BlackBerry UEM Client for iOS

User Guide

Contents

Getting started with BlackBerry UEM Client

You use the BlackBerry UEM Client to activate your device for work. When you activate your device, the device is associated with BlackBerry UEM and is granted access to work data and the productivity apps that your administrator assigned to your device. Your administrator determines the degree of protection for your device based on your role and assigns IT policies and profiles to make sure the appropriate device features are available to you and to secure work data on your device.

You can download the BlackBerry UEM Client for iOS devices from the App Store.

Activate your iOS device

Your device is ready to be activated when you receive an activation email from your administrator.

The activation email includes the information that you need to activate your device. If your activation password has already expired, create a new password in BlackBerry UEM Self-Service or contact your administrator.

If you received an activation QR Code in the activation email, you can use it to activate your device. When you activate a device with a QR Code, you don't need to type any information.

1. Install the BlackBerry UEM Client from the App Store.
2. Open the UEM Client.
3. Read and accept the license agreement.
4. Do one of the following:

Task	Steps
Use a QR Code to activate your device	a. Tap . b. Scan the QR Code in the activation email.
Manually activate your device	a. Type your work email address. This is the email address where you received the activation email. Tap **Go**. b. If necessary, type the server address found in your email and tap **Activate my Device**. c. Type your activation password and tap **Activate My Device**. If your activation password is expired, create a new password in BlackBerry UEM Self-Service or contact your administrator.

5. Tap **Allow** to allow the UEM Client to send you notifications. Choosing **Don't Allow** prevents the device from activating completely.
6. When you are prompted to install a certificate, tap **OK**.
7. When you are prompted to download the configuration profile, tap **Allow**.
8. After the download is complete, open **Settings**.
9. Tap **General** and navigate to **Profiles and Device Management**.
10. To install the profile, tap **UEM Profile** and follow the instructions on the screen.
11. After the installation is complete, return to the BlackBerry UEM Client app to complete the activation.
12. If you are prompted, follow the instructions on the screen to install work apps on your device.

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

- In the UEM Client, tap **About**. In the **Activated Device** section, verify that the device information and the activation time stamp are present.
- In the BlackBerry UEM Self-Service console, 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.

Install or update work apps

If a required app is not installed, your administrator may restrict or remove access to work data. Optional apps are apps that your administrator recommends, but you are not required to install them on your device.

When you download a required app or an optional app that you use for work purposes, you might have to pay for the app and then reclaim the cost from your organization.

Before you begin: Activate your device

1. In the BlackBerry UEM Client app, tap **Work apps**. If there is no Work apps tab, go to your device's home screen and open the **Work apps** app.
2. Do one of the following:
   - To install work apps, tap the **Required** tab and install all required apps, then tap the **All** tab and install any optional apps that you want.
   - To update work apps, tap the **New** tab and tap **Update** beside each app that you want to update.

Setting up work email

After you activate your device, you may receive a notification to set up your work email. Follow the instructions on the screen and complete the setup. If your work email is not automatically configured, contact your administrator for more information.

Using BlackBerry UEM Self-Service

You can use the BlackBerry UEM Self-Service console to set activation passwords, manage BlackBerry Dynamics apps, preauthenticate your devices, and perform basic commands such as lock a device or change a device password. For more information about using BlackBerry UEM Self-Service, see the BlackBerry UEM Self-Service user guide.

Using BlackBerry 2FA

If your administrator enabled BlackBerry 2FA on your device, your device can be used as the second factor of authentication to access your organization's resources. This helps make sure that only authorized users are accessing your organization’s resources. For example, after you enter your directory password to access resources, you are immediately prompted on your device to confirm the connection.

The first factor is your directory password. The second factor can be one of the following:

- A prompt that you must confirm on your device before it expires.
- A one-time password that you enter at the same time as you enter your username or directory password.

On the BlackBerry UEM Client home screen, swipe left or right to access any BlackBerry 2FA features that your administrator has enabled for you.

Use direct authentication

If your administrator has configured BlackBerry 2FA for your device and has enabled the direct authentication feature for your device, you can pre-emptively authenticate from the BlackBerry UEM Client before you log in to access your organization's resources. When you use direct authentication, you must use your directory password to log in to your organization's resources within the time limit that your administrator specifies. You can use the direct authentication feature to authenticate to your organization's resources instead of receiving a confirmation prompt and without using a one-time password.

1. On the BlackBerry UEM Client home screen, swipe to the **Direct Authentication** screen.
2. Tap **Authenticate now**.
   A success message appears when authentication is successful.

After you finish: Log in to your organization's resources using your directory password within the time limit specified on the **Direct Authentication** screen.

Use a One-Time Password

If your administrator has configured BlackBerry 2FA for your device and has enabled the One-Time Password feature for your device, you can use the One-Time Password that appears in the BlackBerry UEM Client when you log in to access your organization's resources. You enter the One-Time Password together with your username or directory password. You can use a One-Time Password when your device cannot receive confirmation prompts because it doesn't have sufficient network connectivity.

1. On the BlackBerry UEM Client home screen, swipe to the **One-Time Password** screen.
2. Make note of the One-Time Password. Each One-Time Password expires after 30 seconds.
3. On the computer or device that you're trying to access work resources from, do one of the following:
   - In the **Username** field, enter your username, a comma (,), then the One-Time Password. Only a comma (no spaces) separates your username and One-Time Password. For example, if your username is "janedoe" and the One-Time Password is "555123", type "janedoe,555123".
   - In the **Password** field, enter the One-Time Password in front of your directory password (without spaces or characters separating them). For example, if the One-Time Password is "123456" and your directory password is "qweRTY", type "123456qweRTY".

Preauthenticate your device

If your administrator has configured BlackBerry 2FA for your device, you can request preauthentication from the BlackBerry UEM Client. Preauthentication allows you to access work resources for a predetermined period without being prompted for confirmation or a password on your device. You can use the preauthentication feature when you know you won't have access to your device, when you know you will be out of mobile coverage, or when you are only able to connect one device to a wireless network or hotspot. For example, if you can only connect one device to a network at a time, you can preauthenticate on your mobile device, and then log in to your work resources from the other device.

You can also preauthenticate your device from the BlackBerry UEM Self-Service console. For more information about using BlackBerry UEM Self-Service, see the BlackBerry UEM Self-Service user guide.

1. On the BlackBerry UEM Client home screen, swipe to the **Preauthentication** screen.
2. Tap **Request preauthentication**.
3. Enter the number of hours that you want to be preauthenticated for. Your administrator specifies the maximum number of hours that you can preauthenticate for.

4. Tap **Request**.
   A confirmation screen displays the expiration date and time of preauthentication.
5. Tap **Close**.

Check out and check in shared devices

If your administrator assigns you a device that you will share with other users, you check out the device when you want to use it. When you are done using the device, you can check it in so that the device is available for the next user.

1. Open the UEM Client.
2. If necessary, read and accept the terms of service.
3. Perform one of the following tasks:

Task	Steps
Check out a device.	**a.** To change the authentication option, tap the drop-down list and do the following: 1. In the drop-down list, select **Microsoft Active Directory** or **Local authentication**. 2. Tap **Done**. **b.** If you selected **Microsoft Active Directory**, type your organization's domain. **c.** Type your username and password. **d.** Tap **Check Out**. **e.** Tap **OK**.
Check in a device.	**a.** Tap **Check In**. **b.** Tap **OK**.

About device compliance

You can tap the compliance status on the BlackBerry UEM Client home screen to view the compliance report. The compliance report lists the policies that your organization is enforcing on your device.

If your device is out of compliance, and the compliance issue is not resolved before the date displayed in the compliance report, your administrator may restrict or block your device from accessing work resources and networks. If you do not know how to resolve the issue, contact your administrator.

Here are some compliance policies that your organization may enforce:

- **Rooted or jailbroken status:** If your device is rooted, it means that you or someone else ran software or performed an action on the device that allows root access to the operating system of the device. You or your administrator might have to remove the rooting software from the device or perform some actions on the device to restore the device to the default state.
- **Password:** The password on your device must meet the complexity requirements that your organization specifies.
- **Device model:** Your organization might allow only specific device models to be activated for work. You must use a device that meets the security requirements for your organization.
- **OS version:** Your organization might allow only devices that are running specific versions of Android OS to be activated for work.
- **Security patch level:** Security patches are distributed by your device manufacturer and can be found when you check for system updates on your device. Install the latest security patch available for your device model.
- **Device out of contact:** A device is out of contact if BlackBerry UEM cannot contact it after a specific length of time. For example, your device might become out of contact if it does not have a network connection.
- **Required work apps installed:** The required apps that your organization wants you to install on your device are displayed on the Assigned work apps screen. Your administrator can detect when required apps are not installed and may restrict your access to work data if the required apps are not installed. If a work app has an update available, you should install it on your device.
- **Nonassigned or restricted apps installed:** If you installed an app on your device that is not a required app or an optional app assigned to you for work purposes, you need to remove the app from your device. Any restricted apps will need to be removed from your device.

About IT policies

An IT policy is a set of rules that control the security features and behavior of your device. For example, if your organization requires that you set a password for your device, your administrator applies an IT policy to your device that includes a rule that requires you to set a password. On the home screen, you can tap the IT policy icon to see the rules that are applied to your device.

You cannot change or turn off an IT policy rule. The IT policy rules that are applied to your device are part of the overall security policy of your organization. For more information, contact your administrator.

About profiles

Profiles permit you to access work resources on your device. For example, your administrator assigns profiles to your user account so that you can access your work email account, Wi-Fi connections, VPN connections, and security certificates.

On the home screen, you can tap the Assigned Profiles section to view profiles that are assigned to your device. Note that only profiles that are applicable to the BlackBerry UEM Client are displayed.

About certificates

Certificates are used to authenticate your device to access work resources and networks.

If your administrator assigns a certificate profile to your user account, you receive a prompt on your device to install the certificate. Record the information displayed in the prompt and follow the instructions to install the certificate. If you are prompted to enter a password that is not provided, contact your administrator.

Import Entrust certificates

If your administrator assigned Entrust smart credentials to you, you must activate them from the Entrust IdentityGuard self-service portal and then import the certificates to the Profiles screen in the BlackBerry UEM Client.

Before you begin:

- Activate your device with the BlackBerry UEM Client.

1. Log in to the Entrust IdentityGuard self-service portal.
2. Obtain the QR Code and password from the Entrust IdentityGuard self-service portal.
   a) Click **I'd like to activate or update my smart credential**.
   b) Select the **I'd like to activate or update my smart credential** option again. Click **Next**.
   c) Select one of the smart credentials that you want to use. Click **OK**.
   d) Select the **I'm activating a mobile smart credential identity hosted on my mobile device** option. Click **Next**.
   e) Select **Activate my smart credential by having my mobile device use its associated data network.** option. Click **Next**.
   f) In the **Identity Name** field, type a name. Click **OK**.
   A QR Code and a password appears.
3. On the device, open the UEM Client.
4. Tap **Profiles > Import certificates**.
5. Beside the Entrust smart credentials, tap **Activate**.
6. Tap the camera icon and scan the QR Code from the Entrust IdentityGuard self-service portal.
7. Enter the password from Entrust IdentityGuard self-service portal. Click **OK**.
   An "Activating. Please wait" message appears. This may take a few minutes.
8. A success confirmation message appears. Click **OK**.

About privacy information

The Privacy information menu allows you to view what information the IT administrator can see and cannot see about your device. The menu also lists the actions that the administrator can perform on your device, as well the actions the administrator cannot perform.

Note: The Privacy information menu is available for all activation types except for BlackBerry 2FA activations.

Note: The Privacy information menu is available only if your device was activated against BlackBerry UEM version 12.11.

About rating and reviewing apps

Your administrator can allow you to rate apps, provide reviews of apps, and see reviews provided by other users. You can rate an app without a review, but you must include a rating when you provide a review of the app. After you rate and provide a review of an app, you can change or delete your rating and review.

Change your BlackBerry Dynamics app password

If your administrator allows BlackBerry UEM Client to authenticate other BlackBerry Dynamics apps, you can change your BlackBerry Dynamics app password in the BlackBerry UEM Client. You can use your BlackBerry Dynamics app password to activate and access apps protected by BlackBerry Dynamics.

1. On the BlackBerry UEM Client home screen, tap .
2. Tap .
3. Tap **Change application password**.
4. Type your current password.
5. Type and confirm the new password.
6. Tap **OK**.

Upload log files to BlackBerry Support

If requested by BlackBerry Support, you can upload log files to help troubleshoot an issue you are having with BlackBerry Dynamics apps.

1. Tap to open the BlackBerry Dynamics Launcher.
2. Tap .
3. In the **Support** section, click **Upload Logs**. The Log upload status bar displays the upload progress.
4. Click **Close**.

Deactivate your device

If you do not want your administrator to manage your device you can deactivate your device. If you deactivate your device, you remove the connection between your device and your work resources. You cannot connect to your work email account or calendar and you cannot access your work Wi-Fi connection or VPN connection after you deactivate your device.

Before you begin: Make sure that your device is connected to the wireless network.

1. On the BlackBerry UEM Client home screen, tap **About**.
2. Tap **Deactivate**.
3. Tap **OK**.

After you finish: Delete the BlackBerry UEM Client

Delete the BlackBerry UEM Client

If you delete the BlackBerry UEM Client from your device, you cannot activate your device.

Before you begin: Deactivate your device.

1. Touch and hold the **BlackBerry UEM Client** icon.
2. Tap the **x** in the upper corner of the icon.
3. Tap **Delete**.

After you finish: If you want to activate your device, reinstall the BlackBerry UEM Client on your device. You might need a new activation password. Use BlackBerry UEM Self-Service to create an activation password, or contact your administrator.

Legal notice

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

Published in Canada