BlackBerry UEM for dark sites

Installation and Administration Guide

12.11

Contents

About BlackBerry UEM for dark sites

BlackBerry UEM is a multiplatform EMM solution from BlackBerry that provides comprehensive device, application, and content management with integrated security and connectivity.

In environments with the highest security requirements, connecting to outside sites such as the BlackBerry Infrastructure may be restricted or impossible. BlackBerry UEM for dark sites was designed to provide a secure mobile device management solution without requiring BlackBerry UEM to connect to the BlackBerry Infrastructure and other services on the Internet.

Supported BlackBerry UEM features

The following BlackBerry UEM features are supported in a dark site environment.

Feature	Description
Multiplatform device management	You can manage BlackBerry 10, Samsung KNOX, and iOS devices.
Trusted and secure experience	Device controls give you precise management of how devices connect to your network, what capabilities are enabled, and what apps are available.
Controlling access to Microsoft Exchange	Your organization can use the BlackBerry Gatekeeping Service to control which devices can access Exchange ActiveSync. Any device that's not whitelisted for Microsoft Exchange is reported in the UEM Restricted Exchange ActiveSync devices list and blocked from accessing work email and organizer data.
App management	You can install and manage internal apps on devices. You can also block devices from installing apps from other sources.
Role-based administration	You can share administrative duties with multiple administrators who can access the administration consoles at the same time. You can use roles to define the actions that an administrator can perform and reduce security risks, distribute job responsibilities, and increase efficiency by limiting the options available to each administrator. You can use predefined roles or create your own custom roles.

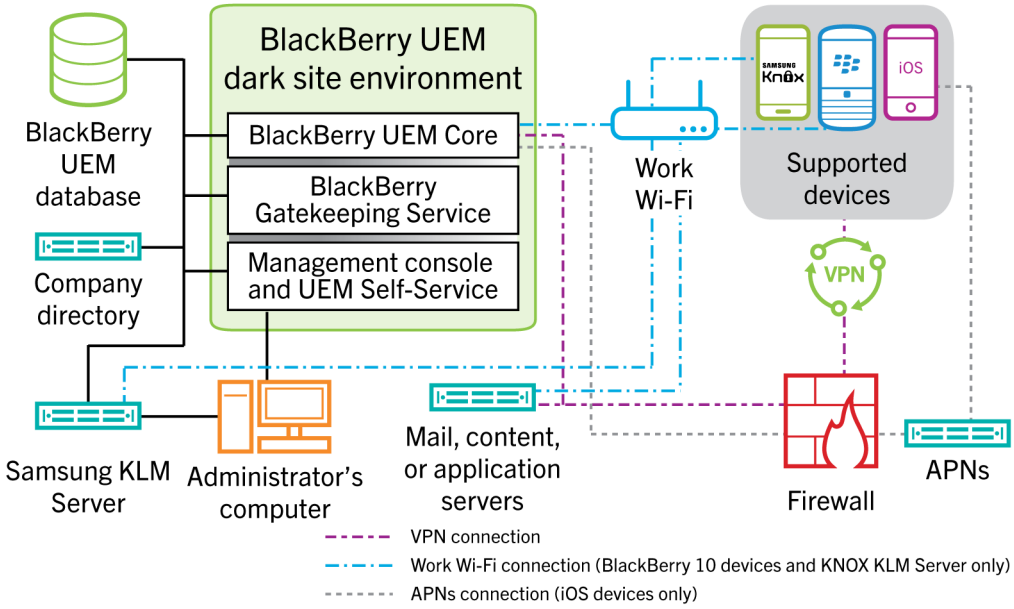
Unsupported BlackBerry UEM features

The following BlackBerry UEM features aren't supported in a dark site environment. These features are disabled in BlackBerry UEM for dark sites.

Unsupported features	Explanation
Devices	BlackBerry UEM for dark sites supports only BlackBerry 10, Samsung KNOX, and iOS devices.

Unsupported features	Explanation
Enterprise connectivity	BlackBerry UEM features that allow devices to connect to your organization's resources through the BlackBerry Infrastructure aren't supported, including: • BlackBerry Secure Connect Plus • BlackBerry Secure Gateway • BlackBerry MDS Connection Service • Using BlackBerry UEM as a proxy for SCEP requests
BlackBerry Dynamics	BlackBerry Dynamics apps, including BlackBerry Work, aren't supported.
Additional BlackBerry enter products	BlackBerry UEM for dark sites doesn't work with other BlackBerry enterprise products, including: • BlackBerry Enterprise Identity • BlackBerry 2FA
Managing public apps and apps protected by Microsoft Intune	BlackBerry UEM for dark sites doesn't support connections to public app vendors such as BlackBerry World, Apple App Store, and Google Play. You can't add public apps to users' devices. BlackBerry UEM for dark sites doesn't support connections to Microsoft Azure. You can't manage apps using Microsoft Intune app protection profiles.

Architecture: BlackBerry UEM for dark sites



Component name	Description
BlackBerry UEM Core	The BlackBerry UEM Core is the central component of the BlackBerry UEM architecture. It consists of several subcomponents that are responsible for: • Logging, monitoring, reporting, and management functions • Authentication and authorization services • Scheduling and sending commands, IT policies, and profiles to devices
BlackBerry UEM database	The BlackBerry UEM database is a relational database that contains user account information and configuration information that BlackBerry UEM uses to manage devices.
BlackBerry Gatekeeping Service	The BlackBerry Gatekeeping Service sends commands to Exchange ActiveSync to add devices to an allowed list when devices are activated on BlackBerry UEM. Unmanaged devices that try to connect to an organization's mail server can be reviewed, verified, and blocked or allowed by an administrator using the BlackBerry UEM management console.
Management console and UEM Self-Service	The management console and UEM Self-Service provide a browser-based user interface for administrator and user access to BlackBerry UEM. You use the management console to manage system settings, users, devices, and apps. Users can use UEM Self-Service to set an activation password and send commands to devices, such as set password, lock device, and delete device data.

Component name	Description
Samsung KLM Server	If you are managing Samsung KNOX devices, a Samsung KNOX License Management server is installed with BlackBerry UEM for dark sites so that BlackBerry UEM doesn't have to connect to the web-based Samsung KNOX License Management System to get license information. Samsung KNOX devices communicate with the KLM server using your work Wi-Fi network.
APNs	To manage iOS devices, BlackBerry UEM must send notifications to devices through an APNs server. When devices receive a notification from APNs, they contact BlackBerry UEM for updates. For information about securing connections to APNs or possible alternatives to using the public APNs, contact your Apple support representative.

Installing or upgrading BlackBerry UEM in a dark site environment

Only the following components are enabled for BlackBerry UEM installed in a dark site environment:

- BlackBerry UEM management console
- BlackBerry UEM Core
- BlackBerry Gatekeeping Service

You can upgrade BlackBerry UEM. For information about migrating devices to a new BlackBerry UEM environment, see the BlackBerry UEM Configuration content.

When you install or upgrade BlackBerry UEM, you can use an existing Microsoft SQL Server or install and use Microsoft SQL Server Express.

Note: Before you install or upgrade BlackBerry UEM, review the requirements and prerequisites in the BlackBerry UEM Planning content and in the Installation and upgrade content. Port requirements are in the Planning content.

Install or upgrade BlackBerry UEM

1. Log on as a user with local administrator privileges to the server where you are installing or upgrading BlackBerry UEM.
2. Download and extract the BlackBerry UEM installation files.
3. Modify the deployer.properties file with the parameters for your environment. The deployer.properties file is located in the same folder as the setup.exe file.
   a) In the **service.account.password=** field, type the password for the account you are logged in as.
   b) If you want to use an existing Microsoft SQL Server, type the information in the appropriate fields for that server.

   For information about how to fill out the fields, see deployer.properties file in the BlackBerry UEMInstallation and upgrade content.
4. Open a command prompt window as an administrator, and in the directory where you extracted the BlackBerry UEM installation files, type one of the following commands:

Option	Command
To use an existing Microsoft SQL Server database	`setup.exe --script --iacceptbeseula --propertyFiles darksite.properties --showlog`
To install a local Microsoft SQL Server database	`setup.exe --script --iacceptbeseula --propertyFiles darksite.properties --showlog --installSQL`

Logging in to BlackBerry UEM

After you install BlackBerry UEM, log in to the management console.

Note: When you log in to BlackBerry UEM for the first time, in addition to providing the name of your organization, the SRP identifier, and the SRP authentication key, you must enter the **license file name**. You obtain the license

file from your BlackBerry Sales representative. The SRP identifier and the SRP authentication key must match the information in the license file.

CAUTION: Do not reuse the SRP ID from previous BES5, BES10, BES12, or BlackBerry UEM instances when you install a new instance of BlackBerry UEM.

Log in to BlackBerry UEM for the first time

Before you begin: Verify that you have the BlackBerry UEM SRP identifier and SRP authentication key available.

If the setup application is still open, you can access the management console directly from the Console addresses dialog box.

1. In the browser, type **https://<*server_name*>:<*port*>/admin**, where <*server_name*> is the FQDN of the computer that hosts the management console. The default port for the management console is port 443.
2. In the **Username** field, type **admin**.
3. In the **Password** field, type **password**.
4. Click **Sign in.**
5. In the Server location drop-down list, select the country of the computer that has BlackBerry UEM installed on it, and click **Next**.
6. Type the name of your organization, the SRP identifier, and the SRP authentication key.
7. Click **Submit**.
8. Change the temporary password to a permanent password.
9. Click **Submit**.

After you finish:

- When you log in to the management console, you can choose to complete or close the **Welcome to BlackBerry UEM** dialog box. If you close the dialog box, it does not appear during subsequent logins.

Configuring BlackBerry UEM for dark sites

The following table summarizes the configuration tasks you may need to perform after you install BlackBerry UEM in a dark site environment.

For more information about configuring BlackBerry UEM, see the BlackBerry UEM Configuration content.

Task	Description
Import a BlackBerry UEM license file	You must manually import license information into BlackBerry UEM in a dark site environment. For more information, see Adding licenses to BlackBerry UEM.
Replace default certificates with trusted certificates	You can replace the default SSL certificate used by the BlackBerry UEM consoles and the default certificate that BlackBerry UEM uses to sign the MDM profile for iOS devices with trusted certificates. For more information, see Changing BlackBerry UEM certificates in the BlackBerry UEM Configuration content.
Configure connections through internal proxy servers	If your organization uses a proxy server for connections between servers inside your network, you may need to configure server-side proxy settings to allow the BlackBerry UEM Core to communicate with remote instances of the management console. For more information, see Configuring connections through internal proxy servers in the BlackBerry UEM Configuration content.
Connect BlackBerry UEM to company directories	You can connect BlackBerry UEM to one or more company directories so that BlackBerry UEM can access user data to create user accounts. For more information, see Connecting to your company directories in the BlackBerry UEM Configuration content.
Connect BlackBerry UEM to an SMTP server	If you want BlackBerry UEM to send activation emails and other notifications to users, you must specify the SMTP server settings that BlackBerry UEM can use. For more information, see Connecting to an SMTP server to send email notifications in the BlackBerry UEM Configuration content.
Obtain and register an APNs certificate	If you want to manage and send data to iOS devices, you must obtain a signed CSR from BlackBerry, use it to obtain an APNs certificate from Apple, and register the APNs certificate with the BlackBerry UEM domain. For more information, see Obtaining an APNs certificate to manage iOS devices.

Task	Description
Control which devices can access Exchange ActiveSync	If you configured Microsoft Exchange to block devices from accessing work email and organizer data unless the devices are added to an allowed list, you must create a Microsoft Exchange configuration in BlackBerry UEM. For more information, see Controlling which devices can access Exchange ActiveSync in the BlackBerry UEM Administration content.
Set up BlackBerry UEM Self-Service	If you want to allow users to perform certain management tasks, such as changing their passwords, you can set up and distribute the BlackBerry UEM Self-Service web application. For more information, see Setting up BlackBerry UEM Self-Service for users in the BlackBerry UEM Administration content.

Adding licenses to BlackBerry UEM

When BlackBerry UEM is installed in a dark site environment, you must manually import license information into BlackBerry UEM.

If you are managing Samsung KNOX devices, you must also set the Samsung KNOX ELM and KLM license keys.

To avoid manually updating licenses in the future, particularly for Samsung KNOX devices, consider purchasing perpetual licenses for your organization's dark site environment.

You can obtain a BlackBerry UEM license file and the Samsung license keys from your BlackBerry Sales representative.

Import BlackBerry UEM licenses

Before you begin: Obtain a BlackBerry UEM license file from your BlackBerry Sales representative.

1. On the menu bar, click **Settings > Licensing**.
2. On the **Licensing Summary** page, click **Import license**.
   If you want to update the existing licenses, click **Update licenses** instead.
3. Click **Browse**.
4. Select the license file that you want to use.
5. Click **Open**.

Set Samsung KNOX license keys

If you are managing Samsung KNOX devices in a dark site environment, you must set Samsung KNOX license keys in BlackBerry UEM.

Before you begin: Obtain Samsung KNOX ELM and KLM license keys from your BlackBerry Sales representative.

1. On the menu bar, click **Settings > Licensing**.
2. On the **Licensing Summary** page, click **Set KNOX license keys**.
3. Paste the Samsung KNOX ELM license key and Samsung KNOX KLM license key into the appropriate fields.
4. Click **Save**.

Obtaining an APNs certificate to manage iOS devices

APNs is the Apple Push Notification Service. To manage iOS devices, Apple requires that BlackBerry UEM be able to connect to APNs. For information about securing connections to APNs or possible alternatives to using the public APNs, contact your Apple support representative.

You must obtain and register an APNs certificate to use BlackBerry UEM to manage iOS devices.

Note: Each APNs certificate is valid for one year. The administration console displays the expiry date. You must renew the APNs certificate before the expiry date, using the same Apple ID that you used to obtain the certificate. If the certificate expires, devices don't receive data from BlackBerry UEM. If you register a new APNs certificate, users must reactivate their devices to receive data.

For more information, visit https://developer.apple.com to read *Issues with Sending Push Notifications* in article TN2265.

It's a best practice to access the administration console and the Apple Push Certificates Portal using the Google Chrome or Safari browsers. These browsers provide optimal support for requesting and registering an APNs certificate.

To obtain and register an APNs certificate to use the public APNs, perform the following actions:

Step	Action
1	Obtain a signed CSR from BlackBerry.
2	Use the signed CSR to request an APNs certificate from Apple.
3	Register the APNs certificate.

Obtain a signed CSR from BlackBerry

You must obtain a signed CSR from BlackBerry before you can obtain an APNs certificate.

1. On the menu bar, click **Settings > External integration > Apple Push Notification**.
2. Click **Get APNs Certificate**.
   If you want to renew the current APNs certificate, click **Renew certificate** instead.
3. In the **Step 1 of 3 - Download signed CSR certificate from BlackBerry** section, click **Download certificate signing request**.
4. Click **Save** to save the unsigned CSR file (.scsr) to your computer.
5. Send the unsigned CSR file to your BlackBerry Customer Support representative.
   Your Customer Support representative will have the CSR file signed by a BlackBerry CA and send the signed CSR back to you.

After you finish: Request an APNs certificate from Apple.

Request an APNs certificate from Apple

Before you begin: Obtain a signed CSR from BlackBerry.

1. On the menu bar, click **Settings > External integration > Apple Push Notification**.

2. In the **Step 2 of 3 - Request APNs certificate from Apple** section, click **Apple Push Certificate Portal**. You are directed to the Apple Push Certificates Portal.
3. Sign in to the Apple Push Certificates Portal using a valid Apple ID.
4. Follow the instructions to upload the signed CSR (.scsr).
5. Download and save the APNs certificate (.pem) on your computer.

After you finish: Register the APNs certificate.

Register the APNs certificate

Before you begin: Request an APNs certificate from Apple.

1. On the menu bar, click **Settings > External integration > Apple Push Notification**.
2. In the **Step 3 of 3 - Register APNs certificate** section, click **Browse**. Navigate to and select the APNs certificate (.pem).
3. Click **Submit**.

After you finish: To test the connection between BlackBerry UEM and the APNs server, click **Test APNs certificate**.

Managing users and devices in a dark site environment

User and device management tasks for most supported features in a dark site environment are the same as in any other BlackBerry UEM environment. For instructions on most administrative tasks not covered in this document, see the BlackBerry UEM Administration content.

Device activation

When you activate a device, you associate the device with BlackBerry UEM so that you can manage the device and users can access work data on the device.

When a device is activated, you can send IT policies and profiles to control the available features and manage the security of work data. You can also assign apps for the user to install. Depending on how much control the selected activation type allows, you may also be able to protect the device by restricting access to certain data, remotely setting passwords, locking the device, or deleting data.

Supported activation types

BlackBerry UEM for dark sites supports only the following activation types for BlackBerry 10, Samsung KNOX, and iOS devices.

BlackBerry 10 devices

Activation type	Description
Work and personal - Corporate	This activation type provides control of work data on devices, while making sure that there is privacy for personal data. When a device is activated, a separate work space is created on the device and the user must create a password to access the work space. Work data is protected using encryption and password authentication. All work data from any previous activations is deleted. You can control the work space on the device using commands and IT policies, but you can't control any aspects of the personal space on the device.
Work space only	This activation type provides full control of the device and doesn't provide a separate space for personal data. When a device is activated, the personal space and all work data from any previous activation is removed, a work space is installed, and the user must create a password to access the device. Work data is protected using encryption and password authentication. You can control the device using commands and IT policies.
Work and personal - Regulated	This activation type provides control of both work and personal data. When a device is activated, a separate work space is created on the device and the user must create a password to access the work space. Work data is protected using encryption and password authentication. All work data from any previous activations is deleted. You can control both the work space and the personal space on the device using commands and IT policies.

Samsung KNOX devices

Activation type	Description
Work and personal - full control (Samsung KNOX)	This activation type lets you manage the entire device using commands and the KNOX MDM and KNOX Workspace IT policy rules. This activation type creates a separate work space on the device and the user must create a password to access the work space. Data in the work space is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. This activation type supports the logging of device activity (SMS, MMS, and phone calls) in BlackBerry UEM log files. During activation users must grant Administrator permissions to the BlackBerry UEM Client.
Work space only - (Samsung KNOX)	This activation type lets you manage the entire device using commands and the KNOX MDM and KNOX Workspace IT policy rules. This activation type removes the personal space and installs a work space. The user must create a password to access the device. All data on the device is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. This activation type supports the logging of device activity (SMS, MMS, and phone calls) in BlackBerry UEM log files. During activation, users must grant Administrator permissions to the BlackBerry UEM Client.

iOS devices

Activation type	Description
MDM controls	This activation type provides basic device management using device controls made available by iOS. A separate work space isn't installed on the device, and there is no added security for work data. You can control the device using commands and IT policies.

Preparing users to activate devices

To prepare to allow users to activate devices, you should create an activation profile, modify the activation email template, and set an activation password for the user.

An activation profile specifies how many and what types of devices a user can activate and the type of activation to use for each device type. The assigned activation profile applies only to devices the user activates after you assign the profile. Devices that are already activated aren't automatically updated to match the new or updated activation profile.

When you add a user to BlackBerry UEM, the Default activation profile is assigned to the user account. The Default activation profile allows activation options that aren't supported in a dark site environment. You can change the Default activation profile to suit your requirements, or you can create a custom activation profile and assign it to users or user groups.

The activation email template defines the email message sent to users instructing them to activate their device.

After the activation profile and email template are completed you can set an activation password for the user and send an activation email message to allow them to complete the activation.

Create an activation profile

Note: The activation profile displays device and activation type options that aren't supported in a dark site environment. When you create or update an activation profile, don't select unsupported options.

1. 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 BlackBerry 10 or iOS devices must accept the notice to complete the activation process.
7. In the **Device types that users can activate** section, select the device types as required. Device types that you don't select aren't included in the activation profile and users can't activate those devices. To allow Samsung KNOX activations, select Android.
8. Perform the following actions for each device type included in the activation profile:
   - Click the tab for the device type.
   - In the **Device model restrictions** drop-down list, select whether to allow or restrict specified devices or to have no restrictions. Click **Edit** to select the devices you want to restrict or allow. Click **Save**.
   - In the **Allowed version** drop-down list, select the minimum allowed version.
   - In the **Activation type** section, select an activation type.
9. Click **Add**.

Create an activation email template

1. On the menu bar, click **Settings** > **General settings**.
2. Click **Email templates**.
3. Click +. Select **Device activation**.
4. In the **Name** field, type a name to identify this template.
5. In the **Subject** field, edit the text to customize the subject line of the first activation email.
6. In the **Message** field, type the body text of the activation email.
   - Use the HTML editor to select the font format and to insert images (for example, a corporate logo).
   - Insert variables in the text to personalize the message (for example, you can use the variable %UserDisplayName% to insert the recipient's name). For a list of available variables, see the BlackBerry UEM Administration content.
   - For BlackBerry 10 and Samsung KNOX devices, include the BlackBerry UEM server address that users need to activate the device.
     - For BlackBerry 10 devices, the URL is: http://*server.name*:8882/*SRP_ID*/mdm
     - For Samsung KNOX devices, the URL is: http://*server.name*:8882/*SRP_ID*
   - To see sample text, click **Suggested text**.
7. To send the activation password separately from the activation instructions, select **Send two separate activation emails - first for complete instructions, second for password**. If you decide to send only one

activation email, make sure that you include the activation password or the activation password variable in the first email.

8. In the **Subject** field, type a subject line for the second activation email.
9. Customize the body text of the second activation email that you send to users. Make sure that you include the activation password or the activation password variable.
10. Click **Save**.

Set an activation password and send an activation email message

You can set an activation password and send a user an activation email with the information required to activate one or more devices.

The email is sent from the email address that you configured in the SMTP server settings.

Before you begin: Create an activation email template.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. In the Activation details pane, click **Set activation password**.
5. In the **Activation option** drop-down list, select **Default device activation**.
6. In the **Activation password** drop-down list, perform one of the following tasks:
   - If you want to automatically generate a password, select **Autogenerate device activation password and send email with activation instructions**. When you select this option, you must select an email template to send the information to the user.
   - If you want to set an activation password for the user and, optionally, send an activation email, select **Set device activation password**.
7. Optionally, change the activation period expiration. The activation period expiration specifies how long the activation password remains valid.
8. If you want the activation password to be valid only for one device activation, select **Activation period expires after the first device is activated**.
9. In the **Activation email template** drop-down list, select the email template that you want to use.
10. Click **Submit**.

Activating BlackBerry 10 devices

You can allow users to activate BlackBerry 10 devices over your work Wi-Fi network, or you can activate multiple BlackBerry 10 devices for users using the BlackBerry Wired Activation Tool.

Activating BlackBerry 10 devices over work Wi-Fi

You can allow users to activate BlackBerry 10 devices over your work Wi-Fi network. To activate devices, users need the following information.

- Work email address
- Activation password
- BlackBerry UEM server address (http://*server.name*:8882/*SRP_ID*/mdm)

You can provide the information in the activation email that BlackBerry UEM sends to users. See Create an activation email template.

Activate a BlackBerry 10 device

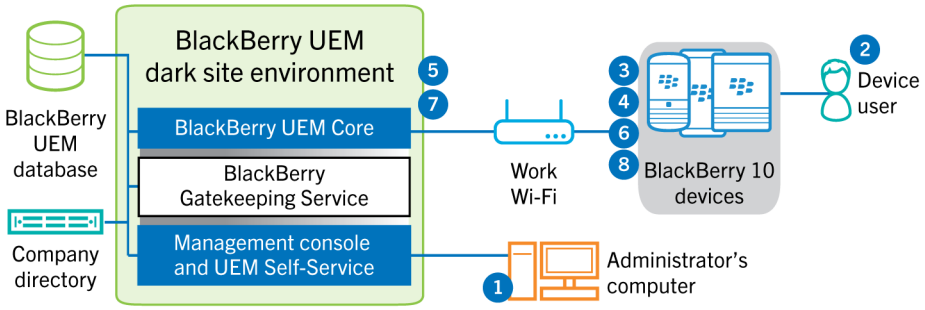
Send the following activation instructions to the device user.

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**.
   You will receive a warning that your device couldn't look up connection information.
7. Tap **Advanced**.
8. Tap **Work Account**.
9. 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.
10. Tap **Done**.
11. 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 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.

Data flow: Activating a BlackBerry 10 device



1. You perform the following actions:
   a. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company directory
   b. Assign an activation profile to the user
   c. Use one of the following options to provide the user with activation details:
      - Automatically generate a device activation password and send an email with activation instructions for the user
      - Set a device activation password and communicate the username and password to the user directly or by email

- Communicate the BlackBerry UEM Self-Service address to the user so that they can set their own activation password

2. The user performs the following actions:
   a. Connects to your work Wi-Fi network
   b. Types the username and activation password on the device
   c. For a "Work and personal - Regulated" or "Work space only" activation, accepts the organization notice, which outlines the terms and conditions that the user must agree to
3. If the activation is a "Work space only" activation, the device deletes all existing data and restarts.
4. The device performs the following actions:
   a. Establishes a connection with BlackBerry UEM
   b. Generates a shared symmetric key that is used to protect the CSR and the response to BlackBerry UEM using the activation password and EC-SPEKE.
   c. Creates an encrypted CSR and HMAC as follows:
      - Generates a key pair for the certificate
      - Creates a PKCS#10 CSR that includes the public key of the key pair
      - Encrypts the CSR using the shared symmetric key and AES-256 in CBC mode with PKCS#5 padding
      - Computes an HMAC of the encrypted CSR using SHA-256 and appends it to the CSR
   d. Sends the encrypted CSR and HMAC to BlackBerry UEM
5. BlackBerry UEM performs the following actions:
   a. Verifies the HMAC of the encrypted CSR and decrypts the CSR using the shared symmetric key
   b. Retrieves the username, work space ID, and your organization's name from the BlackBerry UEM database
   c. Packages a client certificate using the information it retrieved and the CSR that the device sent
   d. Signs the client certificate using the enterprise management root certificate
   e. Encrypts the client certificate, enterprise management root certificate, and the BlackBerry UEM URL using the shared symmetric key and AES-256 in CBC mode with PKCS#5 padding
   f. Computes an HMAC of the encrypted client certificate, enterprise management root certificate, and the BlackBerry UEM URL and appends it to the encrypted data
   g. Sends the encrypted data and HMAC to the device
6. The device performs the following actions:
   a. Verifies the HMAC
   b. Decrypts the data it received from BlackBerry UEM
   c. Stores the client certificate and the enterprise management root certificate in its keystore
7. BlackBerry UEM performs the following actions:
   a. Assigns the new device to a BlackBerry UEM instance in the domain
   b. Sends configuration information, including enterprise connectivity settings, to the device
8. The device sends an acknowledgment over TLS to BlackBerry UEM to confirm that it received and applied the IT policy and other data and created the work space. The activation process is complete.

The elliptic curve protocols used during the activation process use the NIST-recommended 521-bit curve.

Activating BlackBerry 10 devices using the BlackBerry Wired Activation Tool

The BlackBerry Wired Activation Tool allows you to activate multiple BlackBerry 10 devices at the same time using USB connections instead of wireless connections. Your organization may want to use this method for different reasons:

- To make it quick and easy to activate multiple devices at once
- To keep the activation process in the hands of administrators

- To activate devices and configure their security features, such as content encryption requirements and VPN profiles, before giving them to users or connecting them to your organization's network

You can't assign profiles and policies using the BlackBerry Wired Activation Tool. You must assign any profiles and policies to your users in the BlackBerry UEM management console before assigning and activating devices using the BlackBerry Wired Activation Tool. However, you don't need to set any activation passwords to assign and activate devices using the BlackBerry Wired Activation Tool.

To activate devices using the BlackBerry Wired Activation Tool, the devices must be running BlackBerry 10 OS version 10.3 or later.

To obtain the BlackBerry Wired Activation Tool contact your Customer Support representative.

Configure the BlackBerry Wired Activation Tool and log in to a BlackBerry UEM instance

Before you can activate devices with the BlackBerry Wired Activation Tool, you must create a configuration for each BlackBerry UEM instance you need to access. After you create a configuration, you must also use an administrator account to allow the BlackBerry Wired Activation Tool to access BlackBerry Web Services.

1. In the BlackBerry Wired Activation Tool installation folder, double-click the **BWAT.exe** file.
2. In the **Add a BES12 server screen**, in the **Name** field, type a name to identify the configuration you're creating. For example, if you have two BlackBerry UEM instances, you might create a configuration for each one and name them Server 1 and Server 2.
3. In the **BlackBerry Web Services URL** field, type the address for the BlackBerry Web Services component. The default address is https://<*BlackBerry UEM web address*>:18084.

   You can change the port by modifying the `tomcat.bws.port` setting in the BlackBerry UEM database.
4. In the **BCP Endpoint URL** field, type the address to use for device activations. This is also known as the Activation URL or Server name. The default address is: http://*server*.*name*:8882/*SRP_ID*/mdm.

   You can find the address by making sure the %ActivationURL% variable is in the Activation email template and clicking **View activation email** from any User summary screen.

   If necessary, you can also look up the host address and port in the BlackBerry UEM database. In the `def_cfg_setting_dfn` table, find the `id_setting_definition` values for `bdmi.enroll.bcp.host` and `bdmi.enroll.bcp.port`. Then use the `id_setting_definition` values to look up the values of those settings in the `obj_global_cfg_setting`.
5. Click **Submit**.
6. In the **Log in** screen, select a BlackBerry UEM configuration from the drop-down list.
7. In the **Username** field, type the username of a BlackBerry UEM user account with administrator permissions.
8. In the **Password** field, type the password for the account.
9. In the **Directory** drop-down list, select an authentication method.
10. If required, in the **Domain** field, type the Microsoft Active Directory domain.
11. Click **Log in**.

Activate BlackBerry 10 devices using the BlackBerry Wired Activation Tool

Before you begin:

- Configure the BlackBerry Wired Activation Tool and log in to a BlackBerry UEM instance.
- Turn on all connected devices and make sure that all devices have either completed the initial setup process, or that they haven't started it. You can't activate devices if the initial setup process is in progress.

1. Connect one or more BlackBerry 10 devices to your computer using USB cables.

2. Check the **Status** column for each device. Perform one of the following actions:
   - If the Status column displays **Requires password**, click **Requires password** to enter the password for the device
   - If the Status column displays **Unsupported device**, upgrade the device software to BlackBerry 10 OS version 10.3 or later
   - If the Status column displays **Ready**, assign the device to a user
3. In the **Search** field, search for a user account that you want to assign a device to.
4. In the list of search results, click the user account.
5. In the main section of the screen, click a user account name and drag the name to a device to assign the device to that user. Repeat this step to assign devices to multiple users.
6. Select the checkbox next to the user and device pairs that you want to activate.
7. Click **Activate devices**.

The BlackBerry Wired Activation Tool activates all the devices you selected. Check the Status column for the progress and results for each device. If an activation doesn't complete, click the message in the Status column for more information about errors.

Activating Samsung KNOX devices

Users can activate Samsung KNOX Workspace devices over your work Wi-Fi network. BlackBerry UEM for dark sites doesn't support "Samsung KNOX MDM" or "Work and personal - user privacy - (Samsung KNOX)" activations. BlackBerry UEM for dark sites also doesn't support Samsung KNOX Mobile Enrollment.

To activate a devices, users need the following information:

- Work email address
- Activation password
- BlackBerry UEM server address (http://*server.name*:8882/*SRP_ID*)

You can provide the information in the activation email that BlackBerry UEM sends to users. See Create an activation email template.

If your organization is using Samsung KNOX devices in a dark site environment, a Samsung KLM server was installed with BlackBerry UEM. Samsung KNOX devices communicate with the KLM server using your work Wi-Fi network.

Steps to activate Samsung KNOX devices

Step	Action
1	Instruct the users to install the BlackBerry UEM Client app. See Installing the BlackBerry UEM Client on Samsung KNOX devices.
2	Create an activation profile and assign it to a user account or user group.
3	Set an activation password and send an activation email message.

Installing the BlackBerry UEM Client on Samsung KNOX devices

Users must install the BlackBerry UEM Client before activating a Samsung KNOX device. You or users can download the UEM Client from BlackBerry at: https://bbapps.download.blackberry.com/apps/uemclient.apk.

You can allow users to download the file or you can put a copy in a shared location on your network. You can also manage updates to the app on activated devices using BlackBerry UEM. For more information, see Adding internal apps to the app list in the BlackBerry UEM Administration content.

Activate a Samsung KNOX Workspace device

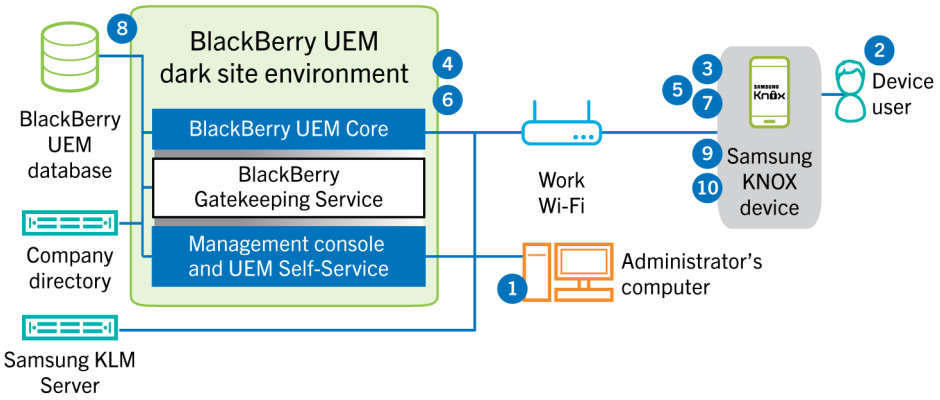
Send the following activation instructions to the device user.

1. Connect the device to the work Wi-Fi network.
2. Download and install the BlackBerry UEM Client from the provided loaction.
3. On the device, tap **UEM Client**.
4. Read the license agreement. Tap **I Agree**.
5. Type your work email address. Tap **Next**.
6. Type the server address. Tap **Next**. You can find the server address in the activation email message you received or in BlackBerry UEM Self-Service.
7. Type your activation password. 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 UEM Client. 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.

Data flow: Activating a device to use KNOX Workspace



1. You perform the following actions:
   a. Add a user to BlackBerry UEM as a local user account or using the account information retrieved from your company directory.

   b. Make sure the "Work and personal - full control (Samsung KNOX)" or "Work space only - (Samsung KNOX)" activation type is assigned to the user.
   c. Instruct the user to download and install the BlackBerry UEM Client.
   d. Use one of the following options to provide the user with activation details:
      - Automatically generate a device activation password and send an email with activation instructions for the user
      - Set a device activation password and communicate the username and password to the user directly or by email
      - Communicate the BlackBerry UEM Self-Service address to the user so that they can set their own activation password
2. The user performs the following actions:
   - Connects to your work Wi-Fi network
   - Downloads and installs the UEM Client on the device
   - Opens the UEM Client and enters the email address and activation password
3. The UEM Client establishes a connection with BlackBerry UEM and sends an activation request to BlackBerry UEM. The activation request includes the username, password, device operating system, and unique device identifier.
4. BlackBerry UEM performs following actions:
   a. Inspects the credentials for validity
   b. Creates a device instance
   c. Associates the device instance with the specified user account in the BlackBerry UEM database
   d. Adds the enrollment session ID to an HTTP session
   e. Sends a successful authentication message to the device
5. The UEM Client creates a CSR using the information received from BlackBerry UEM and sends a client certificate request to BlackBerry UEM over HTTPS.
6. BlackBerry UEM performs the following actions:
   a. Validates the client certificate request against the enrollment session ID in the HTTP session
   b. Signs the client certificate request with the root certificate
   c. Sends the signed client certificate and root certificate back to the UEM Client

   A mutually authenticated TLS session is established between the UEM Client and BlackBerry UEM.
7. The UEM Client requests all configuration information and sends the device and software information to BlackBerry UEM.
8. BlackBerry UEM stores the device information in the database and sends the requested configuration information to the device.
9. The UEM Client determines if the device uses KNOX Workspace and is running a supported version. If the device uses KNOX Workspace, the device connects to the local Samsung KLM server and activates the KNOX management license. After it's activated, the UEM Client applies the KNOX MDM and KNOX Workspace IT policy rules.
10. The device sends an acknowledgment to BlackBerry UEM that it received and applied the configuration information. The activation process is complete.

After the activation is complete, the user is prompted to create a work space password for the KNOX Workspace. Data in the KNOX Workspace is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint.

Note: If the device is activated with the "Work space only - (Samsung KNOX)" activation type, the personal space is removed when the KNOX Workspace is set up.

Activating iOS devices

If you allow users to use iOS devices in a dark site environment, you must prepare the devices using Apple Configurator 2. BlackBerry UEM doesn't support devices enrolled in Apple's Device Enrollment Program. Users complete the activation for prepared devices without using the BlackBerry UEM Client app. They need only their username and activation password.

When the devices are activated, BlackBerry UEM sends the IT policy and profiles that you assigned to users to the devices.

Steps to activate iOS devices

Step	Action
1	Add BlackBerry UEM server information to Apple Configurator 2.
2	Prepare iOS devices using Apple Configurator 2.
3	Create an activation profile and assign it to a user account or user group.
4	Set an activation password and send an activation email message.
5	Distribute the devices to users and have them complete the setup.

Add BlackBerry UEM server information to Apple Configurator 2

Before you begin: Download and install the latest version of Apple Configurator 2 from Apple.

1. In the Apple Configurator 2 menu, select **Preferences > Servers**.
2. Click + > **Next**.
3. In the **Name** field, type a name for the server.
4. In the **Hostname or URL** field type the BlackBerry UEM server URL using the format: *<http or https>://<servername>:<port>*, where the default port number is 8885. For more information about port settings, see BlackBerry UEM listening ports in the Planning content.
5. Click **Next**.
6. Close the **Server** window.

Prepare iOS devices using Apple Configurator 2

When you prepare a device, Apple Configurator 2 wipes the device and upgrades the device OS to the latest version.

Before you begin: Add BlackBerry UEM server information to Apple Configurator 2.

1. Open Apple Configurator 2.
2. Connect one or more iOS devices to your computer.

3. Click **Prepare**.
4. In the **Configuration** drop-down list, select **Manual**. Click **Next**.
5. In the **Server** drop-down list, select the BlackBerry UEM server. Click **Next**.
6. Optionally, select the **Supervise devices** checkbox. Click **Next**.
7. If you selected **Supervise devices**, complete the organization information.
8. Click **Prepare** and wait while the device is prepared. The process can take up to 15 minutes.

After you finish: Distribute the devices to users so they can complete the activation.

Managing BlackBerry 10 devices

For details about managing BlackBerry 10 devices and device users, see the BlackBerry UEM Administration content.

You should keep the following considerations in mind when managing BlackBerry 10 devices in a dark site environment.

Dark site considerations	Description
Connecting to your organization's resources	In a dark site environment, BlackBerry 10 devices can connect to your network using only your work Wi-Fi network or a VPN. To use a VPN, ensure you install an appropriate VPN app on the device and set up a VPN profile.
App management	BlackBerry UEM for dark sites doesn't support connections to BlackBerry World. You can't add public apps to the app list for devices.

Managing Samsung KNOX Workspace devices

For details about managing Samsung KNOX Workspace devices and device users, see the BlackBerry UEM Administration content.

You should keep the following considerations in mind when managing KNOX Workspace devices in a dark site environment.

Dark site considerations	Description
Connecting to your organization's resources	In a dark site environment, after activation, KNOX Workspace devices can connect to BlackBerry UEM and your resources over a VPN connection. To use a VPN, ensure you install an appropriate VPN app on the device and set up a VPN profile.
App management	BlackBerry UEM for dark sites doesn't support connections to Google Play. You can't add public apps to the app list for devices.
Email and organizer data	The default email app on Samsung KNOX devices needs to connect to the Samsung infrastructure before it will send and receive data. You can choose to allow this connection or use a different email app on KNOX Workspace devices.

Dark site considerations	Description
Device notifications	Sending notifications to KNOX Workspace devices using GCM isn't supported in a dark site environment. The BlackBerry UEM Client will poll BlackBerry UEM for updates at regular intervals.

Managing iOS devices

For details about managing iOS devices and device users, see the BlackBerry UEM Administration content.

You should keep the following considerations in mind when managing iOS devices in a dark site environment.

Dark site considerations	Description
Connecting to your organization's resources	In a dark site environment, after activation, iOS devices can connect to BlackBerry UEM and your resources using a VPN connection. To use a VPN, ensure you install an appropriate VPN app on the device and set up a VPN profile.
App management	BlackBerry UEM for dark sites doesn't support connections to the Apple App Store. You can't add public apps to the app list for devices.
Compliance profiles	Because the BlackBerry UEM Client client isn't supported for iOS devices in a dark site environment, Compliance profiles aren't supported.

Product documentation

The following BlackBerry UEM content should be useful to you when managing BlackBerry UEM in a dark site environment.

If your dark site security requirements prevent you from accessing the BlackBerry UEM documentation from within the management console, you can download PDF versions of the documentation from a location with full internet access or ask your BlackBerry Support representative to send them to you.

Resource	Description
Release notes and advisories	• Descriptions of fixed issues • Descriptions of known issues and potential workarounds • What's new
Installation and upgrade	• System requirements • Installation instructions • Upgrade instructions
Configuration	• Instructions for how to configure server components before you start administering users and their devices • Instructions for migrating data from an existing BlackBerry UEM database
Administration	• Basic and advanced administration for all supported device types • Instructions for creating user accounts, groups, roles, and administrator accounts • Instructions for activating devices • Instructions for creating and assigning IT policies and profiles • Instructions for managing apps on devices • Descriptions of profile settings • Descriptions of IT policy rules for BlackBerry 10, iOS, and Android devices
Compatibility matrix	• List of supported operating systems, database servers, and browsers for the BlackBerry UEM server • List of supported Samsung KNOX operating systems

Glossary

AES	Advanced Encryption Standard
APNs	Apple Push Notification service
BlackBerry UEM domain	A BlackBerry UEM domain consists of a BlackBerry UEM database and a BlackBerry Control database and any BlackBerry UEM instances that connect to them.
BlackBerry UEM instance	A BlackBerry UEM instance refers to one installation of the BlackBerry UEM Core and all associated BlackBerry UEM components that communicate with it. The components can be installed on the same server or multiple servers. There can be more than one BlackBerry UEM instance in a BlackBerry UEM domain.
CA	certification authority
CBC	cipher block chaining
certificate	A certificate is a digital document that binds the identity and public key of a certificate subject. Each certificate has a corresponding private key that is stored separately. A certificate authority signs the certificate to indicate that it is authentic and can be trusted.
CSR	certificate signing request
EC-SPEKE	Elliptic Curve – Simple Password Exponential Key Exchange
EMM	Enterprise Mobility Management
FQDN	fully qualified domain name
GCM	Google Cloud Messaging
HMAC	keyed-hash message authentication code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IT policy	An IT policy consists of various rules that control the security features and behavior of devices.
MDM	mobile device management

MMS	Multimedia Messaging Service
PKCS	Public-Key Cryptography Standards
SCEP	simple certificate enrollment protocol
SHA	Secure Hash Algorithm
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
space	A space is a distinct area of the device that enables the segregation and management of different types of data, applications, and network connections. Different spaces can have different rules for data storage, application permissions, and network routing. Spaces were formerly known as perimeters.
SRP	Server Routing Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UEM	Unified Endpoint Manager
VPN	virtual private network

Legal notice

OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR 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