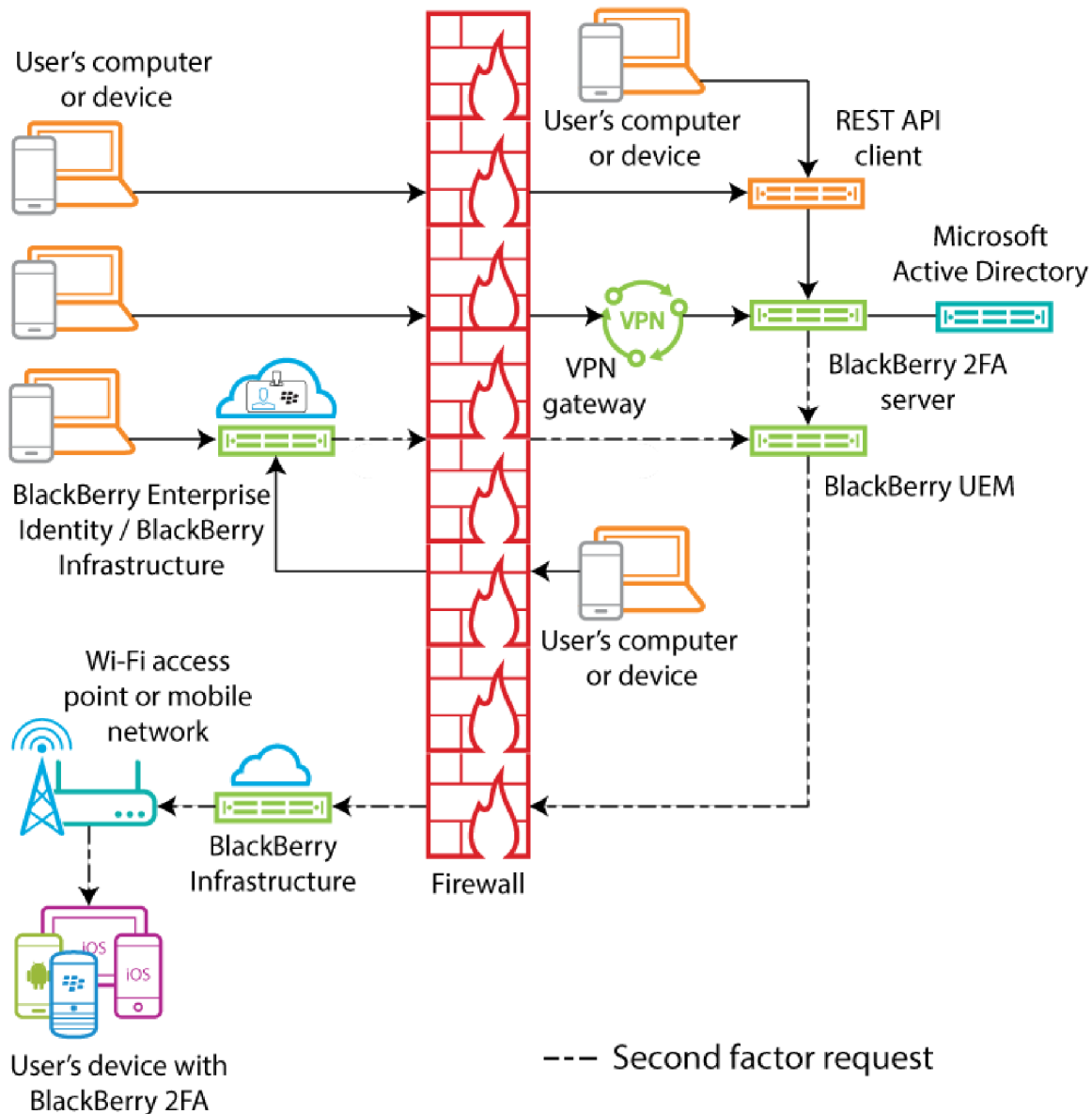
User's computer or device

User's computer or device

REST API client

Microsoft Active Directory

BlackBerry 2FA server

BlackBerry UEM

VPN

VPN gateway

BlackBerry Enterprise Identity / BlackBerry Infrastructure

Wi-Fi access point or mobile network

User's computer or device

BlackBerry Infrastructure

Firewall

User's device with BlackBerry 2FA

--- Second factor request

To initate an authentication request, a user performs one of the following actions:

- Accesses the login interface for a custom service on a computer or device at work and enters their login information
- Accesses the login interface for a custom service on a computer or device outside work and enters their login information
- Opens a VPN client on a computer or device outside work and enters their login information
- Accesses the login interface of a service that is configured to use BlackBerry Enterprise Identity for authentication on a computer or device outside work and enters their login information
- Accesses the login interface of a service that is configured to use BlackBerry Enterprise Identity for authentication on a computer or device at work and enters their login information

The user receives a prompt on their device to confirm that they want to authenticate. Depending on the authentication options configured for the user, they may be required to enter their device or secure container password before they can acknowledge the prompt.

The diagram does not show the data flow for authentication requests that use one-time password (OTP) tokens.

Authentication responses through BlackBerry UEM

In all the responses shown, the user confirms the authentication prompt on their device, and the response travels back to BlackBerry Enterprise Identity or the BlackBerry 2FA server. The user's directory password is verified if the authentication options for the user require it. After it is verified, the user receives a message on their device that the prompt response was sent successfully.

The diagram does not show the data flow of authentications using one-time password (OTP) tokens.

Authentication requests through BlackBerry UEM Cloud

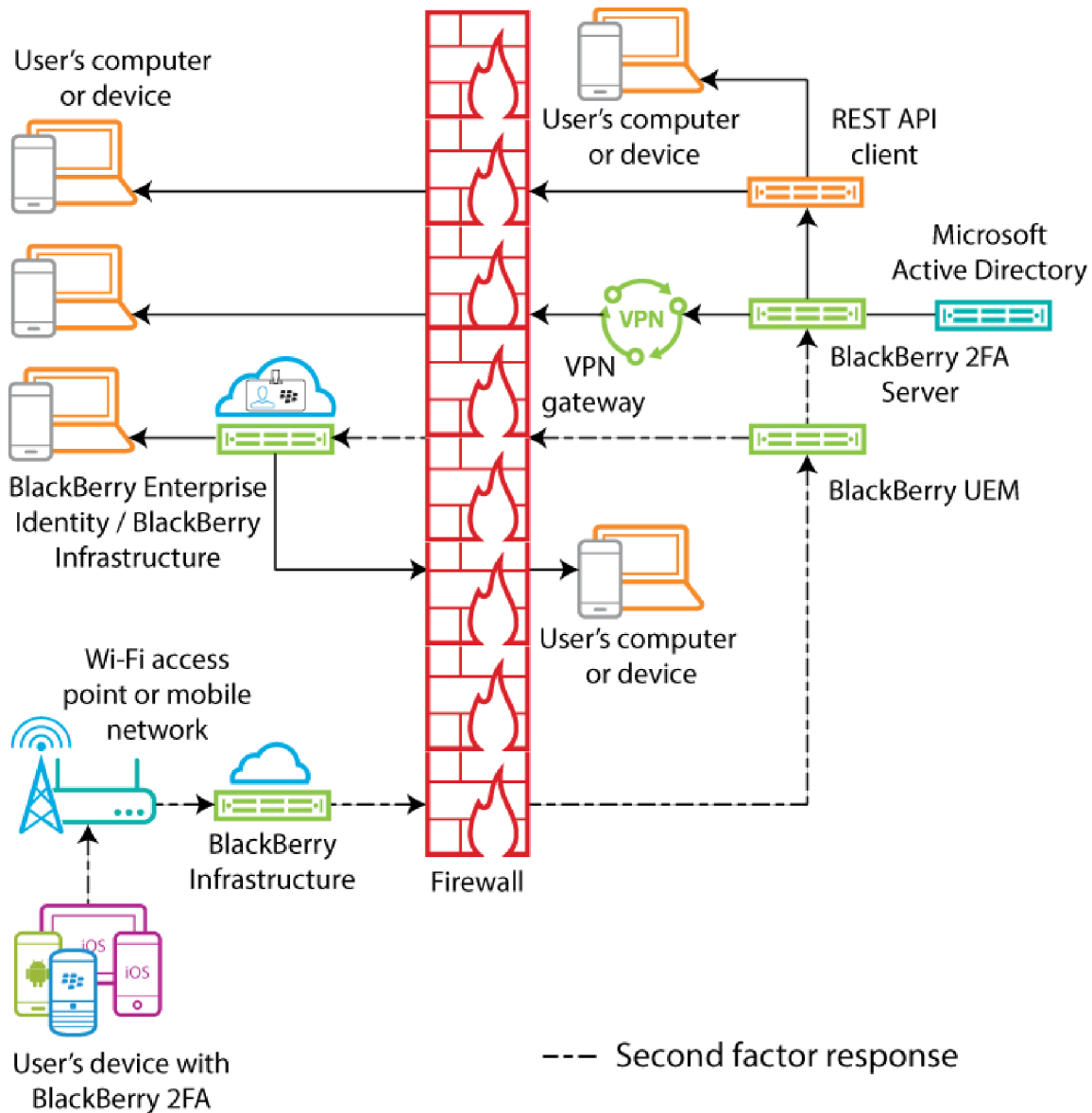To initate an authentication request, a user performs one of the following actions:

- Accesses the login interface of a service that is configured to use BlackBerry Enterprise Identity for authentication on a computer or device outside work and enters their login information
- Accesses the login interface of a service that is configured to use BlackBerry Enterprise Identity for authentication on a computer or device at work and enters their login information

The user receives a prompt on their device to confirm that they want to authenticate. Depending on the authentication options configured for the user, they may be required to enter their device or secure container password before they can acknowledge the prompt.

The diagram does not show the data flow for authentication requests that use one-time password (OTP) tokens.
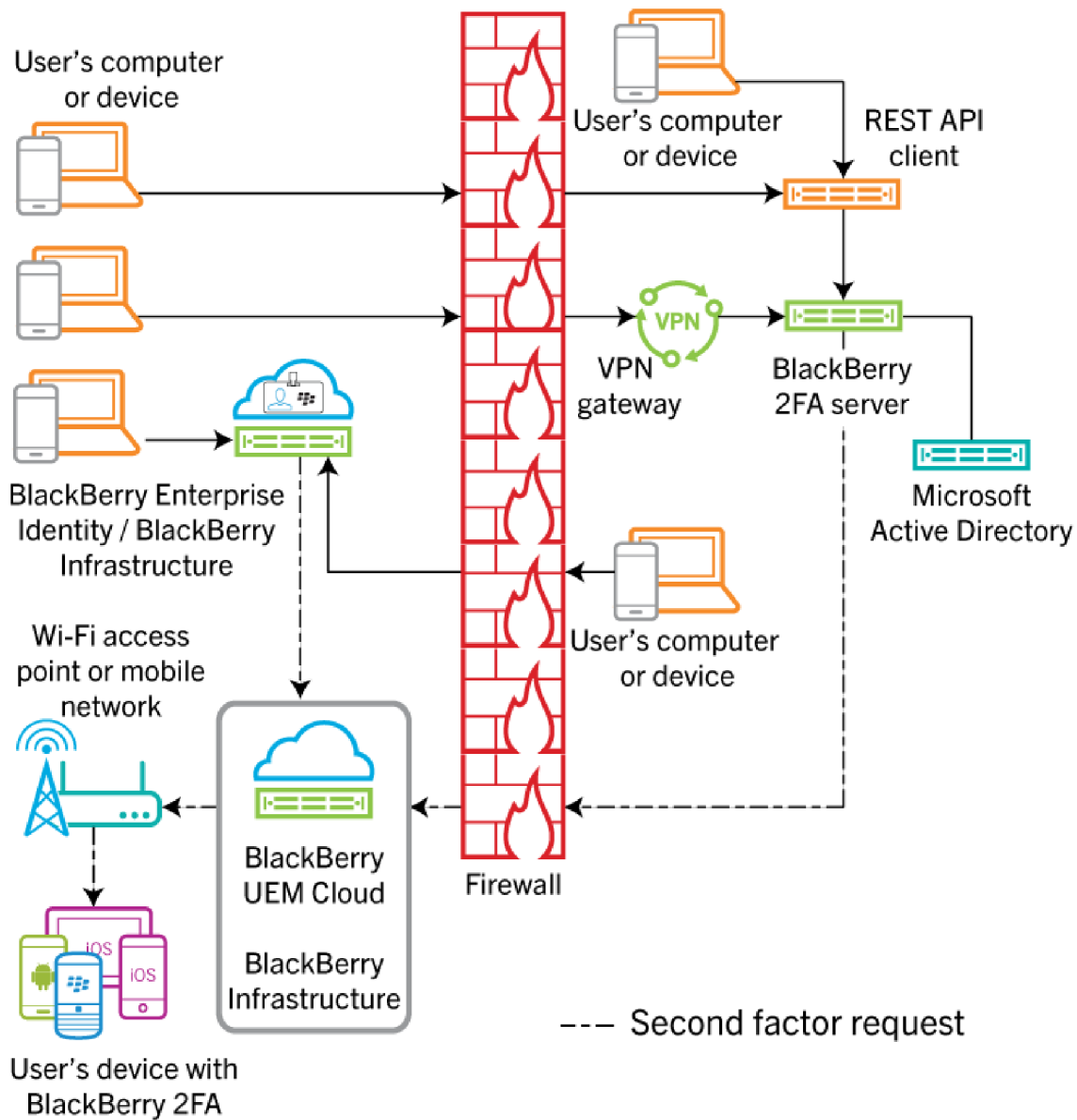
Authentication responses through BlackBerry UEM Cloud

In all the responses shown, the user confirms the authentication prompt on their device, and the response travels back to BlackBerry Enterprise Identity. The user's directory password is verified if the authentication options for the user require it. After it is verified, the user receives a message on their device that the prompt response was sent successfully.

The diagram does not show the data flow of authentications using one-time password (OTP) tokens.

Upgrading BlackBerry UEM

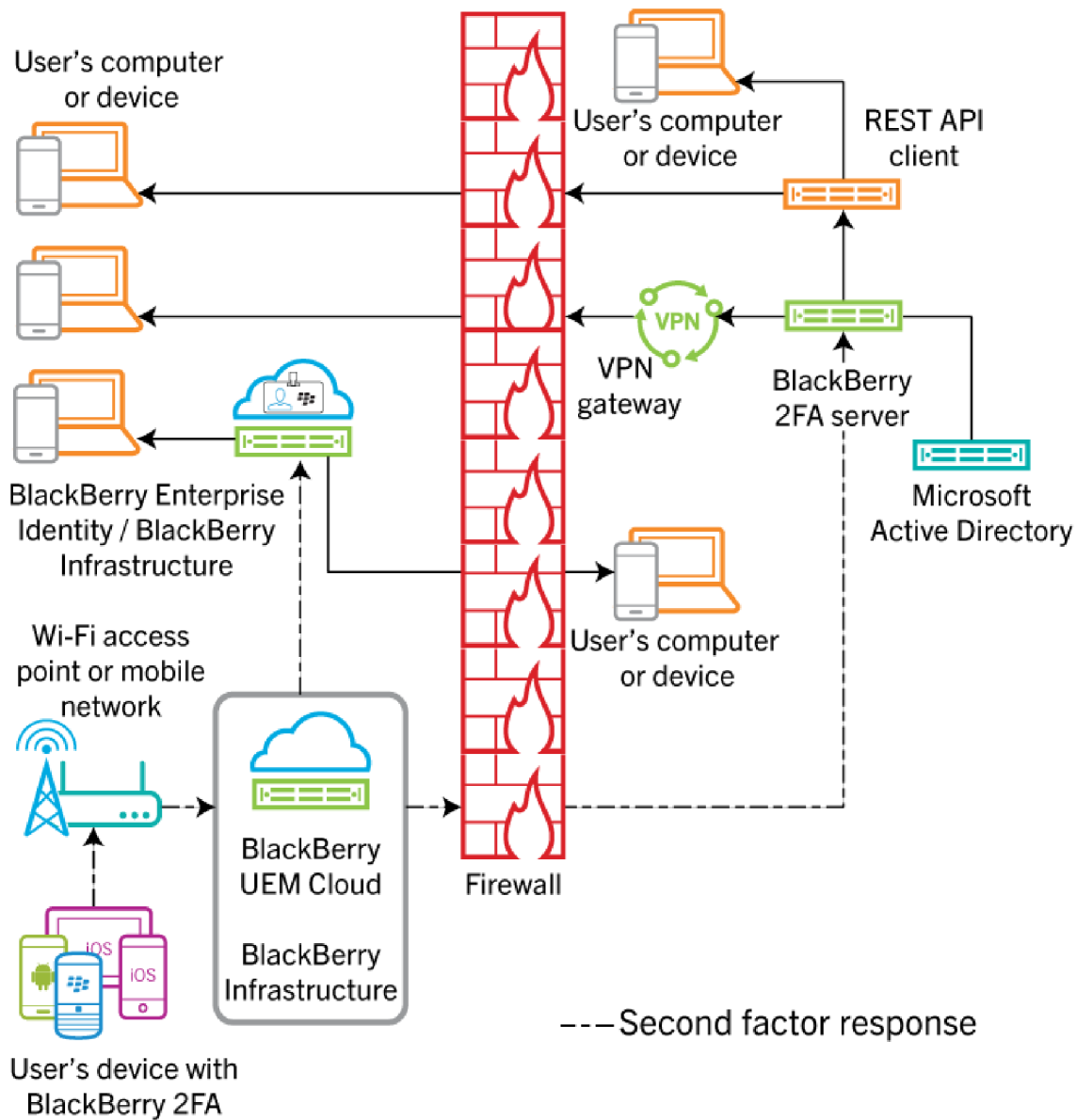If you upgrade BlackBerry UEM and you use a BlackBerry 2FA server, after the upgrade, you must restart the BlackBerry 2FA service on the 2FA server. For example, if you upgrade from BlackBerry UEM version 12.6 to 12.7 and you are running BlackBerry 2FA server 2.5, restart the BlackBerry 2FA service on the 2FA server.

For the latest compatibility information, see the BlackBerry 2FA server compatibility matrix.

BlackBerry 2FA profiles

You can use a BlackBerry 2FA profile to enable authentication for your users. To use the latest version of BlackBerry 2FA and its associated features, such as OTP hardware token support, OTP software token support, BlackBerry 2FA Direct Authentication, BlackBerry 2FA Preauthentication, and self-rescue, your users must have the BlackBerry 2FA profile assigned to them. For information about using the BlackBerry 2FA profile, see Create or modify a BlackBerry 2FA profile in BlackBerry UEM version 12.8 or earlier and Assign a BlackBerry 2FA profile to a user. For information about using BlackBerry 2FA in BlackBerry UEM, see Steps to manage BlackBerry 2FA in BlackBerry UEM .

BlackBerry 2FA for devices managed by BlackBerry UEM

You can activate devices in BlackBerry UEM so that you can manage them and use BlackBerry 2FA. A single activation task provides the device with both MDM control and BlackBerry 2FA, which simplifies device management for both users and administrators.

Any activation profile supported by BlackBerry UEM allows the use of BlackBerry 2FA. For information about using BlackBerry 2FA in BlackBerry UEM, see the Administration content for BlackBerry 2FA.

BlackBerry 2FA for devices not managed by BlackBerry UEM

If BlackBerry UEM management is not an option, or a device is already managed by another MDM solution, you can activate devices with BlackBerry UEM so that they use BlackBerry 2FA only.

Devices activated in this way are not managed by BlackBerry UEM. No work space is created on devices, no administrative control of the device is established, there is no added security for work data, and users' personal data remains private.

This option is available for iOS and Android devices only. For information about using BlackBerry 2FA in BlackBerry UEM, see the Administration content for BlackBerry 2FA.

OTP tokens

BlackBerry UEM supports the use of One-Time Password (OTP) tokens through BlackBerry 2FA service. The OTP tokens feature provides a secure authentication scheme for users who do not have a mobile device or have a mobile device that does not have sufficient connectivity to support the real-time BlackBerry 2FA device notifications. When using an OTP instead of a device notification as the second factor of authentication, the OTP is provided in the same channel as the user's password, and their mobile device is not signaled.

You can enter the OTP code with the username or the password.

- When using an OTP code with the username, after the username, you type a comma (,) then the OTP code with no spaces between them. For example, if the username is "janedoe" and code is "555123", it should be entered as "janedoe,555123". Using this method, users can easily verify the code that they entered.
- When using an OTP code with the password, the code precedes the user's password. For example, if the code is "555123" and the password is "AbCdeF", it should be entered as "555123AbCdeF".

Software tokens

You enable software OTP tokens for users in the BlackBerry 2FA profile that you assign to them. The software token can be found in the BlackBerry UEM Client app by swiping through its home screen.

Hardware tokens

To manage hardware OTP tokens in BlackBerry UEM, the user must have a BlackBerry 2FA profile assigned to them.

For more information about the latest supported hardware tokens, see the BlackBerry 2FA server compatibility matrix.

Preauthentication and self-rescue

BlackBerry 2FA Preauthentication and self-rescue are features that allow users to authenticate to your organization's resources for a predetermined period with only a single factor. These features are enabled and configured independently.

Preauthentication should be used when the user expects to have no device access or no network coverage for a short period of time (for example, when they are on an airplane). Users can request Preauthentication from the their device, or administrators can enable it through the BlackBerry UEM management console. BlackBerry recommends using the software OTP feature instead whenever possible because it retains full two-factor security, even though it is less user-friendly.

Self-rescue should be used when a user has lost their device or has no device access for a longer period of time such as a day or more (for example, the user lost their device and is waiting for a replacement). Users can access the self-rescue feature from BlackBerry UEM Self-Service, which means that it can only be enabled if the user is connected to the organization's network.

Direct Authentication

You can enable BlackBerry 2FA Direct Authentication so that when users want to authenticate to your organization's resources, they start the authentication process from their devices instead of receiving a confirmation prompt and without using a One-Time Password. When you enable Direct Authentication feature for users, users must use their directory password to log in to your organization's resources within the time limit that you specify.

Users can access the direct authentication feature from the BlackBerry UEM Client on Android and iOS devices and the BlackBerry 2FA app on BlackBerry 10 devices.

Steps to manage BlackBerry 2FA in BlackBerry UEM

To use BlackBerry UEM to manage BlackBerry 2FA, you perform the following actions:

Step	Action
1	Verify that your environment meets the device and server requirements. For more information see, System requirements: BlackBerry 2FA.
2	Optionally, install and configure the BlackBerry 2FA server. For more information, see the installation and configuration content.
3	Create a user.
4	Assign the BlackBerry 2FA app to BlackBerry 10 devices.
5	Create or modify a BlackBerry 2FA profile in BlackBerry UEM version 12.8 or earlier or Create or modify a BlackBerry 2FA profile in BlackBerry UEM Cloud or BlackBerry UEM version 12.9 or later .
6	Assign a BlackBerry 2FA profile to a user.
7	Optionally, Create an activation profile to register unmanaged devices with BlackBerry 2FA.
8	Optionally, Assign a registration-only activation profile to a user with an unmanaged device.
9	Activate a BlackBerry 10 device.
10	Activate an iOS device.
11	Activate an Android device.
12	Set or cancel Preauthentication.
13	Optionally, configure BlackBerry UEM for the use of one-time password (OTP) tokens. For more information, see Steps to manage One-Time Password hardware tokens.

System requirements: BlackBerry 2FA

Before you can use BlackBerry UEM to manage BlackBerry 2FA, you must make sure that the following requirements are met:

Item	Requirement
BlackBerry UEM or BlackBerry UEM Cloud	One of the following: • BlackBerry UEM version 12.6 or later • BlackBerry UEM Cloud For information on installing BlackBerry UEM 12.6 or later, see the BlackBerry UEM Installation and upgrade content.
BlackBerry 2FA server	• Version 2.0 or later (version 2.5 for full integration of all new BlackBerry UEM features, including OTP tokens) For more information about system requirements, see the BlackBerry 2FA compatibility matrix content. **Note:** To manage the BlackBerry 2FA server from the BlackBerry UEM management console, BlackBerry 2FA server version 2.5 is required.
BlackBerry 2FA licenses	• BlackBerry 2FA is included in the BlackBerry Enterprise Mobility Suite - Application Edition and the BlackBerry Enterprise Mobility Suite - Content Edition, and it can also be purchased separately. • BlackBerry 2FA is included in the BlackBerry Enterprise Mobility Suite - Collaboration Edition for authentication to Microsoft Office 365 and BlackBerry proprietary enterprise products only. • BlackBerry 2FA is included in all standalone BlackBerry Workspaces licenses for authentication to Workspaces only. • Contact your BlackBerry account representative to get the latest details on packaging, pricing, and licensing.
BlackBerry 10	• All versions. For more information, see the BlackBerry 2FA compatibility matrix content .
iOS	• iOS 8 and later. For more information, see the BlackBerry 2FA compatibility matrix content . • Latest version of the BlackBerry UEM Client installed. For more information, see the BlackBerry UEM Administration content .
Android	• Android 4.0.x and later. For more information, see the BlackBerry 2FA compatibility matrix content . • Latest version of the BlackBerry UEM Client installed. For more information, see theBlackBerry UEM Administration content.
Device licenses	No licenses are required for devices that use BlackBerry 2FA but are not managed by BlackBerry UEM.

Create a user

Every BlackBerry 2FA user needs to exist as user in BlackBerry UEM. Do one of the following:

- If the user is already in BlackBerry UEM, follow the instructions to set an activation password and send an activation email in the BlackBerry UEM administration content.
- If the user is not yet in BlackBerry UEM, follow these steps to create one and send an activation password to the user.

For the advanced version of this task, follow the instructions to create a user account in the BlackBerry UEM administration content.

1. In the BlackBerry UEM management console, on the menu bar, click **Users**.
2. In the left pane, click **Add user**.
3. Do one of the following:

Task	Steps
Add a directory user.	a. On the **Company directory** tab, in the search field, specify the search criteria for the directory user that you want to add. You can search by first name, last name, display name, username, or email address. b. Click 🔍. c. In the search results, select the user account.
Add a local user.	a. Click the **Local** tab. b. Type the **First name** and **Last name** for the user account. c. In the **Display name** field, make changes if necessary. The display name is automatically configured with the first and last name that you specified. d. In the **Username** field, enter a unique username for the user account. e. In the **Email address** field, enter a contact email address for the user account. An email address for the user account is required when you enable a service such as BlackBerry Workspaces or device management. f. In the **Console password** field, enter a password for BlackBerry UEM Self-Service. If the user is assigned an administrative role, they can also use the password to access the management console.

4. Perform one of the following tasks:

Task	Steps
Automatically generate an activation password for the user and send an activation email.	a. Select the **Autogenerate device activation password and send email with activation instructions** option. b. In the **Activation period expiration** field, specify the number of minutes, hours, or days that the user can activate a device before the activation password expires. c. In the **Activation email template** drop-down list, click a template to use for the activation email.

Task	Steps
Set an activation password for the user and, optionally, send an activation email.	**a.** Select the **Set device activation password** option. **b.** Enter an activation password. **c.** In the **Activation period expiration** field, specify the number of minutes, hours, or days that the user can activate a device before the activation password expires. **d.** Perform one of the following actions: **1.** To send activation instructions to the user, in the **Activation email template** drop-down list, click a template to use for the activation email. **2.** If you do not want to send activation instructions to the user, clear the **Send email with activation instructions and activation password** check box. You must communicate the activation password to the user.
Do not set an activation password for the user.	**a.** Select the **Do not set device activation password** option. You can set an activation password and send an activation email later.

5. If you use custom variables, expand **Custom variables** and specify the appropriate values for the variables that you defined.

6. Perform one of the following actions:

   - To save the user, click **Save**.
   - To save the user and create another user account, click **Save and new**.

Assign the BlackBerry 2FA app to BlackBerry 10 devices

You must perform the following task to assign the app to BlackBerry 10 devices when you are using BlackBerry UEM. For more information about assigning apps, see the BlackBerry UEM administration content.

1. Download the app from https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B and copy the .bar file to a location that the BlackBerry UEM management console can access.
2. If necessary, use the BlackBerry UEM management console to specify a shared network location for internal apps.
3. In the BlackBerry UEM management console, add the .bar file as an internal app.
4. In the BlackBerry UEM management console, assign the app to users or groups.

The app is automatically installed on any BlackBerry 10 device the user activates with a workspace.

Create or modify a BlackBerry 2FA profile in BlackBerry UEM version 12.8 or earlier

To use BlackBerry 2FA, you must create a BlackBerry 2FA profile and assign it to users.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections** > **BlackBerry 2FA**.
3. Do one of the following:

- To create a profile, click ＋.
- To modify a profile, click the name of the profile that you want to modify and click ✎.

4. Type a name for the BlackBerry 2FA profile.

5. Optionally, add a description for the BlackBerry 2FA profile.

6. Select an authentication option:

   a) Select **Two-factor authentication** if you are creating a standard BlackBerry 2FA profile.

   b) Select **Single-factor authentication using enterprise password** if you are creating a profile for users who do not have a device but need access to your organization's resources. This option is less secure because the user supplies only a directory password when they request authentication and no confirmation request to authenticate is sent. One-Time Password (OTP) tokens are not supported with this option.

7. Select a password to use with device prompt:

   a) Select **Enterprise password** if you are creating a profile for users who first need to supply their directory password when they request authentication and then receive a confirmation request on their device.

   b) Select **Passive device password** if you are creating a profile for BlackBerry 10 users who should receive a passive prompt to supply their workspace password to unlock their workspace and then receive a confirmation request for authentication on their devices. The passive prompt means that the user is not required to supply a workspace password if the device workspace is already unlocked when they request authentication.

   c) Select **Active device password** if you are creating a profile for BlackBerry 10 users who should receive an active prompt to supply their workspace password to unlock their workspace and then receive a confirmation request to authenticate on their devices. The active prompt means that the user must supply a workspace password if the device workspace is already unlocked when they request authentication.

8. Optionally, if you use the **Enterprise password** authentication policy, do any of the following:

   a) To allow users to use OTPs in the BlackBerry UEM Client app, select **Allow One-Time Password token**. Specify the length of the OTPs that are generated.

   b) To allow users to request Direct Authentication, select **Allow Direct Authentication from user's device**. Specify the duration, in seconds, that users have to compete the two-factor authentication process after they have started it on their mobile device. The maximum setting is "180."

   c) To allow users to set a self-rescue period, select **Allow self-rescue from BlackBerry UEM Self-Service**. Specify, in hours, the default and maximum time that users can access your organization's resources without needing to respond to a confirmation prompt on their devices.

   d) To allow users to set a Preauthentication period, select **Allow Preauthentication from user's device**. Specify, in hours, the default and maximum time that users can access your organization's resources without needing to respond to a confirmation prompt on their devices (the prompt will not appear).

9. Click **Add** or **Save**.

Create or modify a BlackBerry 2FA profile in BlackBerry UEM Cloud or BlackBerry UEM version 12.9 or later

To use BlackBerry 2FA, you must create a BlackBerry 2FA profile and assign it to users.

1. On the menu bar, click **Policies and Profiles**.

2. Click **Networks and connections** > **BlackBerry 2FA**.

3. Do one of the following:

   - To create a profile, click ＋.
   - To modify a profile, click the name of the profile that you want to modify and click ✎.

4. Type a name for the BlackBerry 2FA profile.
5. Optionally, add a description for the BlackBerry 2FA profile.
6. Do one of the following:
   a) Select **Authenticate with BlackBerry 2FA** if you are creating a standard BlackBerry 2FA profile.
   b) Select **Authenticate with Enterprise Password only** if you are creating a profile for users who do not have a device but need access to your organization's resources. This option is less secure because the user supplies only a directory password when they request authentication and no confirmation request to authenticate is sent. One-Time Password (OTP) tokens are not supported with this option.
7. If you selected the "Authenticate with BlackBerry 2FA" authentication mode, configure the following settings:

Setting	Description
Allow Push Authentication	This setting specifies whether to allow users to authenticate using the 2FA confirmation prompt on their device.
Require Enterprise Password	This setting specifies whether users must provide their enterprise password when logging in to your organization's resources. After a user enters their password, the user is prompted to authenticate on their device. This setting is valid only if Allow Push Authentication is selected.
Allow Preauthentication from mobile devices	This setting specifies whether to allow users to use the Preauthentication feature to authenticate to your organization's resources for a short, predetermined period. If you select this option, the feature is available for users in the BlackBerry UEM Client app home screen. Specify the default and maximum duration, in hours, that users can access your organization's resources without being prompted to authenticate on their device. This setting is valid only if Allow Push Authentication and Require Enterprise Password are selected.
Require device password if device locked	This setting specifies whether users must unlock their device before they can respond to the authentication prompt on the device. This setting is valid only if Allow Push Authentication is selected.
Require device password re-entry even if device already unlocked (BlackBerry 10 devices only)	This setting specifies whether BlackBerry 10 device users must enter their device password, even if the device is already unlocked, before they can respond to the authentication prompt on the device.

Setting	Description
	This setting is valid only if Allow Push Authentication and Require device password if device locked are selected.
Allow Direct Authentication from mobile devices	This setting specifies whether to allow users to use the Direct Authentication feature to start the authentication process on their mobile device. If you select this option, the feature is available for users in the BlackBerry UEM Client app home screen.
	You must specify the duration, in seconds, within which the users must compete the two-factor authentication process. The default setting is "120" and the maximum setting is "180."
	This setting is valid only if Allow Push Authentication is selected.
Allow One-Time Password (OTP) authentication	This setting specifies whether to allow users to use OTP codes as the second factor of authentication.
Require Enterprise Password	This setting specifies whether the user must enter their directory password together with the OTP code.
	This setting is valid only if Allow One-Time Password (OTP) authentication is selected.
Allow OTP generation on mobile devices	This setting specifies whether to generate OTP codes on their mobile device. If you select this option, users can use OTP codes that display in the BlackBerry UEM Client app home screen.
	Specify the length of the OTP codes that you want generated in the UEM Client. The default length is "6."
	This setting is valid only if Allow One-Time Password (OTP) authentication is selected.
Allow hardware OTP tokens	This setting specifies whether to allow users to use hardware OTP tokens. If you select this option, users can use OTP codes on the hardware tokens that are assigned to them.
	This setting is valid only if Allow One-Time Password (OTP) authentication is selected.
Allow Self-Rescue from BlackBerry UEM Self-Service	This setting specifies whether to allow users to use the Self-Rescue feature to authenticate to your organization's resources for a predetermined period. If you select this option, users can access the Self-Rescue feature from BlackBerry UEM Self-

Setting	Description
	Service, which users can only access if they are connected to the organization's network.
	Specify the default and maximum duration, in hours, that users can access your organization's resources without being prompted to authenticate on their device.

8. Click **Add** or **Save**.

Assign a BlackBerry 2FA profile to a user

A user must have a BlackBerry 2FA profile assigned to use BlackBerry 2FA.

Before you begin:

- Create or modify a BlackBerry 2FA profile in BlackBerry UEM version 12.8 or earlier.
- Create or modify a BlackBerry 2FA profile in BlackBerry UEM Cloud or BlackBerry UEM version 12.9 or later.

1. In the management console, on the menu bar, click **Users**.
2. Search for a user.
3. In the search results, click the name of the user.
4. In the **IT policy and profiles** section, click ✛.
5. Click **BlackBerry 2FA**.
6. In the **BlackBerry 2FA profile** drop-down list, click a BlackBerry 2FA profile.
7. If the profile type that you selected in step 6 is already assigned directly to the user, click **Replace**. Otherwise, click **Assign**.

Create an activation profile to register unmanaged devices with BlackBerry 2FA

Complete the following task to create an activation profile for users with devices that are not managed by BlackBerry UEM. These devices must be registered through BlackBerry UEM so that they can be used with BlackBerry 2FA. This activation type applies only to iOS and Android devices.

1. In the BlackBerry UEM management console, on the menu bar, click **Policies and Profiles**.
2. Click ✛ beside **Activation**.
3. Type a name and description for the profile.
4. In the **Number of devices that a user can activate** field, specify the maximum number of devices the user can activate.
5. In the **Device ownership** drop-down list, perform one of the following actions:

   - If some users activate personal devices and some users activate work devices, select **Not specified**.
   - If users typically activate work devices, select **Work**.
   - If users typically activate personal devices, select **Personal**.
6. Optionally, select an organization notice in the **Assign organization notice** drop-down list. If you assign an organization notice, users that activate iOS devices must accept the notice to complete the activation.

7. In the **Device types that users can activate** section, select the iOS and Android device types.
8. Click the **iOS** or **Android** tab and complete the following actions:
   - In the **Device model restrictions** drop-down list, select whether to allow only specified devices, or have no restrictions on device types. If you choose an option other than **No restrictions**, click **Edit**, select the devices you want to restrict or allow, and click **Save**.
   - In the **Allowed version** drop-down list, select the minimum allowed version.
   - In the **Activation type** section, select **Device registration for BlackBerry 2FA only**.
9. Click **Add**.

Assign a registration-only activation profile to a user with an unmanaged device

Complete the following task to assign an activation profile to users with devices that are not managed by BlackBerry UEM. These devices need to be registered through BlackBerry UEM so that they can be used with BlackBerry 2FA. This activation type is only available for iOS and Android devices.

Before you begin:

- Create an activation profile to register unmanaged devices with BlackBerry 2FA.

1. In the BlackBerry UEM management console, on the menu bar, click **Users**.
2. Search for a user.
3. In the search results, click the name of the user.
4. In the **IT policy and profiles** section, click ＋.
5. Click **Activation**.
6. In the **Activation profile** drop-down list, click the activation profile that you created to allow registration of unmanaged devices for use with BlackBerry 2FA.
7. If the profile that you selected in step 6 is already assigned directly to the user, click **Replace**. Otherwise, click **Assign**.

Activate a BlackBerry 10 device

Send the following activation instructions to the device user.

1. On the device, navigate to **Settings**.
2. Tap **Accounts**.
3. If you have existing accounts on this device, tap **Add Account**. Otherwise, continue to Step 4.
4. Tap **Email, Calendar and Contacts**.
5. Type your work email address and tap **Next**.
6. In the **Password** field, type the activation password you received. Tap **Next**.
7. If you receive a warning that your device could not look up connection information, complete the following steps:
   a) Tap **Advanced**.
   b) Tap **Work Account**.
   c) In the **Server Address** field, type the server address. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
   d) Tap **Done**.

8. Follow the instructions on the screen to complete the activation process.

After you finish: To verify that the activation process completed successfully, perform one of the following actions:

- On the device, navigate to the BlackBerry Hub and confirm that the email address is present. Navigate to the Calendar and confirm that the appointments are present.
- In BlackBerry UEM Self-Service, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.
- Verify the BlackBerry 2FA app automatically downloaded and installed on the user's device by checking their workspace. If not, the BlackBerry 2FA app can be downloaded from BlackBerry World for Work.

Activate an iOS device

Send the following activation instructions to the device user.

1. Install the BlackBerry UEM Client on the device. You can download it from the Apple App Store.
2. On the device, tap **BlackBerry UEM**.
3. Read the license agreement and tap **I Agree**.
4. Type your work email address and tap **Go**.
5. If necessary, type the server address and tap **Go**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
6. Confirm that the certificate details displayed on the device are correct and tap **Accept**. If your administrator sent you the certificate details separately, you can compare the information displayed with the information you received.
7. Type your activation password and tap **Activate My Device**.
8. Tap **OK** to install the required certificate.
9. Follow the instructions on the screen to complete the activation.
10. If you are prompted to enter the password for your email account or the passcode for your device, follow the instructions on the screen.

After you finish: To verify that the activation process completed successfully, perform one of the following actions:

- On the device, open the BlackBerry UEM Client and tap **About**. In the **Activated Device** and **Compliance Status** sections, verify that the device information and the activation time stamp are present.
- In BlackBerry UEM Self-Service, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.

Activate an Android device

Send the following activation instructions to the device user.

1. Install the BlackBerry UEM Client on the device. You can download the BlackBerry UEM Client from Google Play.
2. On the device, tap **BlackBerry UEM**.
3. Read the license agreement and tap **I Agree**.
4. Type your work email address and tap **Next**.
5. If necessary, type the server address and tap **Next**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.

6. Confirm that the certificate details displayed on the device are correct and tap **Accept**. If your administrator sent you the certificate details separately, you can compare the information displayed with the information you received.
7. Type your activation password and tap **Activate My Device**.
8. Tap **Next**.
9. Tap **Activate**.

After you finish: To verify that the activation process completed successfully, perform one of the following actions:

• On the device, open BlackBerry UEM Client and tap **About**. In the **Activated Device** section, verify that the device information and the activation time stamp are present.
• In BlackBerry UEM Self-Service, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.

Set or cancel Preauthentication

Complete the following task if your organization controls BlackBerry 2FA Preauthentication through IT service requests or you want override the existing Preauthentication settings for a user.

Before you begin:

• Verify that the user has a BlackBerry 2FA profile assigned.

1. In the BlackBerry UEM management console, on the menu bar, click **Users**.
2. Search for a user.
3. In the search results, click the name of the user.
4. In the user summary, click **Enable bypass for BlackBerry 2FA**
5. In the **Set bypass period** dialog box, specify, in hours, how long the user can access your organization's resources without responding to a confirmation prompt on their device or submitting a One-Time Password from a token.
6. Click **Save**. The duration is displayed in the user summary.
7. Optionally, click **Cancel** in the user summary to end the Preauthentication period. Users can also end the Preauthentication period by clicking **Expire now** in BlackBerry UEM Self-Service.

Steps to manage One-Time Password hardware tokens

To use the one-time password (OTP) tokens feature, you perform the following actions:

Step	Action
1	Enable the OTP tokens feature.
2	If necessary, to convert a token information file from a .xml file in PSKC format to a .csv file that you can import into BlackBerry UEM, Use the BlackBerry 2FA Token Conversion Tool. For more information, see Modifying the CSVConfig configuration file.
3	Import OTP tokens into BlackBerry UEM
4	Assign an OTP token to a user

Enable the OTP tokens feature

1. On the menu bar, click **Settings** > **External integration** > **One-Time Password tokens**.
2. Click **Enable**.
3. Click **Enable**.

Disable the OTP tokens feature

1. On the menu bar, click **Settings** > **External integration** > **One-Time Password tokens**.
2. Click **Disable One-Time Password token management**.
3. If neceassary, remove the OTP tokens from BlackBerry UEM. For more information, see Remove an OTP token from BlackBerry UEM .

Supported One-Time Password hardware tokens

BlackBerry 2FA currently supports the following One-Time Password (OTP) hardware tokens from third-parties:

- RCDevs RC200
- Vasco DIGIPASS GO 6
- Feitian OTP C200

Support for more hardware tokens will be included in upcoming releases. For the latest hardware token compatibility information, see the server compatibility matrix.

Use the BlackBerry 2FA Token Conversion Tool

Note: This tool is only available and required for BlackBerry UEM 12.7. For BlackBerry UEM 12.8 and later and BlackBerry UEM Cloud, the token information files can be imported directly into UEM without using the tool.

Use the BlackBerry 2FA Token Conversion Tool to convert a token information file from a .xml file in PSKC format to a .csv file that you can import into BlackBerry UEM. When the file conversion is successful, the generated file is automatically saved in the same folder as the tool.

For Vasco and Feitian tokens, you must use the BlackBerry 2FA Token Conversion Tool to convert the token information files that the token manufacturer provides to a format that BlackBerry UEM can read.

The BlackBerry 2FA Token Conversion Tool only supports token information files in the Portable Symmetric Key Container (PSKC) format. For more information about PSKC, see https://tools.ietf.org/html/rfc6030.

Important: The generated file contains token information in unencrypted form. It is highly recommended that you only run the BlackBerry 2FA Token Conversion Tool in a secure computer environment, and delete the generated file immediately after it is imported into BlackBerry UEM.

Before you begin:

- Download the BlackBerry 2FA Token Conversion Tool at https://swdownloads.blackberry.com/Downloads/entry.do?code=0C52D419A421FB13BB58357E67B7FB4B.
- Place the token information files that you want to convert in the same folder as the tool.

1. Open the command line.
2. Browse to the directory of the BlackBerry 2FA Token Conversion Tool.
3. Run **tokenConversionTool-*\<version\>*.jar** with the following parameters:

Parameter	Description
-h	To display the help usage message.
-v	Optionally, enable verbose mode. If you enable verbose mode, the token information in the specified file is displayed in the command line.
-f	Optionally, specify the format that you want to convert to ('basic' or 'rcdevs'). The default is 'rcdevs.'
-p	If necessary, specify the token key that is required to decrypt the token information file. The password is a sequence of bytes in hexadecimal format (e.g. A12BC34D).
filename	Specify the file that you want to convert. The file must be in the same folder as the tool. This parameter is required.

For example, type one of the following:

- `java -jar <toolName>.jar -f basic -p <password> ./<tokenFileName>.xml`
- `java -jar tokenConversionTool-1.0.4.jar ./vasco.xml`

The output file path appears when the file is successfully generated.

After you finish: Import the generated token information file to the BlackBerry UEM management console. For more information, see Import OTP tokens into BlackBerry UEM.

Modifying the CSVConfig configuration file

The .csv file containing token data requires a configuration file (CSVConfig.json) that defines how the .csv file is parsed by BlackBerry UEM. The .csv file must be parsed correctly before the token data is extracted and imported into the BlackBerry UEM database.

The first time that you log in to BlackBerry UEM after you enable the OTP tokens feature, a default CSVConfig.json file is generated. The file is generated with default values and saved in "BESNG_HOME"/otp/config/CSVConfig.json (or C:\otp\config\CSVConfig.json).

The following information will help you modify your CSVConfig.json file to make sure your .csv file is parsed correctly by BlackBerry UEM.

- The recommended setting for "extension" is "CSV."
- The recommended setting for "stripSpacesAndQuotations" is "true." All spaces and quotes from the columns are removed.
- Columns for each data field can have a maximum of four parameters to determine how BlackBerry UEM will parse and extract the data from the respective column.

  - "column" determines column number in the .csv file. Columns start at "0."
  - "startCharPos" determines where the token data in the column starts. If "stripSpacesAndQuotations" is set to "true," only the characters before the start of the actual token data are counted, and not spaces and quotation marks.
  - "endCharPos" determines where the token data in the column ends. If "stripSpacesAndQuotations" is set to "true," only the characters before the end of the actual token data are counted, and not spaces and quotation marks.
  - "encoding" determines character encoding/decoding used. "base64" is standard.

The following is an example of a CSVConfig.json file updated to parse a .csv file populated with RCDevs token information:

```
{
    "extension" : "CSV",
    "stripSpacesAndQuotations" : true,
    "startRow" : 4,
    "token_serial_number" : {
        "column" : 1,
        "startCharPos" : 0
    },
    "password_seed" : {
        "column" : 3,
        "startCharPos" : 9,
        "encoding" : "base64"
    },
    "password_length" : {
        "column" : 6,
        "startCharPos" : 10,
        "encoding" : "base64"
    },
    "time_step" : {
        "column" : 7,
        "startCharPos" : 13,
        "encoding" : "base64"
    },
```

```
    "vendor" : {
        "column" : 2,
        "startCharPos" : 0,
        "endCharPos" : 6
    },
    "model" : {
        "column" : 2,
        "startCharPos" : 6,
        "endCharPos" : 14
    },
    "t0" : {
        "column" : 5,
        "startCharPos" : 11,
        "encoding" : "base64"
    }
}
```

The following is a plaintext example of a .csv file populated with RCDevs token information:

```
1 # Inventory Import File for RCDevs WebADM
2 # Generated on June 29, 2016, 2:40 pm
3
4 Type                    Reference                Description                    Data
5 "OTP Token", "2308602200271", "RCDevs RC200-T6",
  "TokenKey=P6chCRszGaawHhpzWUHCS8Ua8WE=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TO
6 "OTP Token", "2308602200272", "RCDevs RC200-T6",
  "TokenKey=Zghe8fbekGOXpwGM2vmEcZyZnaE=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TO
7 "OTP Token", "2308602200273", "RCDevs RC200-T6",
  "TokenKey=EH//86f6pnup3F4AS7w7HNazYjU=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TO
8 "OTP Token", "2308602200274", "RCDevs RC200-T6", "TokenKey=tzrVqKFMns9/
rbAyCYCdDxb04Ig=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TOTPTimeStep=MzA="
9 "OTP Token", "2308602200275", "RCDevs RC200-T6", "TokenKey=0FuZ/
A6ZCVGClaYW3EFCtXWNFFk=,TokenType=VE9UUA==,TokenState=MA==,OTPLength=Ng==,TOTPTimeStep=MzA="
```

Import OTP tokens into BlackBerry UEM

To import OTP tokens, you need a .csv (comma delimited) file that contains information about the tokens. The.csv file is read by BlackBerry UEM using a configuration file (CSVConfig.json).

Before you begin: You need to modify the default CSVConfig.json file so that BlackBerry UEM can correctly parse and then store the token information in the database. For more information, see Modifying the CSVConfig configuration file.

1. On the menu bar, click **Settings** > **External integration** > **One-Time Password tokens**.
2. Click **Browse**.
3. Navigate to and select the .csv file that contains the information about the tokens.
4. Click **Upload**.

Remove an OTP token from BlackBerry UEM

1. On the menu bar, click **Settings** > **External integration** > **One-Time Password tokens**.
2. Search for and select the serial number of the token that you want to remove.

3.

Click 🗑 .

4. Click **Delete**.

Assign an OTP token to a user

Before you begin: Assign a BlackBerry 2FA profile to a user.

1. On the menu bar, click **Users**. Search for and select the name of the user.
2. On the user detail page, click **One-Time Password Tokens**.
3. Search for and select the serial number of the token that you want to assign to the user.
4. Click **Assign**.

Remove an OTP token from a user

1. On the menu bar, click **Users**. Search for and select the name of the user.
2. On the user detail page, click **One-Time Password Tokens**.
3. Under **Assigned tokens**, click **Remove** .
4. Click **Submit** to unassign the One-Time Password token.

Automatically accommodate out-of-sync hardware tokens

You can adjust the time-step window for hardware tokens to automatically accommodate token drift. When the internal clock of the hardware token drifts too far from the correct time, the token displays invalid codes. If you increase the time-step window, any code within that window is valid, even if the token is out of sync.

For example, if you set the time-step window to "2", the code that is displayed on the token is accepted as a valid code if it precedes or follows the expected code by two refresh intervals. In this example, if the code displayed on the token is the third code preceding or following the expected code, the code would be considered invalid and the One-Time Password would be rejected.

This setting adjusts the time-step window for all hardware tokens. Adjust the time-step window according to the number of refresh intervals by which you think the tokens are out of sync.

1. In the management console, click **Settings > External Integration**.
2. Click **BlackBerry 2FA one-time password tokens**.
3. In the **Time-step window** field, click ✏.
4. Enter a value between 0 and 50. The default value is 3. To accept only the expected code, which may or may not match the code displayed on the token, set the time-step window value to 0.
5. Click **Update**.

Manually resync a hardware token

If a one-time password hardware token that is assigned to a user is not usable because the drift was not automatically accommodated, you can try to manually resync the token. To manually resync a token with BlackBerry UEM, the user needs to give you two new consecutive codes.

1. On the menu bar, click **Users**. Search for and select the name of the user.
2. Click **One-time password tokens**.
3. In the **Assigned token** section, click **Resync**.
4. In the **Time-step window** field, enter the maximum number of time-steps that you want to resync to for the out-of-sync token.
5. In the **First token code** field, enter the code that displays on the token.
6. In the **Second token code** field, enter the next consecutive code that displays on the token.
7. Click **Resync**.

Logging and reporting

BlackBerry UEM generates logs for the preauthentication and self-rescue features in BlackBerry 2FA. The logs are stored in the BlackBerry UEM Core (CORE) log file.

In addition to logging information for general troubleshooting purposes, BlackBerry UEM generates special log lines for preauthentication and self-rescue activity for auditing purposes. You can extract theses log lines to monitor the overall usage of the preauthentication and self-rescue features. These log lines are logged at the INFO level and consist of comma-separated data that is prefixed by universal CORE log information that can be discarded.

These special log lines are tagged with markers that allow you to extract them easily. Two types of activity are monitored: preauthentication requests and authentication requests while the user is preauthenticated. When you extract these lines and discard the universal CORE log information, you can open the comma-delimited data in any software that supports the CSV format. For more information about loggining and reporting, see the BlackBerry UEM maintenance and monitoring content.

Auditing Preauthentication requests

BlackBerry UEM logs each request for BlackBerry 2FA Preauthentication and each request for authentication while in Preauthentication. Data is logged when the request completes or expires.

The audit log file includes the following information about each request for Preauthentication:

- Marker1: BB2FA_AUDIT. This is the identifier for all BlackBerry 2FA audit log lines in the BlackBerry UEM Core log. This also indicates where to trim the log lines to discard universal CORE log information.
- Marker2: PREAUTH_REQUEST. This is the identifier for the event type (request for Preauthentication).
- Date
- Time
- Source: BlackBerry UEM management console, BlackBerry UEM Self-Service, user's device
- Username
- BlackBerry 2FA profile name: The name is logged in quotation marks to prevent the field from being split by commas in the profile.
- Requested Preauthentication duration in hours
- Configured maximum Preauthentication duration in hours
- Result: SUCCESS, FAILED_INVALID_REQUEST
- Preauthentication expiration time

For example:

```
2BB2FA_AUDIT,PREAUTH_REQUEST,2016-11-05,13:27:17.822,admin,user1,"Sales BB2FA
Profile",3,12,May 11 16:41
```

The audit log file includes the following information about each request for authentication while in Preauthentication:

- Marker1: BB2FA_AUDIT. This is the identifier for all BlackBerry 2FA audit log lines in the BlackBerry UEM Core log. This also indicates where to trim the log lines to discard universal CORE log information.
- Marker2: AUTH_USER_IN_PREAUTH. This is the identifier for the event type (request for authentication while inPreauthentication).
- Date
- Time

- Transaction ID
- Source: BlackBerry 2FA app, BlackBerry Enterprise Identity, and so on.
- Username
- Authentication policy: enterprise password, active device password, passive device password
- Profile name: The name is logged in quotation marks to prevent the field from being split by commas in the profile.
- Preauthentication expiration time

For example:

```
BB2FA_AUDIT,AUTH_USER_IN_PREAUTH,2016-11-05,13:27:17.822,50dbe1cc,BB2FA,user1,Enterprise
 Password,"Sales BB2FA Profile",May 11 16:41
```

Legal notice

SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES 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
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada