BlackBerry UEM for dark sites
Installation and Administration Guide

12.17

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.

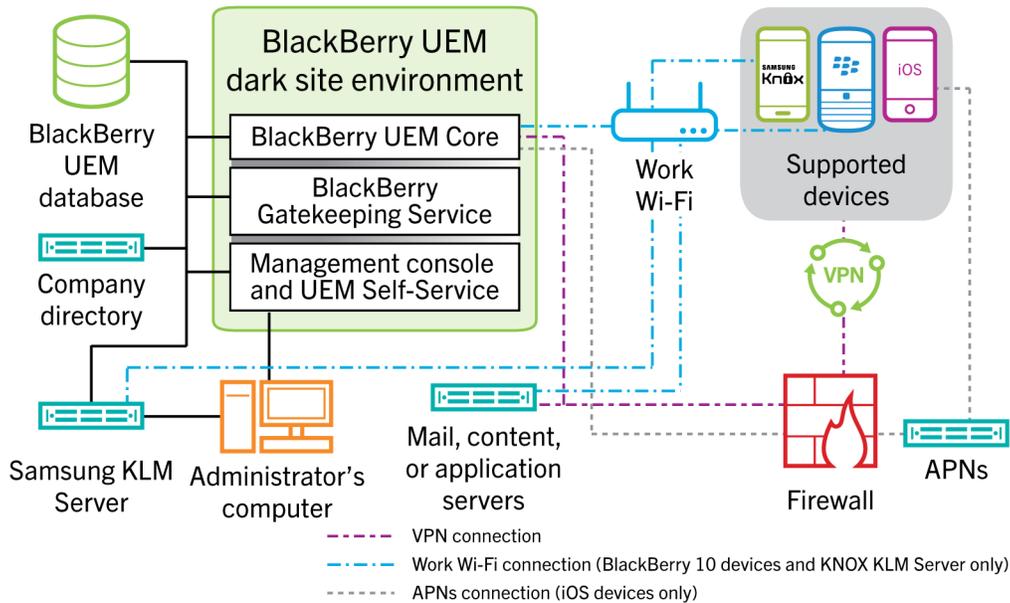| Feature	Description
Multiplatform device management	You can manage iOS and Samsung Knox devices.
Trusted and secure experience	Device controls give you precise management of how devices connect to your network, what capabilities are enabled, and what apps are available.
Controlling access to Microsoft 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 iOS and Samsung 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 • Using BlackBerry UEM as a proxy for SCEP requests
BlackBerry Dynamics	BlackBerry Dynamics apps, including BlackBerry Work, aren't supported.
Additional BlackBerry enterprise 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

BlackBerry UEM database

BlackBerry UEM dark site environment
- BlackBerry UEM Core
- BlackBerry Gatekeeping Service
- Management console and UEM Self-Service

Company directory

Samsung KLM Server

Administrator's computer

Mail, content, or application servers

Work Wi-Fi

Supported devices

VPN

Firewall

APNs

- – · – · – VPN connection
- – · – · – Work Wi-Fi connection (BlackBerry 10 devices and KNOX KLM Server only)
- – – – – APNs connection (iOS devices only)

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
Mail, content, or application servers	Your internal network includes various services that devices and BlackBerry UEM can communicate with.
	If you are activating Samsung Knox devices using Android Enterprise activation types, you require a server that contains the BlackBerry UEM Client .apk file and a PAC file that prevents devices from attempting to connect to Google Play during activation.
Samsung KLM license server	If you are managing Samsung Knox devices, an on-premises 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.
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.

Task	Description
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 create and import the Samsung Knox KPE license keys. You can use your Samsung portal account to create the Samsung license keys.

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**.

Import KPE keys into your Samsung Knox License On-Premises server

You must log in to the Samsung Knox License On-Premises server and import the KPE keys that you use in BlackBerry UEM.

Before you begin:

Make sure that you have already generated Samsung license keys. For more information, see the information from Samsung.

1. Log in to the Samsung Knox License On-Premises server
2. Click the **License** tab.
3. Click **License Add/Update**.
4. Click **Browse** and navigate to the location where you stored your Samsung license keys.
5. Type the security text that is displayed on the screen.
6. Click **Activate**.

Set Samsung Knox license keys in BlackBerry UEM

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

Note:

- If you are using Samsung Knox ELM and KLM license keys, and you do not plan to activate or reactivate Android devices that are using BlackBerry UEM Client version 12.40.x and later, you can continue to use those keys.
- If you plan to activate Android devices that are using BlackBerry UEM Client version 12.40.x and later, you must import the KPE standard license key and KPE premium license keys into BlackBerry UEM.

Before you begin:

- You must update the local Samsung on-premises licensing server to version 2.3 or later to support KPE licensing.
- You must import the KPE standard license key and KPE premium license key into the local Samsung Knox License On-Premises server before you import them into BlackBerry UEM. See Import KPE keys into your Samsung Knox License On-Premises server.

1. On the menu bar, click **Settings > Licensing**.
2. On the **Licensing Summary** page, click **Set KNOX license keys**.
3. Paste the Samsung Knox KPE Standard license key in the **Samsung KNOX ELM** field and the Samsung Knox KPE Premium license key into the **KLM Samsung KNOX** field.
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). Note that if the following error displays: "**You have uploaded an invalid file type. Supported file extensions are .txt, .rtf, .plist, .b64.**", you can rename the .scsr file to a .txt file format, and upload the CSR again.
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 the following activation types for Samsung Knox and iOS devices.

Samsung Knox devices

Note: Samsung Knox activation types will be deprecated in a future release. Devices that support Knox Platform for Enterprise can be activated using the Android Enterprise activation types. For more information, visit https://support.blackberry.com/community to read article 54614.

Activation type	Description
Work space only (Android Enterprise fully managed device)	This activation type lets you manage the entire device using commands and IT policy rules. This activation type requires the user to reset the device to factory settings before activating. The activation process installs a work profile and no personal profile. 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.
	During activation, the device installs the BlackBerry UEM Client automatically and grants it Administrator permissions. Users cannot revoke the Administrator permissions or uninstall the app.
	Following activation, Work space only devices have only a limited set of the standard pre-installed apps, such as Camera, Phone, and Settings, plus any apps you have assigned with a required disposition. The list of retained pre-installed apps depends on the device vendor and OS version.
	This activation type requires the device to be reset to factory default settings before activating. If the BlackBerry UEM Client is deleted or the work profile is removed from the device, it is automatically reset to factory default settings.

Activation type	Description
Work and personal - user privacy (Android Enterprise with work profile)	This activation type maintains privacy for personal data but lets you manage work data using commands and IT policy rules. This activation type creates a work profile on the device that separates work and personal data. Work and personal data are both protected using encryption and password authentication. Users do not have to 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 **Policy > Activation**.
3. Click ＋.
4. Type a name and description for the profile.
5. In the **Number of devices that a user can activate** field, specify the maximum number of devices the user can activate.
6. In the **Device ownership** drop-down list, perform one of the following actions:

   - Select **Not specified** if some users activate personal devices and some users activate work devices.

- Select **Work** if most users activate work devices.
- Select **Personal** if most users activate their personal devices.

7. 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 process.

8. 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.

9. Perform the following actions for each device type included in the activation profile:

   a) Click the tab for the device type.

   b) In the **Device model restrictions** drop-down list, select one of the following options:

      - **No restrictions**: Users can activate any device model.
      - **Allow selected device models**: Users can activate only the device models that you specify. Use this option to limit the allowed devices to only some models.
      - **Do not allow selected device models**: Users can't activate the device models that you specify. Use this option to block activation of some device models or devices from specific manufacturers.

      If you restrict the device models users can activate, click **Edit** to select the devices you want to allow or restrict and click **Save**.

   c) In the **Minimum allowed version** drop-down list, select the minimum allowed OS version.

      Many older OS versions are no longer supported by BlackBerry UEM. You only need to select a minimum version if you don't want to support the earliest version currently supported by BlackBerry UEM. For more information on supported versions, see the Compatability Matrix.

   d) Select the supported activation types.

      For Samsung Knox devices, you can select multiple activation types and rank them. For all other device types, you can select only one activation type.

10. For iOS devices, if you only want to activate supervised devices, select **Do not allow unsupervised devices to activate**

11. For Samsung devices, perform the following actions:

    a) If you selected more than one activation type type, click the up and down arrows to rank them.

    b) If you selected an Android Enterprise activation type, select **When activating Android Enterprise devices, enable premium UEM functionality such as BlackBerry Secure Connect Plus** to enable Knox Platform for Enterprise features.

    c) Deselect **Add Google Play account to work space**.

       This feature isn't supported in a dark site environment.

    d) In the **Hardware attestation options** section, select **Enforce attestation compliance rules during activation** if you want BlackBerry UEM to send challenges to devices when they are activated to ensure the required security patch level is installed.

12. 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 Samsung Knox devices, include the BlackBerry UEM server address that users need to activate the device.
    - 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 Samsung Knox devices

Users can activate Samsung Knox 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.

Note: Samsung Knox activation types will be deprecated in a future release. Devices that support Knox Platform for Enterprise can be activated using the Android Enterprise activation types. For more information, visit https://support.blackberry.com/community to read article 54614.

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 on-premises licensing server was installed with BlackBerry UEM. Samsung Knox devices communicate with the licensing server using your work Wi-Fi network. If you are activating devices with Android Enterprise activation types and the licensing server certificate is signed by an internal CA, you need to send the licensing server certificate to devices using a CA certificate profile. For more information, see the BlackBerry UEM administration content.

Steps to activate Samsung Knox devices

Step	Action
1	Create and assign any required profiles, apps, and an IT policy to users. If you intend to set up VPN for Samsung Knox devices, Set up VPN using Knox StrongSwan.
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.
4	Provide activation instructions to users for Android Enterprise devices or Samsung Knox Workspace devices.

Installing the BlackBerry UEM Client on Samsung Knox devices

Users must install the BlackBerry UEM Client to activate a Samsung Knox device. You can manually download the UEM Client from BlackBerry and save it to a network location that devices have access to. To download the .apk file of the latest UEM Client , visit support.blackberry.com/community to read article 42607.

If users are activating devices using the Samsung Knox Workspace or Android Enterprise (Work and personal - user privacy) activation types you can instruct users to obtain and install the UEM Client before they start the activation process.

For devices that will be activated with the Android Enterprise (Work space only) or (Work and personal - full control) activation types, the device must be set to factory default settings before starting the activation. You can set activation options to install the UEM Client from a server on your network during activation. To provide the download location to the device, you can include the location in a QR Code that the user scans to start activation.

Setting activation options for Android Enterprise activations

For devices that will be activated with the Android Enterprise (Work space only) or (Work and personal - full control) activation types, the device must be set to factory default settings before starting the activation. You can

set activation options to install the BlackBerry UEM Client from a server on your network during activation. To provide the download location to the device, you can include the location in a QR Code that the user scans to start activation.

You must also create a PAC file that prevents devices from attempting to connect to Google Play during activation and store the PAC file in the same location as the UEM Client .apk file.

Before you begin: Download the UEM Client from BlackBerry and save it to a network location that devices have access to. For more information, visit support.blackberry.com/community to read article 42607.

1. Create a PAC file in the following format that specifies the HTTP URL where the PAC file is hosted and save it to the same location as the UEM Client .apk file.

```
function FindProxyForURL(url, host)
{
return "DIRECT";
}
```

Users will need to specify the **PAC web address** when they set up the Wi-Fi connection on their device during activation. The PAC file must be available at the default HTTP port 80.

2. On the menu bar, click **Settings > General settings**.
3. Click **Activation defaults**.
4. Under **Device activation defaults** set the following QR Code options.
    a) Select **Allow QR codes for device activation**.
    b) Select **Allow QR code to contain location of UEM Client app source file**.
    c) In the **Location of UEM Client app source file** field, specify the network location where you saved the .apk file.
5. Verify that the following options are not selected:

   - **Enable MDM controls activation type for Android devices**
   - **Use QR codes to unlock BlackBerry Dynamics apps**
   - **Turn on registration with the BlackBerry Infrastructure**
6. Click **Save**.

Activate an Android Enterprise device

These instructions apply to Android Enterprise (Work space only) or (Work and personal - full control) activation types. For these devices, the device must be set to factory default settings before starting the activation.

For Android Enterprise (Work and personal - user privacy) activations, follow the instructions to Activate a Samsung Knox Workspace device.

Send the following activation instructions to the device user.

1. On the device that you want to activate, if you do not see the device setup Welcome screen, reset your device to the factory default settings.
2. Tap the device screen seven times.

   A QR Code reader opens on the device.
3. Scan the QR code provided to you by your administrator.
4. Specify the information to connect to your work Wi-Fi network, including the **PAC web address** provided by your administrator.

   The device installs the BlackBerry UEM Client and begins the activation process. The activation process takes several minutes.

5. Respond to any prompts on the device, including providing the activation password if requested, accepting any License Agreements, setting up a work profile and creating a device password.
6. If necessary, depending on your server configuration, when the activation pauses, connect the device to a computer on your network using a USB-C cable before continuing.

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.

Activate a Samsung Knox Workspace device

These instructions also apply to Android Enterprise (Work and personal - user privacy) activations. 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 location provided by your administrator.
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 an Android Enterprise device
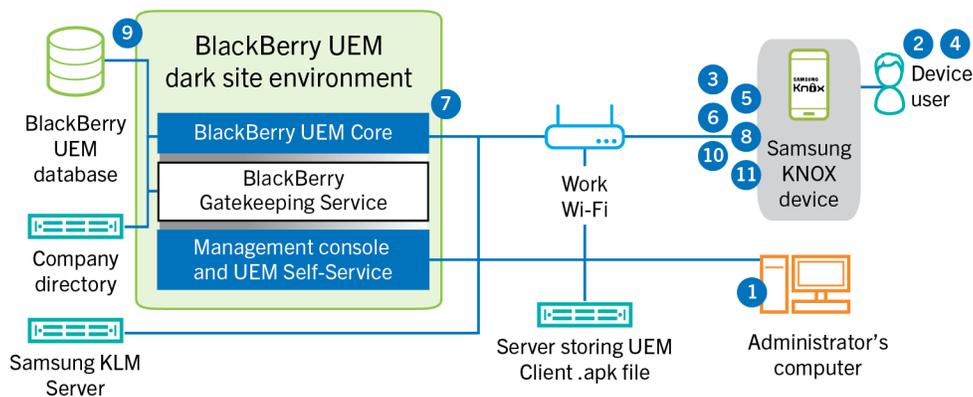
This data flow applies to devices activated with the Android Enterprise (Work space only) or (Work and personal - full control) activation types.

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 that the " Android Enterprise (Work space only)" or "Work and personal - full control" activation type is assigned to the user
   c. Allow activation QR codes to include the activation password and the location to download the BlackBerry UEM Client.
2. The user resets their device to the factory default settings.
3. The device restarts and displays a Welcome or Start screen.
4. The user performs the following actions:

   a. Opens the activation email they received on their computer or another device
   b. Taps the device screen seven times to open a QR code reader
   c. Connects the device to the work Wi-Fi network
   d. Scans the QR code in the activation email
5. The device performs the following actions:

   a. Prompts the user to encrypt the device and restarts
   b. Downloads the UEM Client from the download location specified by the QR code and installs it
6. 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.
7. 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
8. The UEM Client requests all configuration information and sends the device and software information to BlackBerry UEM.
9. BlackBerry UEM stores the device information in the database and sends the requested configuration information to the device.
10. The UEM Client determines if the device uses Knox Platform for Enterprise and is running a supported version. If the device uses Knox Platform for Enterprise, the device connects to the local Samsung on-premises licensing server and activates the Knox management license. After it's activated, the UEM Client applies the appropriate Android Enterprise IT policy rules.
11. The device sends an acknowledgment to BlackBerry UEM that it received and applied the configuration information. The activation process is complete.

Data flow: Activating a device to use Knox Workspace
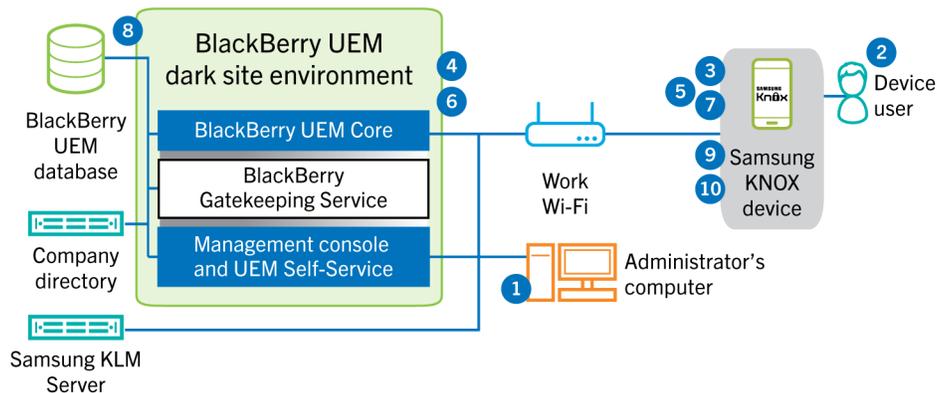
1. You perform the following actions:

   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 on-premises licensing 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 Samsung Knox devices

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

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

Dark site considerations	Description
Connecting to your organization's resources	In a dark site environment, after activation, Samsung Knox devices can connect to BlackBerry UEM and your resources over a VPN connection. For more information see "Set up VPN using Knox StrongSwan".
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 Samsung Knox devices.
Device notifications	Sending notifications to Samsung Knox devices using GCM isn't supported in a dark site environment. The BlackBerry UEM Client will poll BlackBerry UEM for updates at regular intervals.

Set up VPN using Knox StrongSwan

You can set up VPN access to your environment for Samsung Knox devices.

Before you begin: Download the Knox Service Plugin and Android VPN Management for Knox StrongSwan apps and add the .apk files to the shared network location for internal apps.

1. Add the Knox Service Plugin and Android VPN Management for Knox StrongSwan apps to the app list.

2. Select the Knox Service Plugin app and click + to set app configuration options.
    a) Under **VPN profile**, select **Knox built-in VPN**.
    b) Under **Parameters for Knox built-in VPN) for StrongSwan)**, set the following options:
        • Set the **Authentication type** to "ipsec_ike2_rsa".
        • Set the **User certificate alias** to the user name with "_1 [Knox]" appended. You can use variables for the user name (for example `%UserFirstName% %UserLastName% _1 [Knox]`.)
        • Set the **CA certificate alias** to the user name with " [Knox]" appended. You can use variables for the user name (for example `%UserFirstName% %UserLastName% [Knox]`.)

3. Assign the app to the user.

4. Create a CA certificate profile to send the VPN server certificate to devices and assign it to users.

5. Add a VPN client certificate for each user.

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	• 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 iOS, and Android devices
Compatibility matrix	• List of supported operating systems, database servers, and browsers for the BlackBerry UEM server • List of supported device operating systems

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada