BlackBerry UEM

Configuration Guide

12.23

Contents

Configuring BlackBerry UEM

The following table summarizes the initial configuration tasks that are covered in this guide. Review them to determine which tasks you should complete based on your organization's needs. After you complete the appropriate tasks, you are ready to set up administrators, create and manage users and groups, set up device controls, and activate devices.

When you perform the configuration tasks in this guide, use the administrator account that you created when you installed UEM. If you create additional administrator accounts to configure UEM, you should assign the Security Administrator role to the accounts to ensure that the proper level of permissions are granted.

Task	On-prem	Cloud	Description
Change the default certificates that UEM uses for authentication	√		You can replace the default self-signed certificates that UEM uses to authenticate communication between components and with devices.
Install the BlackBerry Connectivity Node		√	You can install and configure the BlackBerry Connectivity Node in a UEM Cloud environment to provide access to your organization's on-premises company directory and to enable secure connectivity features.
Configure UEM to send data through a proxy server	√	√	You can configure UEM to send data through a proxy server before it reaches the BlackBerry Infrastructure. In UEM Cloud environments you can install a standalone BlackBerry Router to function as a proxy server.
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 UEM components to communicate with remote instances of the management console.
Connect to an SMTP server to send email notifications	√		If you want UEM to send activation emails and other notifications to users, you must specify the SMTP server settings that UEM can use.
Connect UEM to company directories	√	√	Connect UEM to your company directories to create user accounts, enable directory-linked groups, and to configure user onboarding and directory synchronization.
Connect BlackBerry UEM to Entra ID to create directory user accounts	√	√	Connect UEM to Entra to create directory user accounts in UEM.
Configure UEM to manage Intune app protection profiles	√	√	Use UEM to create, manage, and assign Microsoft Intune app protection profiles to protect data in Office 365 apps.

Task	On-prem	Cloud	Description
Configure UEM as an Intune compliance partner	√	√	Configure UEM to support Entra ID conditional access.
Register an APNs certificate to manage iOS and macOS devices	√	√	Obtain and register an APNs certificate if you want to manage and send data to iOS and macOS devices.
Configure UEM for the Apple Device Enrollment Program	√	√	You can use the UEM management console to manage iOS devices that your organization purchased from Apple for DEP.
Configure UEM to support Android Enterprise devices	√	√	To support Android Enterprise devices, you must configure your Google Workspace or Google Cloud domain to support third-party mobile device management providers and configure UEM to communicate with your Google Workspace or Google Cloud domain.
Configure UEM to support Android Management devices	√	√	To support Android Management devices, you configure Android Management in the Google Cloud console and then add an Android Management connection in UEM.
Configure UEM to manage Chrome OS devices	√	√	You can configure UEM to support certain Chrome OS management features.
Simplify Windows 10 activations	√	√	You can simplify the process for activating Windows 10 devices so that users don't need to specify a server address.
Migrating users, devices, groups, and other data from a source server	√	√	You can migrate users, devices, groups and other data from supported BlackBerry servers.
Configure network communication and properties for BlackBerry Dynamics apps	√	√	You can configure network communications and other properties for BlackBerry Dynamics apps.
Encrypt the connection between BlackBerry UEM and Microsoft SQL Server	√		You can encrypt the connection between UEM and Microsoft SQL Server.
Integrate UEM with Cisco ISE	√		You can create a connection with Cisco ISE to enable it to retrieve device data from UEM and enforce network access control policies.
Set up VPN using Knox StrongSwan for UEM dark site environments	√		In a UEM dark site environment, you must set up VPN access so that Samsung Knox devices can access your internal servers and resources.

Changing the certificates that BlackBerry UEM uses for secure communication

When you install BlackBerry UEM on-premises, the setup application generates several self-signed certificates that are used to authenticate communication between various UEM components and with devices. You can change the certificates if your organization's security policy requires that certificates be signed by your organization's CA, or if you want to use certificates issued by a CA that devices and browsers already trust.

If problems occur when you change a certificate, communication between UEM components and between UEM and devices can be disrupted. If you choose to change any certificates, plan and test the change carefully.

You can change the following certificates:

Certificate	Description
Apple profile signing certificate	This is the certificate that UEM uses to sign the MDM profile that users must accept when they activate iOS devices. If you are using a certificate signed by a CA, verify that the root certificate for the CA is installed on users' iOS devices before activation.
SSL certificate for consoles	This is the SSL certificate that the management console and UEM Self-Service use to authenticate browsers. If you configure high availability, the certificate must have the name of the UEM domain. You can find the domain name in the management console under Settings > Infrastructure > Instances.
SSL certificates for the BlackBerry Web Services	This is the SSL certificate that the BlackBerry Web Services use to authenticate applications that use the BlackBerry Web Services APIs to manage UEM. If you configure high availability, the certificate must have the name of the UEM domain. You can find the domain name in the management console under Settings > Infrastructure > Instances.
SSL certificate for BlackBerry Dynamics apps	This is the SSL certificate that the BlackBerry Dynamics Launcher uses to establish a secure communication channel with UEM. BlackBerry Dynamics apps that include the integrated BlackBerry Dynamics Launcher can present the certificate to UEM to authenticate with the server.
Certificate for application management	This is the SSL certificate that is used for authentication between UEM and BlackBerry Dynamics apps. The root CA certificate is stored in the list of trusted CA certificates on the device. When the server authenticates with the device, the server presents this certificate to the device for validation. If you change this certificate and the change becomes effective before UEM pushes the certificate to all BlackBerry Dynamics apps, any apps that did not receive the certificate must be reactivated.

Certificate	Description
Certificate for Direct Connect	This is the SSL certificate that is used for authentication between a BlackBerry Proxy server configured for BlackBerry Dynamics Direct Connect and BlackBerry Dynamics apps on devices. When you update this certificate, the new version will always be sent to devices over a non-BlackBerry Dynamics Direct Connect connection. Any devices or containers that are not online at the time of the change will receive the update when they come back online. Updating this certificate should be done on the UEM server and any applicable networking appliances at the same time. For more information on setting up Direct Connect, see Configuring Direct Connect with BlackBerry UEM.
Certificate for BlackBerry Dynamics servers	This is the SSL certificate that authenticates connections between UEM and BlackBerry Proxy.

Considerations for changing BlackBerry Dynamics certificates

Review the following considerations if you want to change any of the BlackBerry Dynamics SSL certificates. If problems occur when you change a certificate, communication between BlackBerry UEM components and between UEM and BlackBerry Dynamics apps could be disrupted. Plan and test certificate changes carefully.

Consideration	Details
Add new certificates to peripheral equipment	If you have added BlackBerry Dynamics certificates to peripheral equipment on your network, add the new certificate to peripheral equipment before adding it to UEM.
Use the latest versions of BlackBerry Dynamics apps	If you are replacing the BlackBerry Dynamics certificate for application management or Direct Connect, ensure that users are using the latest available version of BlackBerry Dynamics apps before you replace the certificate.
BlackBerry Dynamics apps must be open to receive a certificate	A user must open a BlackBerry Dynamics app on their device for it to receive a certificate from UEM. If you are replacing the BlackBerry Dynamics certificate for application management or Direct Connect and the change becomes effective before UEM pushes the certificate to all BlackBerry Dynamics apps, any apps that did not receive the certificate must be reactivated. Apps do not receive certificates while they are suspended on iOS devices or while Android devices are in Doze mode.
Verify that the BlackBerry Connectivity Node is accessible	If any BlackBerry Proxy instances are unreachable by UEM when BlackBerry Dynamics certificates are replaced, BlackBerry Dynamics apps will not be able to connect to those instances following the certificate replacement.
Scheduling certificate changes	If you are replacing the certificate for BlackBerry Dynamics servers, choose a period of low activity to restart the servers. Allow sufficient time for new certificates to propagate to BlackBerry Proxy and BlackBerry Dynamics apps. If you are replacing only the certificate for BlackBerry Dynamics servers, allow at least 10 minutes before the server restarts.

Change a BlackBerry UEM certificate

Before you begin:

- Review the Considerations for changing BlackBerry Dynamics certificates.
- Obtain a certificate signed by a trusted CA. The certificate must be in a keystore format (.pfx, .pkcs12) and must be encrypted with the TripleDES-SHA1 encryption type.

1. In the management console, on the menu bar, click **Settings > Infrastructure > Server certificates**.
2. On the **Server certificates** or **BlackBerry Dynamics certificates** tabs, in the section for the certificate that you want to replace, click **View details**.
3. Click **Replace certificate**.
4. Click **Browse**. Navigate to and select the certificate file.
5. In the **Encryption password** or **Password** field, type a password.
6. Click **Replace**.

After you finish:

- If you replaced any of the certificates on the Server certificates tab, restart the UEM Core service on all servers.
- For certificates on the BlackBerry Dynamics certificates tab, you can click **Revert to default** to switch back to using a self-signed certificate.
- On the BlackBerry Dynamics certificates tab, you can clear the **Trust BlackBerry UEM CA** and **Trust BlackBerry Dynamics CA** check boxes if you do not need to trust the self-signed certificates. You can clear the **Trust BlackBerry Dynamics CA** check box only if you have replaced all of the certificates on the BlackBerry Dynamics certificates tab.
- If BlackBerry Dynamics apps stop communicating after you change the certificates, ensure that the apps are up to date and then instruct users to reactivate the apps.

Installing the BlackBerry Connectivity Node to connect to resources behind your organization's firewall

The BlackBerry Connectivity Node is a collection of components that you can install on a dedicated computer to enable additional features for BlackBerry UEM Cloud. The following components are included in the BlackBerry Connectivity Node.

Component	Purpose
BlackBerry Cloud Connector	The BlackBerry Cloud Connector allows UEM Cloud to access your organization's on-premises company directory. You can create directory user accounts in UEM by searching for and importing user data from the company directory. User data is synchronized with the directory on a schedule that you configure. UEM Cloud must be able to access your company directory if you want to use SCEP. Directory users can use their directory credentials to access BlackBerry UEM Self-Service. If you assign an administrative role to directory users, the users can also use their directory credentials to log into the management console. The BlackBerry Cloud Connector also allows a PKI connector to send certificates to BlackBerry Dynamics apps.
BlackBerry Proxy	BlackBerry Proxy maintains a connection between your organization and the BlackBerry Dynamics NOC that allows BlackBerry Dynamics apps to communicate securely with resources behind your organization's firewall. It also supports BlackBerry Dynamics Direct Connect, which allows app data to bypass the BlackBerry Dynamics NOC. For more information, see Configuring network communication and properties for BlackBerry Dynamics apps.
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus gives users access to work resources behind your organization’s firewall while ensuring the security of data using standard protocols and end-to-end encryption. For more information, see Using BlackBerry Secure Connect Plus for connections to work resources.
BlackBerry Secure Gateway	BlackBerry Secure Gateway provides iOS devices that use the MDM controls activation type with a secure connection to your organization’s mail server through the BlackBerry Infrastructure. For more information, see Protecting email data sent to iOS devices using the BlackBerry Secure Gateway.
BlackBerry Gatekeeping Service	The BlackBerry Gatekeeping Service makes it easier to control which devices can access Exchange ActiveSync. For more information, see Controlling which devices can access Exchange ActiveSync.

The installation and activation files for the BlackBerry Connectivity Node are available in the UEM management console. You can use these files to install new instances of the BlackBerry Connectivity Node and upgrade existing instances.

Steps to install and activate the BlackBerry Connectivity Node

You can install one or more instances of the BlackBerry Connectivity Node to provide redundancy.

Step	Action
1	Review the requirements and considerations for installing the BlackBerry Connectivity Node.
2	Install and configure the BlackBerry Connectivity Node.
3	Optionally, Create a server group to manage regional connections.
4	Perform additional configuration for BlackBerry Secure Connect Plus, BlackBerry Secure Gateway, the BlackBerry Gatekeeping Service, and BlackBerry Dynamics apps.

Requirements: BlackBerry Connectivity Node

Item	Requirements or considerations
Hardware	Install The BlackBerry Connectivity Node on a dedicated computer that is reserved for technical purposes, instead of a computer that is used for everyday work. The computer must be able to access the Internet and your company directory. You cannot install the BlackBerry Connectivity Node on a computer that already hosts an on-premises BlackBerry UEM instance. You can install one or more instances of the BlackBerry Connectivity Node to provide redundancy. You must install each instance on a dedicated computer. Any computer that hosts the BlackBerry Connectivity Node must meet the following requirements: • 6 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 12 GB of available memory • 64 GB of disk space

Item	Requirements or considerations
Single-service performance mode	Optionally, you can designate each BlackBerry Connectivity Node in a server group to handle a single connection type: BlackBerry Secure Connect Plus only, BlackBerry Secure Gateway only, or BlackBerry Proxy only. This can free up resources to support fewer servers for the same number of users or containers. Each BlackBerry Connectivity Node that is enabled for single-service performance mode can support up to 10,000 devices. If you enable single-service performance mode for a BlackBerry Connectivity Node, note the following adjustments to the hardware requirements listed above: • BlackBerry Secure Connect Plus only: 4 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • BlackBerry Secure Gateway only: 8 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • BlackBerry Proxy only: No differences.
Scalability and high availability	Each BlackBerry Connectivity Node can support up to 5000 devices. You can install additional instances to support up to 50,000 additional devices. You can deploy more than one BlackBerry Connectivity Node in a server group to allow for high availability and load balancing.
Software	Any computer that hosts a BlackBerry Connectivity Node instance must meet the following requirements: • A supported OS • Windows PowerShell 2.0 or later; required for the setup application to install RRAS for BlackBerry Secure Connect Plus and the BlackBerry Gatekeeping Service • Install the required version of the JRE and set the BB_JAVA_HOME variable. For more information, see Set an environment variable for the Java location.
Directory connections	Verify that you are using a supported directory service. You can configure one or more directory connections, but if you have multiple BlackBerry Connectivity Node instances, all of the directory connections must be configured identically. If one directory connection is missing or incorrectly configured, that BlackBerry Connectivity Node will appear as disabled in the management console.
Ports	Verify that the following outbound ports are open in your organization's firewall so that the BlackBerry Connectivity Node components and any associated proxy servers can communicate with the BlackBerry Infrastructure: • 443 (HTTPS) to activate the BlackBerry Connectivity Node • 3101 (TCP) for all other outbound connections

Item	Requirements or considerations
Administrator accounts	When you install and configure the BlackBerry Connectivity Node, use administrator accounts that meet the following requirements: • Use a Windows account with permissions to install and configure software on the computer. • Choose a directory account with read permissions for each directory connection that you want to configure. • Use a UEM Cloud administrator account with permissions to download the BlackBerry Connectivity Node installation and activation files (for example, Security Administrator).

Install and configure the BlackBerry Connectivity Node

Before you begin:

- Review the requirements and considerations for installing the BlackBerry Connectivity Node.
- In the management console, on the menu bar, click **Settings > External integration > BlackBerry Connectivity Node setup**. Click and download the setup application for the BlackBerry Connectivity Node. If you want to add the BlackBerry Connectivity Node instance to an existing server group when you activate it, in the **Server group** drop-down list, click the appropriate server group. Generate and save the activation file. The activation file is valid for 60 minutes.
- Transfer the setup application and the activation file to the computer that you want host the BlackBerry Connectivity Node instance. Complete the steps below on that computer.
- If you want to install the BlackBerry Connectivity Node using the command prompt, see Install the BlackBerry Connectivity Node for UEM Cloud using the command prompt.

1. Run the BlackBerry Connectivity Node setup application.
2. Choose your language. Click **OK**.
3. Click **Next**.
4. Select your country or region. Read and accept the license agreement. Click **Next**.
5. The installation program verifies that your computer meets the installation requirements. Click **Next**.
6. To change the installation file path, click **...** and navigate to the file path that you want to use. Click **Install**.
7. When the installation completes, click **Next**.

   The address of the BlackBerry Connectivity Node console is displayed (http:/localhost:8088). Click the link and save the site in your browser.
8. Select your language. Click **Next**.
9. When you activate the BlackBerry Connectivity Node, it sends data over port 443 (HTTPS) to the BlackBerry Infrastructure (for example na.bbsecure.com or eu.bbsecure.com). After it is activated, the BlackBerry Connectivity Node uses port 3101 (TCP) for all other outbound connections through the BlackBerry Infrastructure. If you want to send data from the BlackBerry Connectivity Node through an existing transparent TCP proxy server behind your organization's firewall, click **Click here to configure the proxy settings for your organization's environment**, select the **Proxy server** option, and do any of the following:

   - To send activation data through a transparent TCP proxy server, in the **Enrollment proxy** fields, type the FQDN or IP address and the port number of the proxy server. The proxy server must be able to send data over port 443 to bbsecure.com. Click **Save**.

- To send other outbound connections from the components of the BlackBerry Connectivity Node through a transparent TCP proxy server, in the appropriate fields, type the FQDN or IP address and the port number of the proxy server. The proxy server must be able to send data over port 3101 to bbsecure.com. Click **Save**.

10. In the **Friendly name** field, type a name for the BlackBerry Connectivity Node. Click **Next**.
11. Click **Browse**. Select the activation file.
12. Click **Activate**.

    If you want to add a BlackBerry Connectivity Node instance to an existing server group when you activate it, your organization's firewall must allow connections from that server over port 443 through the BlackBerry Infrastructure to activate the BlackBerry Connectivity Node and to the same bbsecure.com region as the main BlackBerry Connectivity Node instance.
13. Click + and select the type of company directory that you want to configure.
14. Follow the steps for your organization's directory type:

Directory type	Steps
Microsoft Active Directory	**a.** In the **Connection name** field, type a name for the directory connection. If you have a Microsoft Entra ID directory configured, this connection name must be different than the name of the Entra directory connection. **b.** In the **Username** field, type the username of the Microsoft Active Directory account. **c.** In the **Domain** field, type the FQDN of the domain that hosts Microsoft Active Directory. For example, domain.example.com. **d.** In the **Password** field, type the password of the Microsoft Active Directory account. **e.** In the **Domain controller discovery** drop-down list, click one of the following: • If you want to use automatic discovery, click **Automatic**. • If you want to specify the domain controller computer, click **Select from list below**. Click + and type the FQDN of the computer. Repeat this step to add more computers. **f.** In the **Global catalog search base** field, type the search base that you want to access (for example, OU=Users,DC=example,DC=com). To search the entire Global Catalog, leave the field blank. **g.** In the **Global catalog discovery** drop-down list, click one of the following: • If you want to use automatic catalog discovery, click **Automatic**. • If you want to specify the catalog computer, click **Select from list below**. Click + and type the FQDN of the computer. If necessary, repeat this step to specify more computers. **h.** If you want to enable support for linked Microsoft Exchange mailboxes, in the **Support for linked Microsoft Exchange mailboxes** drop-down list, click **Yes**. To configure the Microsoft Active Directory account for each forest that you want UEM Cloud to access, in the **List of account forests** section, click +. Specify the forest name, user domain name (the user can belong to any domain in the account forest), username, and password. **i.** To synchronize more user details from your company directory, select the **Synchronize additional user details** check box. The additional details include company name and office phone. **j.** Click **Save**.

Directory type	Steps
LDAP directory	If you want to use an LDAP directory configuration to connect to Active Directory, and your organization's Active Directory uses the new policy settings to enforce channel binding and signing requirements, you must use LDAPS (SSL) to connect (see steps c and d). **a.** In the **Connection name** field, type a name for the directory connection. If you have a Microsoft Entra ID directory configured, this connection name must be different than the name of the Entra directory connection. **b.** In the **LDAP server discovery** drop-down list, click one of the following: • If you want to use automatic discovery, click **Automatic**. In the **DNS domain name** field, type the DNS domain name. • If you want to specify the LDAP computer, click **Select server from list below**. Click + and type the FQDN of the computer. Repeat this step to add more computers. **c.** In the **Enable SSL** drop-down list, select whether you want to enable SSL authentication for LDAP traffic. If you click **Yes**, click **Browse** and select the SSL certificate for the LDAP computer. **d.** In the **LDAP port** field, type the TCP port number for communication (default 636 SSL enabled, 389 SSL disabled). **e.** If the LDAP connection is SSL encrypted, beside the **LDAP server SSL certificate** field, click **Browse** and select the LDAP server certificate. **f.** In the **Authorization required** drop-down list, select whether UEM Cloud must authenticate with the LDAP computer. If you click **Yes**, type the username and password of the LDAP account in DN format (for example, CN=John Smith,OU=Sales,DC=example,DC=com). **g.** In the **Search base** field, type the search base to access (for example, OU=Users,DC=example,DC=com). **h.** In the **LDAP user search filter** field, type the filter to use for LDAP users. For example: (&(objectCategory=person)(objectclass=user)(memberOf=CN=Local,OU=Users,DC=example,DC=com)). **i.** In the **LDAP user search scope** drop-down list, click one of the following: • If you want user searches to apply to all levels below the base DN, click **All levels**. • If you want to limit user searches to one level below the base DN, click **One level**. **j.** In the **Unique identifier** field, type the immutable and globally unique attribute for each user's unique identifier (for example, uid). **k.** In the **First name** field, type the attribute for each user's first name (for example, givenName). **l.** In the **Last name** field, type the attribute for each user's last name (for example, sn). **m.** In the **Login attribute** field, type the attribute for each user's login attribute (for example, cn). Users will use this to log in to UEM Self-Service with directory credentials. **n.** In the **Email address** field, type the attribute for each user's email (for example, mail). **o.** In the **Display name** field, type the attribute for each user's display name (for example, displayName). **p.** In the **User Principal Name** field, type the user principal name for SCEP (for example, mail). **q.** If you are using the LDAP directory configuration to connect to Active Directory, and if you want to use SCEP profiles to distribute user credential certificates to devices, in the **User Security Identifier** field, enter `objectSid`. **r.** To synchronize more user details from your company directory, select the **Synchronize additional user details** check box and fill in the desired fields. **s.** To enable directory-linked groups, select the **Enable directory-linked groups** check box. For more information about directory-linked groups, see Enable directory-linked groups. **t.** Click **Save**.

15. In the management console, click **Settings > External integration > BlackBerry Connectivity Node setup**.
16. In the **Step 4: Test connection** section, click **Next**.

To view the status of a BlackBerry Connectivity Node instance, in the management console, on the menu bar, click **Settings > External integration > BlackBerry Connectivity Node status**.

After you finish:

- To install additional BlackBerry Connectivity Node instances, download the installation and activation files again and repeat this task on a different computer. This should be done after the first instance is activated.
- If you install more than one BlackBerry Connectivity Node, you must configure identical directory connections on each instance. You can use the BlackBerry Connectivity Node console to export the directory connections for an instance (.txt file), then transfer and import those connections to a different BlackBerry Connectivity Node using the console for that instance. Note that the exported (.txt file) will not include any passwords, and they will need to be re-entered before importing it into any other BlackBerry Connectivity Node. Remove any existing directory connections from an instance before you import directory configurations.
- Optionally, Create a server group to manage regional connections.
- If you want to send data through an HTTP proxy before it reaches the BlackBerry Dynamics NOC, in the BlackBerry Connectivity Node console, click **General settings > BlackBerry Router and proxy**. Select the **Enable HTTP proxy** check box and configure the proxy settings.
- If you want to change the default settings for BlackBerry Connectivity Node instances, in the management console, on the menu bar, click **Settings > External integration > BlackBerry Connectivity Node setup** and click  . You can change logging settings, disable instances of the BlackBerry Gatekeeping Service, and configure BlackBerry Secure Gateway settings.
- When you are notified of an update to the BlackBerry Connectivity Node, repeat this task to upgrade each instance. Use the BlackBerry Connectivity Node console to record or export directory configurations. You must upgrade all instances of the BlackBerry Connectivity Node to the same version. When you upgrade the first instance, directory services are disabled until all of the nodes are upgraded to the same version.
- For instructions for enabling BlackBerry Secure Connect Plus, see Using BlackBerry Secure Connect Plus for connections to work resources in the Administration content.
- For instructions for enabling the BlackBerry Secure Gateway, see Protecting email data sent to iOS devices using the BlackBerry Secure Gateway in the Administration content.
- For instructions for configuring the BlackBerry Gatekeeping Service, see Controlling which devices can access Exchange ActiveSync in the Administration content.

Install the BlackBerry Connectivity Node for UEM Cloud using the command prompt

In a UEM Cloud environment, you can install or upgrade an instance of the BlackBerry Connectivity Node using the command prompt window.

Before you begin:

- You must review the BlackBerry Solution License Agreement for your jurisdiction ("BBSLA"). You must acknowledge your acceptance of the BBSLA when you run the command to install the BlackBerry Connectivity Node. By acknowledging your acceptance of the BBSLA or by installing or using the software, you agree to the terms and conditions of the BBSLA.
- Download the setup application for the BlackBerry Connectivity Node (Settings > External integration > BlackBerry Connectivity Node setup) and transfer it to the computer that you want to host the instance.
- Verify that the computer meets the requirements for the BlackBerry Connectivity Node.

1. Extract the setup application.
2. Open a command prompt as an administrator and change the directory to the location where you extracted the BlackBerry Connectivity Node setup application.

3. Run the following command:

```
setup.exe -s -a --iAcceptBESEULA [--properties service.account.name=<domain
\service_account_username>,service.account.password=<service_account_password>,
 install.path=<install_directory>,logging.common.path=<log_file_directory>]
```

Argument	Description
-s or --silent	This argument enables a silent install. If not included, the command will launch the UI for the setup application.
-a or --executionArgs	This argument must be used to accept other required arguments.
--iAcceptBESEULA	This argument indicates acceptance of the BBSLA, and is required to install the software.
--properties	This argument can be used to specify the following optional arguments: • service.account.name=<*domain\service_account_username*> • service.account.password=<*services_account_password*> • install.path=<*install_directory*> • logging.common.path=<*log_file_directory*> Optional arguments must be included as a comma-separated list. If you do not specify a service account name and password, the setup application uses the credentials of the account that you are using to run the command prompt. If you do not specify an installation path, the default installation path is used (C:/Program Files/BlackBerry/BlackBerry Connectivity Node). If you do not specify a log file directory, the default directory is used (C:/Program Files/BlackBerry/BlackBerry Connectivity Node/Logs).

Create a server group to manage regional connections

If you want to manage regional connections for the enterprise connectivity features offered by the BlackBerry Connectivity Node, you can deploy multiple instances of the BlackBerry Connectivity Node in a dedicated region as a server group. When you create a server group, you specify the regional data path that you want the components to use to connect to the BlackBerry Infrastructure. Server groups also support redundancy, high availability, and load balancing for BlackBerry Connectivity Node instances.

Before you begin: Install and configure multiple instances of the BlackBerry Connectivity Node.

1. In the management console, on the menu bar, click **Settings > External integration > BlackBerry Connectivity Node setup**.
2. Click  .
3. Type a name and description for the server group.
4. In the **Country** drop-down list, select the appropriate country.
5. If you want to disable the company directory connection for the instances in the server group, select the **Override Directory Service settings** check box.
6. By default, the BlackBerry Gatekeeping Service in each BlackBerry Connectivity Node instance is active. If you want gatekeeping data to be managed only by the main BlackBerry Connectivity Node instance, select the

Override BlackBerry Gatekeeping Service settings check box to disable each BlackBerry Gatekeeping Service in the server group.

7. If you want to use DNS settings for BlackBerry Secure Connect Plus that are different from the default settings (Settings > Infrastructure > BlackBerry Secure Connect Plus), select the **Override DNS servers** check box. Do the following:
   a) In the **DNS servers** section, click +. Type the DNS server address in dot-decimal notation (for example, 192.0.2.0). Click **Add**. Repeat as necessary.
   b) In the **DNS search suffix** section, click +. Type the DNS search suffix (for example, domain.com). Click **Add**. Repeat as necessary.
8. If you want to configure logging settings for the BlackBerry Connectivity Node instances in the server group, select the **Override logging settings** check box. Do any of the following:
   - In the **Server log debug levels** drop-down list, select the appropriate log level.
   - If you want to route log events to a syslog server, select the **Syslog** check box and specify the host name and port of the syslog server.
   - If you want to change local log settings, select the **Enable local file destination** check box. Specify the size limit (in MB), the age limit (in days), and select whether you want to compress log folders.
   - If you want to configure different log levels for BlackBerry Connectivity Node components, in the **Service logging override** section, click + and select the appropriate component and log level. Repeat as necessary.
9. If you want to use the instances in the server group for only one type of connection, select the **Enable single-service performance mode** check box. In the **Connection type** drop-down menu, select the connection type (BlackBerry Secure Connect Plus only, BlackBerry Secure Gateway only, or BlackBerry Proxy only).
10. If you want to specify the BlackBerry Secure Gateway settings for the instances in the server group, select the **Override BlackBerry Secure Gateway settings** check box. For iOS devices that use modern authentication to connect to Microsoft Exchange Online, specify the discovery endpoint and mail server resource:
    a) Select the **Enable OAuth for mail server authentication** check box.
    b) In the **Discovery endpoint** field, specify the URL to use for discovery requests. Enter the discovery endpoint in the format https://<*identity provider*>/.well-known/openid-configuration (for example, `https://login.microsoftonline.com/common/.well-known/openid-configuration`) or `https://login.windows.net/common/.well-known/openid-configuration`).
    c) In the **Mail server resource** field, specify the URL of the mail server resource to use for authorization and token requests using OAuth. For example, `https://outlook.office365.com`.
11. Click **Save**.

After you finish: Select the server group and click to add BlackBerry Connectivity Node instances to it. You can add an instance to a server group or remove an instance from a server group at any time.

Troubleshooting: BlackBerry Connectivity Node

Problem	Possible solution
The BlackBerry Connectivity Node does not activate with UEM Cloud.	• Verify that you uploaded the latest activation file that you generated in the management console. Only the latest activation file is valid. • An activation file expires after 60 minutes. Generate and upload a new activation file, then try to activate again. • See KB 38964.

Problem	Possible solution

The BlackBerry Connectivity Node does not connect with UEM Cloud.	• Verify that the following outbound ports are open in your organization's firewall so that the BlackBerry Connectivity Node components (and any associated transparent proxy servers) can communicate with the BlackBerry Infrastructure (*region*.bbsecure.com):
	  • 443 (TCP) to activate the BlackBerry Connectivity Node
	  • 3101 (TCP) for all other outbound connections
	• Review the most recent log file for information about why the BlackBerry Connectivity Node cannot connect with UEM Cloud. By default, the log files are located in <*drive:*>:\Program Files\BlackBerry \BlackBerry Connectivity Node\Logs.

The BlackBerry Connectivity Node does not connect with the company directory.	• If you have multiple instances of the BlackBerry Connectivity Node, verify that they are all at the same version. • Verify that you specified the correct settings for the company directory. • Verify that all instances have a directory connection and that the directory connections are configured the same on all instances. • Verify that you specified the correct login information for the directory account and that the account has the necessary permissions to access the company directory. • Verify that the correct ports are open in your organization's firewall. • Verify that you did not use the same activation file for two different installations. • Verify that you are using the most recent activation file. • Review the most recent log file for details about why the BlackBerry Connectivity Node cannot access the company directory. By default, the log files are located in <*drive:*>:\Program Files\BlackBerry \BlackBerry Connectivity Node\Logs. • If you are using Microsoft Active Directory, see KB 36955.

Configuring BlackBerry UEM to send data through a proxy server

You can use the following proxy configurations in your BlackBerry UEM environment:

Environment	Proxy options
UEM on-premises	You can configure UEM to send data through a TCP proxy server before it reaches the BlackBerry Infrastructure. By default, UEM connects directly to the BlackBerry Infrastructure using port 3101. If your organization's security policy requires that internal systems cannot connect directly to the Internet, you can install a TCP proxy server. The TCP proxy server acts as an intermediary between UEM and the BlackBerry Infrastructure. You can install a proxy server outside your organization’s firewall in a DMZ. Installing a TCP proxy server in a DMZ provides an extra level of security for UEM. Only the proxy server connects to UEM from outside the firewall. All connections to the BlackBerry Infrastructure between UEM and devices go through the proxy server.
UEM Cloud	To use a proxy server with the BlackBerry Connectivity Node, you can install the BlackBerry Router to act as a proxy server, or you can use a TCP proxy server that is already installed in your organization's environment. You can install the BlackBerry Router or a proxy server outside your organization’s firewall in a DMZ. Installing the BlackBerry Router or a TCP proxy server in a DMZ provides an extra level of security. Only the BlackBerry Router or the proxy server connects to the BlackBerry Connectivity Node from outside the firewall. All connections to the BlackBerry Infrastructure between the BlackBerry Connectivity Node and devices go through the proxy server. By default, the BlackBerry Connectivity Node connects directly to the BlackBerry Infrastructure using port 3101. If your organization's security policy requires that internal systems cannot connect directly to the Internet, you can install the BlackBerry Router or a TCP proxy server. The BlackBerry Router or TCP proxy server acts as an intermediary between the BlackBerry Connectivity Node and the BlackBerry Infrastructure.

Sending data through a TCP proxy server to the BlackBerry Infrastructure

In UEM on-premises environments, you can configure a transparent TCP proxy server for the BlackBerry UEM Core service. This service requires an outbound connection and may also have different ports configured. You cannot install or configure multiple transparent TCP proxy servers for each service.

In UEM Cloud environments, the BlackBerry Connectivity Node sends activation data over port 443 (TCP). After it is activated, the BlackBerry Connectivity Node sends and receives data over port 3101 (TCP). You can configure the BlackBerry Connectivity Node to route TCP data through a transparent proxy server that is behind your organization’s firewall. The BlackBerry Connectivity Node does not support authentication with a proxy server.

You can configure multiple TCP proxy servers configured with SOCKS v5 (no authentication) to connect to UEM. Multiple TCP proxy servers configured with SOCKS v5 (no authentication) can provide support if one of the active proxy server instances is not functioning correctly.

You configure only a single port that all SOCKS v5 service instances must listen on. If you are configuring more than one TCP proxy server with SOCKS v5, each server must share the proxy listening port.

Configure BlackBerry UEM to use a transparent TCP proxy server

Before you begin: Install a compatible transparent TCP proxy server in the UEM domain.

1. Follow the steps for your environment:

Environment	Steps
UEM on-premises	**a.** In the management console, on the menu bar, click **Settings > Infrastructure > BlackBerry Router and proxy**. **b.** Under **Global settings**, select **Proxy server**. **c.** For each service that you want to use the proxy server, specify the FQDN or IP address and port number of the transparent proxy server. Each field requires a single value.
UEM Cloud	**a.** In the BlackBerry Connectivity Node console (http:/localhost:8088), click **General settings > Proxy**. **b.** Select **Proxy server**. **c.** If you want to route activation data for the BlackBerry Connectivity Node through a transparent proxy server, in the **Enrollment proxy** fields, type the FQDN or IP address and the port number of the proxy server. The transparent proxy server must send data over port 443 to <*region*>.bbsecure.com without authentication or negotiation. **d.** If you want to route outbound connections from the components of the BlackBerry Connectivity Node through a transparent proxy server, in the appropriate fields, type the FQDN or IP address and the port number of the proxy server. The transparent proxy server must be able to send data over port 3101 to <*region*>.bbsecure.com without authentication or negotiation.

2. Click **Save**.

Enable SOCKS v5 on a TCP proxy server

Before you begin: Install a compatible TCP proxy server with SOCKS v5 (no authentication) in the UEM domain.

1. Do one of the following:
   - In a UEM on-premises environment, in the management console, on the menu bar, click **Settings > Infrastructure > BlackBerry Router and proxy**.
   - In a UEM Cloud environment, in the BlackBerry Connectivity Node console (http:/localhost:8088), click **General settings > Proxy**.
2. Select **Proxy server**.
3. Select the **Enable SOCKS v5** check box.
4. Click +.
5. In the **Server address** field, type the IP address or host name of the SOCKS v5 proxy server.
6. Click **Add**.
7. Repeat steps 2 to 6 for each SOCKS v5 proxy server that you want to configure.

8. In the **Port** field, type the port number.
9. Click **Save**.

Install a standalone BlackBerry Router in a UEM Cloud environment

The BlackBerry Router is an optional component that you can install in a DMZ outside your organization's firewall. The BlackBerry Router connects to the Internet to send data between the BlackBerry Connectivity Node and devices that use the BlackBerry Infrastructure. The BlackBerry Router functions as a proxy server and can support SOCKS v5 (no authentication).

You can configure multiple instances of the BlackBerry Router for high availability. You configure only one port for BlackBerry Router instances to listen on. By default, the BlackBerry Connectivity Node connects to the BlackBerry Router using port 3102. The BlackBerry Router supports all outbound traffic from the BlackBerry Connectivity Node components.

Before you begin: You must install a standalone BlackBerry Router on a computer that does not host an instance of the BlackBerry Connectivity Node.

1. In the UEM management console, on the menu bar, click **Settings > External integration > BlackBerry Connectivity Node setup**.
2. Click .
3. Click **Download**.
4. On the software download page, answer the required questions and click **Download**. Save and extract the installation package.
5. In the **router** folder, extract the **setupinstaller** .zip file. This .zip file contains an **Installer** folder with the **Setup.exe** file that you use to install the BlackBerry Router.
6. Transfer the **Setup.exe** file to the computer that you want to install the BlackBerry Router on and double-click it to run the setup application.

   The installation runs in the background and displays no dialog boxes. Once the installation completes, the BlackBerry Router service appears in the Services window.
7. In the BlackBerry Connectivity Node console (http:/localhost:8088), click **General settings > Proxy**.
8. Select **BlackBerry Router**.
9. Click .
10. Type the IP address or host name of the BlackBerry Router instance that you want to connect to UEM.
11. Click **Add**.
12. In the **Port** field, type the port number that all BlackBerry Router instances listen on. The default value is 3102.
13. Click **Save**.

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 your BlackBerry UEM on-premises environment to:

- Allow the UEM Core to communicate with the management console if it is installed on a separate computer.
- Allow UEM to communicate with other internal services, such as certification authorities and servers hosting push applications.

Server-side proxy settings do not apply to outbound connections. For information about configuring UEM to use a TCP proxy server, see Configuring BlackBerry UEM to send data through a proxy server.

1. In the management console, on the menu bar, click **Settings > Infrastructure > Server-side proxy**.
2. Do one of the following:

Task	Steps
Configure global proxy settings for most or all of the servers in your UEM domain.	**a.** Expand **Global server-side proxy settings**. **b.** In the **Type** drop-down list, click **PAC Configuration** or **Manual Configuration**. **c.** Complete the required fields. **d.** Click **Save**.
Configure proxy settings for one or more servers that are different from the global proxy settings.	**a.** Expand the server name. **b.** In the **Type** drop-down list, click **None**, **PAC Configuration**, or **Manual Configuration**. **c.** Complete the required fields. **d.** Click **Save**.

Connect to an SMTP server to send email notifications

You must connect BlackBerry UEM on-premises to an SMTP server to enable it to send activation instructions, device compliance warnings, passwords for UEM Self-Service, and email notifications to device users.

1. In the management console, on the menu bar, click **Settings > External integration > SMTP server**.
2. Click .
3. In the **Sender display name** field, type a name to use for email notifications from UEM (for example, `donotreply` or `UEM Admin`).
4. In the **Sender address** field, type the email address that you want UEM to use to send email notifications.
5. In the **SMTP server** field, type the FQDN of the SMTP server.
6. In the **SMTP server port** field, type the SMTP server port number. The default port number is 25.
7. In the **Supported encryption type** drop-down list, select the appropriate encryption type.
8. If the SMTP server requires authentication, specify the username and password.
9. If necessary, import an SMTP CA certificate:
   a) Copy the SSL certificate file for your organization's SMTP server to the computer that you are using.
   b) Click **Browse**.
   c) Navigate to and select the SSL certificate file and click **Upload**.
10. Click **Save**.

After you finish: Click **Test connection** if you want to test the connection to the SMTP server and send a test email message. UEM sends the message to the email address you specified in the **Sender address** field.

Connecting to your company directories

You can connect BlackBerry UEM to your organization's company directory to take advantage of the following features:

- You can create user accounts in UEM using user data from the directory, and UEM can authenticate administrators for the management console and users for BlackBerry UEM Self-Service.
- You can link company directory groups with UEM groups to organize users in the same way that they are organized in your company directory, and to simplify the assignment and management of IT policies, profiles, and apps for users. These are called directory-linked groups.
- You can enable onboarding for specific groups in your company directory to create UEM users automatically. These are called onboarding directory groups. When you add new users to these directory groups, new user accounts are created for these users in UEM. If you enable onboarding, you can also configure offboarding to delete device data and UEM user accounts when users are disabled or removed from the company directory.

If you do not connect UEM to a company directory, you can manually create local user accounts and authenticate administrators using default authentication.

Step	Action
1	In a UEM on-premises environment, Connect to a Microsoft Active Directory instance or Connect to an LDAP directory. In a UEM Cloud environment, install and configure the BlackBerry Connectivity Node to connect to your company directory. For instructions for connecting UEM on-premises or UEM Cloud to Entra ID, see Connect BlackBerry UEM to Entra ID to create directory user accounts.
2	Optionally, Enable directory-linked groups.
3	Optionally, Enable and configure onboarding and offboarding.
4	Optionally, configure directory synchronization.

Connect to a Microsoft Active Directory instance

The task below applies to a UEM on-premises environment. In a UEM Cloud environment, install and configure the BlackBerry Connectivity Node to connect to your company directory.

Before you begin:

- Create a Microsoft Active Directory account that UEM can use. The account must meet the following requirements:
  - It must be located in a Windows domain that is part of the Microsoft Exchange forest.
  - It must have permission to access the user container and read the user objects stored in the global catalog servers in the Microsoft Exchange forest.
  - The password must be configured not to expire and does not need to be changed at the next login.

  - If you enable single sign-on, constrained delegation must be configured for the account.
  - The UEM server must also be joined to the Active Directory domain.
- Review the port requirements for connections from UEM to Active Directory.
- If your organization uses a Microsoft Exchange resource forest, you must create a mailbox in the resource forest for each user account and associate them with the user accounts in the account forests. UEM uses the mailboxes to look up the user accounts in the individual domains. To authenticate users who log in to UEM, UEM must read the user information that is stored in the global catalog servers that are part of the resource forest. You must create an Active Directory account for UEM that is located in a Windows domain that is part of the resource forest. When you create the directory connection, you provide the Windows credentials for the Active Directory account, and, if required, the names of the global catalog servers that UEM can use.

1. In the UEM management console, on the menu bar, click **Settings > External integration > Company directory**.
2. Click + **> Microsoft Active Directory connection**.
3. In the **Directory connection name** field, type a name for the directory connection.
4. In the **Username** field, type the username of the Active Directory account.
5. In the **Domain** field, type the name of the Windows domain that is part of the Microsoft Exchange forest, in DNS format (for example, example.com).
6. In the **Password** field, type the account password.
7. In the **Kerberos Key Distribution Center selection** drop-down list, do one of the following:
   - To permit UEM to automatically discover the key distribution centers (KDCs), click **Automatic**.
   - To specify the list of KDCs for UEM to use for authentication, click **Manual**. In the **Server names** field, type the name of the KDC domain controller in DNS format (for example, kdc01.example.com). Optionally, include the port number that the domain controller uses (for example, kdc01.example.com:88). Click + to specify additional KDC domain controllers that you want UEM to use.
8. In the **Global catalog selection** drop-down list, do one of the following:
   - If you want UEM to automatically discover the global catalog servers, click **Automatic**.
   - To specify the list of global catalog servers for UEM to use, click **Manual**. In the **Server names** field, type the DNS name of the global catalog server that you want UEM to access (for example, globalcatalog01.example.com). Optionally, include the port number that the global catalog server uses (for example, globalcatalog01.com:3268). Click + to specify additional servers.
9. Click **Continue**.
10. In the **Global catalog search base** field, do one of the following:
    - To permit UEM to search the entire global catalog, leave the field blank.
    - To control which user accounts UEM can authenticate, type the distinguished name of the user container (for example, OU=sales,DC=example,DC=com).
11. If you want to enable support for global groups, in the **Support for global groups** drop-down list, click **Yes**.

    If you want to use global groups for onboarding, you must select **Yes**. To configure a global group domain, in the **List of global group domains** section, click +. In the **Domain** field, click the domain that you want to add. The default selection for the **Specify username and password?** field is No. If you keep this default selection, the username and password for the forest connection is used. If you select Yes, you must provide valid credentials for an Active Directory account in the domain that you selected. In the **KDC selection** field, you can select Automatic to permit UEM to automatically discover the key distribution centers, or Manual to specify the list of KDCs for UEM to use for authentication. Click **Add**.
12. If your environment contains a Microsoft Exchange resource forest, to enable support for linked Microsoft Exchange mailboxes, in the **Support for linked Microsoft Exchange mailboxes** drop-down list, click **Yes**.

    To configure the Active Directory account for each forest that you want UEM to access, in the **List of account forests** section, click +. Specify the user domain name (the user may belong to any domain in the account

forest), and the username and password. If necessary, specify the KDCs that you want UEM to search. If necessary, specify the global catalog servers that you want UEM to access. Click **Add**.

13. To enable single sign-on, select the **Enable Windows single sign-on** check box. For more information about single sign-on, see Configure single sign-on for BlackBerry UEM in the Administration content.
14. To synchronize more user details from your company directory, select the **Synchronize additional user details** check box. The additional details include company name and office phone.
15. Click **Save**.
16. Click **Close**.

After you finish:

- Do any of the following optional tasks:
  - Enable directory-linked groups.
  - Enable and configure onboarding and offboarding.
  - Configure directory synchronization.
- If you want to remove a directory connection, you must first remove all of the associated directory users and directory-linked groups from UEM.

Connect to an LDAP directory

The task below applies to a UEM on-premises environment. In a UEM Cloud environment, install and configure the BlackBerry Connectivity Node to connect to your company directory.

Before you begin:

- Create an LDAP account for UEM that is located in the relevant LDAP directory. The account must meet the following requirements:
  - The account must have permission to read all users in the directory.
  - The password must be configured to not expire and does not need to be changed at the next login.
- If the LDAP connection is SSL encrypted, verify that you have the server certificate for the LDAP connection and that the LDAP server supports TLS 1.2. If SSL is enabled, the LDAP connection to UEM must use TLS 1.2.
- Verify the LDAP attribute values that your organization uses (the steps below give examples for typical attribute values), you will use them in the steps below.
- If you want to use an LDAP directory configuration to connect to Active Directory, and your organization's Active Directory uses the new policy settings to enforce channel binding and signing requirements, you must use LDAPS (SSL) to connect (see steps 5 and 6). For more information, see Microsoft KB4520412.

1. In the UEM management console, on the menu bar, click **Settings > External integration > Company directory**.
2. Click + **> LDAP connection**.
3. In the **Directory connection name** field, type a name for the directory connection.
4. In the **LDAP server discovery** drop-down list, do one of the following:
   - To automatically discover the LDAP server, click **Automatic**. In the **DNS domain name** field, type the domain name for the server that hosts the company directory.
   - To specify a list of LDAP servers, click **Select server from list below**. In the **LDAP server** field, type the name of the LDAP server. To add more LDAP servers, click +.
5. In the **Enable SSL** drop-down list, perform one of the following actions:
   - If the LDAP connection is SSL encrypted, click **Yes**. Beside the **LDAP server SSL certificate** field, click **Browse** and select the LDAP server certificate.

- If the LDAP connection is not SSL encrypted, click **No**.

6. In the **LDAP port** field, type the TCP port number for communication. The default values are 636 for SSL enabled or 389 for SSL disabled.
7. In the **Authorization required** drop-down list, do one of the following:
   - If authorization is required for the connection, click **Yes**. In the **Login** field, type the DN of the user that is authorized to log in to LDAP (for example, an=admin,o=Org1). In the **Password** field, type the password.
   - If authorization is not required for the connection, click **No**.
8. In the **User search base** field, type the value to use as the base DN for user information searches.
9. In the **LDAP user search filter** field, type the LDAP search filter that is required to find user objects in your organization's directory server. For example, for an IBM Domino Directory, type `(objectClass=Person)`.
10. In the **LDAP user search scope** drop-down list, do one of the following:
    - To search all objects following the base object, click **All levels**. This is the default setting.
    - To search objects that are one level directly following the base DN, click **One level**.
11. In the **Unique identifier** field, type the name of the attribute that uniquely identifies each user in your organization's LDAP directory (must be a string that is immutable and globally unique). For example, `dominoUNID`.
12. In the **First name** field, type the attribute for each user's first name (for example, `givenName`).
13. In the **Last name** field, type the attribute for each user's last name (for example, `sn`).
14. In the **Login attribute** field, type the login attribute to use for authentication (for example, `uid`).
15. In the **Email address** field, type the attribute for each user's email address (for example, `mail`). If you do not set the value, a default value is used.
16. In the **Display name** field, type the attribute for each user's display name (for example, `displayName`). If you do not set the value, a default value is used.
17. In the **User Principal Name** field, type the user principal name for SCEP (for example, `mail`).
18. If you are using the LDAP directory configuration to connect to Active Directory, and if you want to use SCEP profiles to distribute user credential certificates to devices, in the **User Security Identifier** field, you must enter the following: `objectSid`
19. In the **Department** field, type the attribute for each user's department.
20. In the **Job Title** field, type the attribute for each user's job title.
21. If you want to synchronize additional fields from the LDAP directory, select the **Synchronize additional user details** check box. Type the attributes for the additional fields as necessary.
22. To enable directory-linked groups for the directory connection, select the **Enable directory-linked groups** check box.
    a) In the **Group search base** field, type the value to use as the base DN for group information searches.
    b) In the **LDAP group search filter** field, type the LDAP search filter that is required to find group objects in your company directory. For example, for IBM Domino Directory, type `(objectClass=dominoGroup)`.
    c) In the **Group Unique Identifier** field, type the attribute for each group's unique identifier. This attribute must be immutable and globally unique (for example, type `cn`).
    d) In the **Group Display name** field, type the attribute for each group's display name (for example, type `cn`).
    e) In the **Group Membership attribute** field, type the name of the attribute for group membership. The attribute values must be in DN format (for example, `CN=jsmith,CN=Users,DC=example,DC=com`).
    f) In the **Test Group Name** field, type an existing group name for validating the group attributes specified.
    g) If you want to enable paged searching for group members, select the **Enable paged group search** check box.
23. Click **Save**.
24. Click **Close**.

After you finish:

- Do any of the following optional tasks:
  - Enable directory-linked groups.
  - Enable and configure onboarding and offboarding.
  - Configure directory synchronization.
- If you want to remove a directory connection, you must first remove all of the associated directory users and directory-linked groups from UEM.

Enable directory-linked groups

You can link groups in BlackBerry UEM to groups in your company directory to organize users in UEM the same way that they are organized in the directory, and to simplify the assignment and management of IT policies, profiles, and apps for users. For more information, see Creating and managing user groups in the Administration content.

Before you begin:

- Connect to your organization's directory:
  - UEM on-premises: Connect to a Microsoft Active Directory instance or Connect to an LDAP directory.
  - UEM Cloud: Install and configure the BlackBerry Connectivity Node to connect to Microsoft AD or LDAP.
  - On-premises or Cloud: Connect BlackBerry UEM to Entra ID to create directory user accounts.
- Verify that a company directory synchronization is not in progress. You cannot save the changes you make to the company directory connection until the synchronization is complete.

1. In the management console, on the menu bar, click **Settings > External integration > Company directory**.
2. Click a company directory connection.
3. On the **Sync settings** tab, select the **Enable directory-linked groups** check box.
4. If you want to force the synchronization of company directory groups, select the **Force synchronization** check box.

   If enabled, when a group is removed from the company directory, the links to that group are removed from directory-linked groups and onboarding directory groups. If all of the company directory groups associated with a directory-linked group are removed, the directory-linked group is converted to a local group.
5. In the **Sync limit - percent of users to be off-boarded or removed** field, specify the maximum percentage of users in a group that can be removed or offboarded in a synchronization activity. If this maximum is exceeded, UEM does not carry out any removal or offboarding actions on the group during a synchronization. For example, if you specify the limit as 80%, if 81% or more of the users in a group would be removed or offboarded in a synchronization activity, UEM will not remove or offboard any users from that group. By default, the limit is 100%, which means that UEM will not carry out removal or offboarding actions on a group if all of the users that belong to that group are impacted.
6. In the **Sync limit - minimum group size threshold field**, specify the minimum number of users that a directory group must contain before UEM will apply the maximum limit that you specified in **Sync limit - percent of users to be off-boarded or removed**. The maximum sync limit percentage does not apply to groups with fewer users than the minimum group size that you specify. The default minimum threshold is 10 (a group must contain at least 10 users for UEM to factor in the maximum sync limit percentage; the maximum synch limit does not apply to groups of 9 or less users). Type 0 if you want UEM to apply the maximum sync limit to all groups regardless of group size.
7. In the **Maximum nesting level of directory groups** field, type the number of nested levels to synchronize for company directory groups.
8. Click **Save**.

After you finish:

- Optionally, Enable and configure onboarding and offboarding.
- Optionally, configure directory synchronization.
- Create directory-linked groups. For more information, see Creating and managing user groups in the Administration content.

Enable and configure onboarding and offboarding

When you enable onboarding, you add universal or global directory groups to UEM as onboarding directory groups (onboarding is not supported for domain local groups). During a synchronization process, if UEM detects a directory user in an onboarding directory group that does not have a corresponding UEM user account, it creates that user account in UEM. When you enable onboarding you can also configure offboarding; when you disable or remove a user from an onboarding directory group, UEM can delete device data and remove the user from UEM.

Note: When offboarding is enabled, any UEM user accounts that are not members of an onboarding directory group, regardless of how they were added to UEM, are offboarded during the next synchronization process.

Before you begin:

- Connect to your organization's directory:
  - UEM on-premises: Connect to a Microsoft Active Directory instance or Connect to an LDAP directory.
  - UEM Cloud: Install and configure the BlackBerry Connectivity Node to connect to Microsoft AD or LDAP.
  - On-premises or Cloud: Connect BlackBerry UEM to Entra ID to create directory user accounts.
- Verify that a company directory synchronization is not in progress. You cannot save the changes you make to the company directory connection until the synchronization is complete.
- To onboard members of global groups, you must enable support for global groups in your Microsoft Active Directory connection settings.

1. In the management console, on the menu bar, click **Settings > External integration > Company directory**.
2. Click a company directory connection.
3. On the **Sync settings** tab, select the **Enable directory-linked groups** check box.
4. Select the **Enable onboarding** check box.
5. Do any of the following:

Task	Steps
Add onboarding directory groups and configure device activation options.	**a.** Click +. **b.** Search for and add universal or global directory groups. **c.** For each directory group, select whether you want to link nested groups. **d.** In the **Device activation** section, select whether you want onboarded users to receive an autogenerated activation password and email, or no activation password. If you select the autogenerated password option, configure the activation period and select an activation email template.

Task	Steps
Onboard users that you only want to use BlackBerry Dynamics apps.	Follow these steps if you want to onboard users who will use BlackBerry Dynamics apps only. These users will not activate their devices on UEM using the UEM Client and their devices will not be managed by UEM. **a.** Select the **Onboard users with BlackBerry Dynamics apps only** check box. **b.** Click +. **c.** Search for and add universal or global directory groups. **d.** For each directory group, select whether you want to link nested groups. **e.** Specify the number of access keys to generate per user, the access key expiration period, and the email template.
Configure offboarding.	If you want to delete device data when a user is offboarded from UEM, select the **Delete device data when the user is removed from all onboarding directory groups** check box. Do the following: • Select the appropriate option for the data that you want to remove from the device. • If you want to remove a user from UEM when that user is removed from all onboarding directory groups, select the **Delete user when the user is removed from all onboarding directory groups** check box. • If you want to delay the deletion of users and device data for two hours after a synchronization cycle, select the **Offboarding protection** check box. This option can help avoid unexpected deletions because of directory replication latency.

6. In the **Sync limit - percent of users to be off-boarded or removed** field, specify the maximum percentage of users in a group that can be removed or offboarded in a synchronization activity. If this maximum is exceeded, UEM does not carry out any removal or offboarding actions on the group during a synchronization. For example, if you specify the limit as 80%, if 81% or more of the users in a group would be removed or offboarded in a synchronization activity, UEM will not remove or offboard any users from that group. By default, the limit is 100%, which means that UEM will not carry out removal or offboarding actions on a group if all of the users that belong to that group are impacted.
7. In the **Sync limit - minimum group size threshold field**, specify the minimum number of users that a directory group must contain before UEM will apply the maximum limit that you specified in **Sync limit - percent of users to be off-boarded or removed**. The maximum sync limit percentage does not apply to groups with fewer users than the minimum group size that you specify. The default minimum threshold is 10 (a group must contain at least 10 users for UEM to factor in the maximum sync limit percentage; the maximum synch limit does not apply to groups of 9 or less users). Type 0 if you want UEM to apply the maximum sync limit to all groups regardless of group size.
8. If you want to force the synchronization of company directory groups, select the **Force synchronization** check box.

   If enabled, when a group is removed from the company directory, the links to that group are removed from directory-linked groups and onboarding directory groups. If all of the company directory groups associated with a directory-linked group are removed, the directory-linked group is converted to a local group.
9. In the **Maximum nesting level of directory groups** field, type the number of nested levels to synchronize for company directory groups.
10. Click **Save**.

After you finish: Optionally, configure directory synchronization.

Synchronize a directory connection

After you connect UEM to your organization's company directory, you can manually start the synchronization process at any time or you can schedule recurring synchronizations. You can preview a synchronization report before the next synchronization occurs, and you can view the report after a synchronization process completes.

Before you begin:

- Connect to your organization's directory:
  - UEM on-premises: Connect to a Microsoft Active Directory instance or Connect to an LDAP directory.
  - UEM Cloud: Install and configure the BlackBerry Connectivity Node to connect to Microsoft AD or LDAP.
  - On-premises or Cloud: Connect BlackBerry UEM to Entra ID to create directory user accounts.
- Optionally, Enable directory-linked groups and Enable and configure onboarding and offboarding.

1. In the management console, on the menu bar, click **Settings > External integration > Company directory**.
2. Do any of the following:

Task	Steps
Preview a synchronization.	**a.** Click for the directory connection that you want to preview the synchronization for. **b.** Click **Preview now**. **c.** When the report finishes processing, click on the date in the **Last report** column.
Manually start a directory synchronization.	**a.** Click for the directory connection that you want to synchronize. **b.** When the synchronization is complete, click on the date in the **Last report** column. **c.** To export a .csv file of the report, click .
Add a synchronization schedule.	**a.** Click the directory connection that you want to schedule synchronization for. **b.** On the **Sync schedule** tab, click +. **c.** In the **Synchronization type** drop-down list, choose one of the following: • **All groups and users**: Users are onboarded and offboarded as required, group membership changes are synchronized, and changes to user attributes are synchronized. • **On-boarding groups**: Users are onboarded and offboarded as required and changes to user attributes are synchronized. • **Directory linked groups**: Group membership changes are synchronized and changes to user attributes are synchronized. • **User attributes**: Only changes to user attributes are synchronized. **d.** In the **Recurrence** drop-down list, select the appropriate option and configure the recurrence settings as necessary. **e.** Click **Add**. **f.** Click **Save**.

Connect BlackBerry UEM to Entra ID to create directory user accounts

You can connect BlackBerry UEM to Microsoft Entra ID to create directory user accounts in UEM. After you configure the connection, you can search for and import user data from the directory to create UEM users. Directory users can use their directory credentials to access BlackBerry UEM Self-Service. If you assign an administrative role to a directory user, the user can use their directory credentials to log in to the management console.

If your organization uses an on-premises Active Directory and accounts are synchronized to Entra ID, you should create a directory connection for your on-premise Active Directory instead (see Connect to a Microsoft Active Directory instance). Connecting UEM to Entra ID is appropriate when Entra ID is your primary directory service and you do not have an on-premises Active Directory.

Note: After you connect UEM to Entra ID, the UEM console URLs change to the following ("&redirect=no" is removed from the end of the URL):

- Management console: https://<*server_name*>:<*port*>/admin/index.jsp?tenant=<*tenant_ID*>
- Self-service console: https://<*server_name*>:<*port*>/mydevice/index.jsp?tenant=<*tenant_ID*>

Before you begin: You must have a Microsoft Entra ID account. If you don't have an account, visit https://azure.microsoft.com to create an account. Use this account to log in to the Entra portal.

1. Log in to the Entra portal.
2. In the section for Entra ID app registrations, add a new registration.
3. Specify the following and complete the registration:
   a) Type a name for the registration.
   b) Select which account types can use the application or access the API.
   c) For the redirect URI, click **Web** and type `http://localhost`.
4. Copy the application ID.
   This is the Client ID that you will register with UEM.
5. In the section for managing API permissions (Register button), add a permission and select the following:
   - **Microsoft Graph**
   - **Application permissions**
   - Set the following permissions: **Group.Read.All (Application)**, **User.Read.All (Application)**
   - Verify that the **User.Read** delegated permission is granted.
6. Grant administrator consent for all accounts in the current directory.
7. In the section for managing certificates and secrets, add a new client secret and specify a description and duration.
8. Copy the Value field of the new client secret (not the Secret ID).
   This is the Client key that you will register with UEM.
9. In the UEM management console, on the menu bar, click **Settings > External integration > Company directory**.
10. Click + > **Microsoft Entra ID connection**.
11. In the **Directory connection name** field, type a name for the connection.
12. In the **Domain** field, type the Entra ID domain.
13. In the **Client ID** field, type the ID you recorded in step 4.
14. In the **Client key** field, type the value you recorded in step 8.
15. Click **Continue**.

16. Click **Save**.

After you finish: You can complete any of the following optional tasks:

- Enable directory-linked groups
- Enable and configure onboarding and offboarding
- Synchronize a directory connection

Configuring BlackBerry UEM to manage Microsoft Intune app protection profiles

If you want to use BlackBerry UEM to create, manage, and assign Microsoft Intune app protection profiles to protect data in Office 365 apps, you must do the following:

Step	Action
1	Review the Prerequisites to support Intune app protection.
2	Create an app registration in Entra.
3	Configure BlackBerry UEM to synchronize with Microsoft Intune.

Prerequisites to support Intune app protection

- To synchronize BlackBerry UEM with Intune, you must use a Microsoft administrator account with an Intune license and with one of the following permissions in the Entra portal: global administrator, limited administrator with the Intune Service administrator role.
- User accounts that you want to assign Intune app protection profiles to must exist in Entra ID.
- Users must be added to UEM as directory users.
- If you integrated your on-premise Microsoft Active Directory, then users must be synchronized to Entra ID. For more information, see the Microsoft documentation for Entra ID Connect.

Create an app registration in Entra

You must create an app registration in Entra that UEM can use to authenticate with Entra.

Before you begin:

- Review the Prerequisites to support Intune app protection.
- In the UEM management console, on the menu bar, click **Settings > External integration > Microsoft Intune**. Record the value of the **Reply URL**. You will use this URL in step 3.

1. Log in to the Entra portal.
2. In the section for app registrations, add a new registration.
3. Specify the following and complete the registration:
   a) Type a name for the registration.
   b) Select which account types can use the application or access the API.
   c) For the redirect URI, click **Public client/native (mobile & desktop)** and enter the Reply URL from the management console.
4. Register, then copy the application ID. The application ID is the Client ID that you will register with UEM.
5. In the section for managing API permissions, add a permission and select the following:

- **Microsoft Graph**
- **Delegated permissions**
- Set the following delegated permissions:
  - **Read and write Microsoft Intune apps (DeviceManagementApps > DeviceManagementApps.ReadWrite.All)**
  - **Read all groups (Group > Group.Read.All)**
  - **Read all users' basic profile (User > User.ReadBasic.All)**

6. Grant administrator consent for all accounts in the current directory.
7. In the section for managing certificates and secrets, add a new client secret and specify a description and duration.
8. Copy the Value field of the new client secret (not the Secret ID).

   This is the Client key that you will register with UEM.

After you finish: Configure BlackBerry UEM to synchronize with Microsoft Intune.

Configure BlackBerry UEM to synchronize with Microsoft Intune

Before you begin: Create an app registration in Entra.

1. In the management console, on the menu bar, click **Settings > External Integration > Microsoft Intune**.
2. In the **Entra tenant ID** field, type the ID of your organization's Entra ID tenant.
3. In the **Client ID** field, type the ID that you recorded in Create an app registration in Entra.
4. In the **Client key** field, type the value that you recorded in Create an app registration in Entra.
5. Click **Next**.
6. Specify the credentials of the Intune administrator account that you want to use for the synchronization process.

After you finish:

- See Managing apps protected by Microsoft Intune in the Administration content.
- If you need to re-enter the credentials of the Intune administrator account (for example, you change the password of the account), in **Settings > External Integration > Microsoft Intune**, click **Update credentials**.

Configuring BlackBerry UEM as an Intune compliance partner in Entra

If you have configured Entra ID conditional access for your organization, you can configure BlackBerry UEM as a compliance partner so that iOS and Android devices that are managed by UEM can be recognized as compliant by Intune when accessing your cloud-based apps such as Office 365.

You can configure more than one UEM tenant for each Entra tenant, but all UEM tenants will share the same partner compliance management entry. Entra cannot differentiate which UEM tenant a compliance status update originates from. You can configure a UEM tenant to connect to one or more Entra tenants. You must add a directory connection to UEM for each Entra tenant.

When users activate their devices on UEM, UEM reports the device compliance status to Entra. The compliance requirement is satisfied without having to enroll devices directly with Intune. UEM will notify Entra when a device is out of compliance or when a device returns to compliance.

If you do not want to use the "Required device to be marked as compliant" conditional access control in Entra, and you want to use trusted locations to control access from devices that are inside your network, you can accomplish this in UEM by routing traffic to Microsoft services through your organization's BlackBerry Connectivity Node instances. In this scenario, you do not need to follow the instructions in this section to connect UEM to Entra ID for conditional access.

Prerequisites to configure Entra ID conditional access

Prerequisite	Description
Microsoft account	Verify that you have a Microsoft account with an Intune license and with one of the following Entra ID roles (or a custom role with equivalent permissions): • Global Administrator • Intune Service Administrator
Requirements for device users	• Users must exist in Entra ID and must have a valid Intune license. For more information, see Microsoft Intune licenses. • If you synchronize your on-premises Active Directory with Entra ID, users' on-premises Active Directory UPN must match their Entra ID UPN. • Users must be added to UEM as directory users. UEM can connect to Entra ID or Microsoft AD for the directory connection. Use Entra ID if your organization's users are cloud-only. Use AD if users are hybrid (on-premises AD synchronized to Entra ID). In either scenario UPN alignment beween UEM and Entra ID is critical for compliance evaluation.
Microsoft Endpoint Manager configuration	In the Microsoft Endpoint Manager admin center, in the section for Partner Compliance Management, add BlackBerry UEM Conditional Access as a compliance partner for iOS and Android devices and assign the compliance partner configuration to users and groups. For more information, see Microsoft Intune: Support third-party device compliance partners in Intune.

Prerequisite	Description
Entra ID configuration	In Entra ID, create and configure a conditional access policy and enable the option "Require device to be marked as compliant". Note that this is the only conditional access profile setting that UEM interacts with. The conditional access policy is required if you want to enforce access control based on compliance status. Without the conditional access policy, compliance is tracked but not enforced.

After you verify the prerequisites above, follow the steps in Configure Entra ID conditional access.

- Note that the configuration steps will instruct you to enable the UEM Client to enroll in BlackBerry Dynamics and to install the UEM Client on devices.
- The steps will instruct you to install the Microsoft Authenticator app on users' devices before activation with UEM. If you want to delay conditional access enrollment on the device until the Microsoft Authenticator app is installed (either manually by the user or deployed with UEM), you can enable the "Start Entra Conditional Access enrollment after authentication broker is installed" setting in the assigned BlackBerry Dynamics profile. Note that this option is not supported for Android devices with the User privacy activation type (it does apply to Android Enterprise user privacy and Android Management user privacy). If enabled, after the Microsoft Authenticator app is installed, the conditional access enrollment process is initiated when the user opens the UEM Client. On Android devices, if the work space is unlocked, the user will be prompted to open the UEM Client to start the conditional access enrollment.

Configure Entra ID conditional access

Before you begin: Verify that you meet the prerequisites for Entra ID conditional access.

1. In the UEM management console, on the menu bar, click **Settings > External integration > Entra ID Conditional Access**.
2. Click +.
3. Type a name for the configuration.
4. In the **Entra cloud** drop-down list, click **GLOBAL**.
5. In the **Entra tenant ID** field, type your organization's tenant name in FQDN format or unique tenant ID in GUID format.
6. Under **Device mapping override**, click **UPN** or **Email**.

   If you choose UPN, verify that the Entra ID tenant and all mapped directories share the same UPN value for users before you save the connection. After you save the connection, you cannot change the device mapping override.
7. In the **Available company directories** list, select and add the appropriate company directories.
8. Click **Save**.
9. Select the administrator account that you want to use to log in to your organization's Entra tenant.
10. When prompted, authenticate with your Entra tenant using the appropriate Microsoft account.
11. On the menu bar, click **Policies and Profiles > Policy > BlackBerry Dynamics**. Perform the following steps for any BlackBerry Dynamics profile that you plan to assign to device users (for example, the default profile and any custom profiles).
    a) Open and edit the profile.
    b) Select **Enable UEM Client to enroll in BlackBerry Dynamics**.

c) If you want to delay the conditional access enrollment process until the Microsoft Authenticator app is installed on devices, select **Start Entra Conditional Access enrollment after authentication broker is installed**.
d) Click **Save**.
e) Assign the profile to users and groups as necessary.

12. On the menu bar, click **Policies and Profiles > Networks and Connections > BlackBerry Dynamics connectivity**. Perform the following steps for any BlackBerry Dynamics connectivity profile that you plan to assign to device users (for example, the default profile and any custom profiles).
    a) Open and edit the profile.
    b) In the **App servers** section, click **Add**.
    c) Search for and click **Feature - Azure Conditional Access**.
    d) Click **Save**.
    e) In the **Azure Conditional Access** table, click +.
    f) In the **Server** field, type `gdas-<UEM_SRP_ID>.<region_code>.bbsecure.com`.
    g) In the **Port** field, type 443.
    h) Under **Route type**, click **Direct**.
    i) Click **Save**.
    j) Assign the profile to users and groups as necessary.
13. Create and configure a compliance profile and assign the profile to users and groups as necessary. The following table details how UEM compliance actions are reported to Intune:

UEM compliance enforcement action	Behavior
Enforcement action: Monitor and log	Nothing is reported to Intune.
Enforcement action: • Untrust • Delete only work data • Delete all data	UEM notifies Entra ID after all user prompts have expired.
Enforcement action for BlackBerry Dynamics apps: Monitor and log	Nothing is reported to Intune.
Enforcement action for BlackBerry Dynamics: • Do not allow BlackBerry Dynamics apps to run • Delete BlackBerry Dynamics app data	UEM notifies Entra ID as soon as the compliance violation is detected.

14. Optionally, if your conditional access policies include network-based restrictions (for example, blocking access from untrusted locations or allowing access only from the work network), you can route Microsoft Authenticator traffic through BlackBerry Secure Connect Plus to ensure the traffic comes from a trusted network path. Follow the instructions in Using BlackBerry Secure Connect Plus for connections to work resources to create and assign an enterprise connectivity profile. Use the following configuration:

Platform	Configuration
iOS	**a.** In the enterprise connectivity profile, select **Enable per-app VPN**. **b.** Add the Microsoft Authenticator app to UEM so you can deploy it to users and groups. **c.** When you assign the Microsoft Authenticator app to users and groups, in the **Per-app VPN** drop-down list, select the enterprise connectivity profile.
Android	**a.** In the enterprise connectivity profile, if you want to use per-app routing, select **Enable per-app VPN** and add the app package ID of the Microsoft Authenticator app. Otherwise, select **Container wide VPN**. **b.** Assign the enterprise connectivity profile to the appropriate users and groups.

15. Assign the **Feature – Azure Conditional Access** app to users or groups. For more information, see Manage user accounts and Manage a user group.
16. Install both the UEM Client and the Microsoft Authenticator app on users' devices. You can assign and deploy the Microsoft Authenticator app with UEM (see Adding public apps to the app list), or you can instruct users to download it themselves.
17. Instruct users to activates their devices.

    When a user activates their device, the UEM Client prompts the user to register with Entra conditional access (Microsoft Online Device Registration). Users with activated devices are prompted to register with Entra conditional access the next time they open the UEM Client.

    Note: Instruct users to initiate the registration with Entra using the UEM Client, not using any sign-in options within Microsoft Authenticator. The registration prompt from the UEM Client will open Microsoft Authenticator to prompt the user for credentials and to complete the registration process.

After you finish:

- Depending on the email client that your organization wants to use, you must complete additional steps to ensure that the mail client can validate and communicate with Entra:
  - For BlackBerry Work, see Configuring the BlackBerry Work app configuration for Entra ID conditional access in the BlackBerry Work Administration Guide.
  - For the iOS native mail client, see KB 94163.
  - For Android Gmail, see KB 94494.
- After a user activates a device with UEM, you can check the user's device properties in Microsoft Endpoint Manager to confirm that it was registered with Entra as expected. The name of the device will be in the following format: <*username*> - <*platform*> unknown unknown - <*xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx*>.
- If you change the scope of users or groups in the Entra partner compliance configuration, in the Entra portal, navigate to the security permissions for BlackBerry UEM Conditional Access and grant administrator consent for BlackBerry again.
- When you remove a device from UEM, the device remains registered for Entra ID conditional access. Users can remove their Entra ID account from the account settings in the Microsoft Authenticator app, or you can remove the device from the Entra portal.

Obtaining an APNs certificate to manage iOS and macOS devices

APNs is the Apple Push Notification Service. You must obtain and register an APNs certificate if you want to use BlackBerry UEM to manage iOS or macOS devices. If you set up more than one UEM domain, each domain requires an APNs certificate.

You can obtain and register the APNs certificate using the first login wizard or by using the external integration section of the management console.

Each APNs certificate is valid for one year. The management 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. You can note the Apple ID in the management console. You can also create an email event notification to remind you to renew the certificate 30 days before it expires. If the certificate expires, devices do not receive data from UEM. If you register a new APNs certificate, device users must reactivate their devices to receive data.

It is a best practice to access the management console and the Apple Push Certificates Portal using Google Chrome or Safari, as these browsers provide optimal support for requesting and registering an APNs certificate.

Request and register an APNs certificate

1. In the management console, on the menu bar, click **Settings > External integration > Apple Push Notification**.
2. In section **Step 1 of 3 - Download signed CSR certificate from BlackBerry**, click **Download certificate**.
3. Save the signed CSR file to your computer.
4. In section **Step 2 of 3 - Request APNs certificate from Apple**, click **Apple Push Certificate Portal**.
5. Sign in to the Apple Push Certificates Portal using a valid Apple ID.
6. Follow the instructions to upload the signed CSR.
   If an invalid file type error displays, you can rename the file to a .txt file and upload it again.
7. Download and save the APNs certificate on your computer.
8. In the management console, in section **Step 3 of 3 - Register APNs certificate**, click **Browse**.
9. Navigate to and select the APNs certificate.
10. Click **Submit**.

After you finish:

- To test the connection between UEM and the APNs server, click **Test APNs certificate**.
- The APNs certificate is valid for one year. You must renew the APNs certificate each year before it expires, using the same Apple ID that you used to obtain the original APNs certificate. To renew the certificate, repeat the steps above but click **Renew certificate** at step 2.

Troubleshooting: APNs

Problem	Possible solution
When you try to obtain a signed CSR, you get the following error: "The system encountered an error. Try again."	See KB 37266.
When you try to register the APNs certificate, you receive the error "The APNs certificate does not match the CSR."	If you downloaded multiple CSR files from BlackBerry, only the last one that you downloaded is valid. If you know which CSR is the most recent, return to the Apple Push Certificates Portal and upload it. If you are not sure which CSR is the most recent, obtain a new one from BlackBerry, then return to the Apple Push Certificates Portal and upload it.
You cannot activate iOS or macOS devices.	The APNs certificate may not be registered correctly. Check the following: • In the management console, on the menu bar, click **Settings > External integration > Apple Push Notification**. Verify that the APNs certificate status is "Installed." If the status is not correct, try to register the APNs certificate again. • Click **Test APNs certificate** to test the connection between BlackBerry UEM and the APNs server. • If necessary, obtain a new signed CSR from BlackBerry and a new APNs certificate.

Configure BlackBerry UEM for DEP

You can configure BlackBerry UEM to synchronize with the Apple Device Enrollment Program (DEP) if you want to use the UEM management console to manage the activation of the iOS devices that your organization purchased for DEP.

1. In the management console, navigate to **Settings > External integration > Apple Device Enrollment Program**.

   If you are using UEM on-premises, click + and type a name for the account.
2. In section **1 of 4: Create an Apple DEP account**, click **Create an Apple DEP account**.
3. Complete the fields and follow the prompts to create your account.
4. In section **2 of 4: Download a public key**, click **Download public key**.
5. Save the public key on your local machine.
6. In section **3 of 4: Generate server token from Apple DEP account**, click **Open the Apple DEP portal**.
7. Sign in to Apple Business Manager. In the preferences for your account, download the server token for the MDM server. For more information, see the Apple Business Manager User Guide: Link to a third-party MDM server in Apple Business Manager.
8. In section **4 of 4: Register the server token with BlackBerry UEM**, click **Browse**.
9. Navigate to and select the .p7m server token file. Click **Open** then click **Next**.
10. In the enrollment configuration window, type a name for the configuration.
11. If you want UEM to automatically assign the enrollment configuration to devices when you register them with Apple DEP, select the **Automatically assign all new devices to this configuration** check box. Do not select this option if you want to use the UEM management console to manually assign the enrollment configuration to specific devices.

    Note: UEM synchronizes with Apple DEP daily and whenever you view the Apple DEP devices page. You can automatically assign only one enrollment configuration to new DEP devices. If you previously created an enrollment configuration with this setting, the setting is removed from the previous configuration and added to the new one. If you previously created an enrollment configuration with this setting and the configuration was applied to devices, UEM does not assign the new enrollment configuration.
12. Optionally, type a department name and support phone number to be displayed on devices during setup.
13. In the **Device configuration** section, select any of the following options:

    - **Allow pairing**: Users can pair the device with a computer.
    - **Mandatory**: Users can activate devices using their company directory username and password.
    - **Allow removal of MDM profile**: Users can deactivate devices.
    - **Wait until device is configured**: Users cannot cancel the device setup until activation with UEM is complete.
14. In the **Skip during setup** section, select the items that you do not want to include in the device setup. Hover over an option to view a tooltip with additional details.
15. Click **Save**. If you selected **Automatically assign new devices to this configuration** click **Yes**.

After you finish:

- Activate iOS devices. For more information about activating devices that are enrolled in DEP, see Activating iOS devices that are enrolled in DEP.
- The server token is valid for one year. You must renew the token each year before it expires. To see the status of the token, see the Expiry date in the Apple Device Enrollment Program window. To renew the token, in **Settings > External integration > Apple Device Enrollment Program**, click the DEP account and click **Update server token**. Complete both steps to generate a new server token and register it with UEM.
- You can remove any DEP connection that you create. If you remove all DEP connections, you cannot activate new Apple DEP devices. If you assigned enrollment configurations to devices and the configurations have not

been applied, UEM removes the enrollment configurations assigned to the devices. Removing the connection does not affect devices that are active on UEM.

Configuring BlackBerry UEM to support Android Enterprise devices

Android Enterprise devices provide additional security for organizations that want to manage Android devices. The following table summarizes the different options for configuring BlackBerry UEM to support Android Enterprise devices:

Method	When to choose this method	User account type	Supported Google services
Connect one UEM domain to a Google Workspace domain.	Your organization uses a Google Workspace domain.	Google Workspace accounts (for organizations)	• All Google Workspace services such as Gmail, Google Calendar, and Drive • App management through Google Play
Connect one UEM domain to a Google Cloud domain.	Your organization uses a Google Cloud domain.	Google Cloud accounts, also known as Managed Google accounts (for organizations)	• Similar to Google Workspace but without access to paid products such as Gmail, Google Calendar, and Drive • App management through Google Play
Allow UEM to manage Android Enterprise devices as managed Google Play accounts.	Your organization doesn't use a Google domain or uses a Google domain that is already connected to one UEM domain and you want to use Android Enterprise devices on a second UEM domain.	Android Enterprise devices that have managed Google Play accounts	• App management through Google Play • Google Services are not supported

Configure BlackBerry UEM to support Android Enterprise devices

Before you begin: If you previously connected a UEM domain to a Google domain and you want to connect a new UEM domain, you must remove the existing connection. In the management console, on the menu bar, click **Settings > External integration > Google domain connection** and remove the connection. You can also remove the connection from the Admin Settings in Google Play (https://play.google.com/work) using the same Google account you used to create the connection. When you remove a connection, all devices that are activated with an Android Enterprise activation type will be deactivated.

1. In the management console, on the menu bar, click **Settings > External integration > Android and Chrome Management**.
2. Do one of the following:

Task	Steps
Use Android Enterprise devices that have managed Google Play accounts.	a. Select **Allow BlackBerry UEM to manage Google Play Accounts**. b. Click **Next**. c. In the Google prompt, specify the email address of the Google or Gmail account that will become the administrator account for the Bring Android to Work service. Follow the prompts to complete the registration process.
Use a Google domain.	a. Select **Connect BlackBerry UEM to your existing Google domain**. Note that you cannot share Google domains between multiple UEM domains. This option supports Android Enterprise and Chrome OS Enterprise. b. Click **Next**. c. Complete the fields to create a service account and click **Next**.

3. Do one of the following:
   - To send app configuration details using the BlackBerry Infrastructure, select **Send app configuration using UEM Client**.
   - To send app configurations details using the Google infrastructure, select **Send app configuration using Google Play**.
4. When prompted, click **Accept** to accept the permissions set for some or all of the displayed Google and BlackBerry apps.
5. Click **Done**.

After you finish:

- Complete the steps to activate Android Enterprise devices. For more information about device activation, see Activating Android devices in the Administration content.
- You can edit the Google domain connection from Settings > External integration to change the type of Google domain that you use or to test the domain connection.
- If you ever plan to decommission a UEM domain that is connected to a Google, remove the connection before you decommission the domain (Settings > External integration > Google domain connection). You can also remove the connection from the Admin Settings in Google Play (https://play.google.com/work) using the same Google account you used to create the connection. When you remove a connection, all devices that are activated with an Android Enterprise activation type will be deactivated.

Configuring BlackBerry UEM to support Android Management devices

Android Management devices provide additional security for organizations that want to manage devices using the Android Management API.

Before activating devices with Android Management activation types, review the Considerations for Android Management activation types.

Step	Action
1	Configure Android Management in the Google Cloud console.
2	Configure Android Management in BlackBerry UEM.

Configure Android Management in the Google Cloud console

You must set up Android Enterprise using a managed Google Play account before you can access the option to configure Android Management.

When you set up Android Management, you must use a dedicated Gmail email address. You cannot use an email address that was used to set up Android Enterprise.

1. Go to https://console.developers.google.com and sign in using the Gmail email address that will be used for Android Management.
2. In the Cloud Console, click **New Project**.
3. Click **APIs and Services > Select Library**.
4. In the search bar, search for Android Management API.
5. In the list of search results, enable **Android Management API** and **Cloud Pub/Sub API**.
6. In the Cloud Console, on the menu bar, click **IAM & Admin > Service Accounts > Select > Create Service Account**.
7. In the **Grant this service account access to the project** section, in the **Role** drop-down list, select **Android Management User**.
8. In the second **Role** drop-down list, select **Pub/Sub Admin**.
9. In the **Grant users access to the service account** section, enter the email address that you used in step 1.
10. Click **Done**.
11. On the menu bar, click **Service Accounts** and select the account that you created.
12. Click **Keys > Add Key**.
13. In the **Create a private key for "***<service_account_name>***"** dialog box, select **JSON**. Click **Create**.
14. Record the service account name, the Gmail email address you used for the Android Management administrator (step 1), and the JSON private key.

After you finish: Configure Android Management in BlackBerry UEM.

Configure Android Management in BlackBerry UEM

Before you begin:

- Configure Android Management in the Google Cloud console.
- Verify that Android Enterprise has already been configured in UEM. See Configuring BlackBerry UEM to support Android Enterprise devices.
- Verify that you have the Android Management service account name, the Gmail email address of the Android Management administrator, and the JSON private key.

1. In the UEM management console, on the menu bar, click **Settings > External Integration > Android and Chrome Management**.
2. Click **Add Android Management connection**.
3. In the **Enterprise display name** field, specify the name of the service account.
4. In the **Administrator email address** field, specify the Gmail email address of the Android Management administrator account.
5. In the **Service account info (json format)** field, specify the JSON private key.
6. Click **Save**.
7. In the **Domain name or Business name** dialog box, in the **Your answer** field, enter the Android Management service account name. Click **Next**.

Extending the management of Chrome OS devices to BlackBerry UEM

You can integrate BlackBerry UEM with a Google managed domain to extend some Chrome OS management functionality to UEM. The Google domain must include the Chrome Enterprise Upgrade. Note that the enrollment and some management of Chrome OS devices continues to be done through the Google managed domain console.

UEM synchronizes org units from the Google admin console into UEM org unit groups. After the initial synchronization, UEM registers with the Google domain to be notified of any changes to org units, users, or devices. When UEM is notified of a change, it synchronizes and updates the database accordingly.

Step	Action
1	Create a service account to authenticate with the Google domain.
2	Enable UEM to synchronize Chrome OS data.
3	Integrate UEM with the Google domain.

If you already configured UEM to support Android Enterprise devices, you can follow these steps to allow UEM to manage Chrome OS devices:

Step	Action
1	Verify that your organization's Google domain has Chrome OS enterprise enabled.
2	Verify that the Chrome Policy API is enabled in your organization's Google domain. For more information, see Create a service account to authenticate with the Google domain.
3	Verify that all scopes are added. For more information, see Enable UEM to synchronize Chrome OS data.
4	Enable Chrome OS management in the UEM console. For more information, see Integrate UEM with the Google domain.

Create a service account to authenticate with the Google domain

Perform these steps only if BlackBerry UEM is not already connected to an existing Google managed domain.

1. Log in to the Google Developers Console with the Google account that you want to use to manage your project.
2. Create a project.
3. Select the project and create a service account for it.

4. Give the service account the **Basic > Editor** role.
5. Select the service account and add a new P12 key.
6. Copy the private key password and save the certificate on your local machine.
7. Locate and copy the unique client ID and email address of the service account.
8. In the section for enabled APIs and services, search for and enable the following APIs:
   - **Admin SDK API**
   - **Google Play EMM API**
   - **Chrome Policy API**

After you finish: Enable UEM to synchronize Chrome OS data.

Enable UEM to synchronize Chrome OS data

You must use your organization's Google administration console to enable additional APIs that allow UEM to synchronize Chrome OS data.

Before you begin: Create a service account to authenticate with the Google domain.

1. Log in to the Google administration console using the administrator account for your Google domain.
2. Navigate to the section for third-party integrations for mobile devices.
3. Verify that third-party Android mobile management is enabled.
4. In the section for adding EMM providers, generate a token.
5. Copy the token.
6. In the section for security API controls, click the option to manage domain-wide delegation.
7. Add a new configuration.
8. For the client ID, paste the unique client ID for the Google service account.
9. For OAuth scopes, type or paste the following in a comma-delimited list:
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/admin.directory.customer
   - https://www.googleapis.com/auth/admin.directory.device.chromeos
   - https://www.googleapis.com/auth/admin.directory.device.mobile
   - https://www.googleapis.com/auth/admin.directory.orgunit
   - https://www.googleapis.com/auth/chrome.management.policy
   - https://www.googleapis.com/auth/admin.reports.audit.readonly
10. Authorize the connection.

After you finish: Integrate UEM with the Google domain.

Integrate UEM with the Google domain

Before you begin: Enable UEM to synchronize Chrome OS data.

1. Log in to the UEM management console using a Security Administrator account.
2. On the menu bar, click **Settings > External integration > Android and Chrome Management**.
3. Select **Connect BlackBerry UEM to your existing Google domain**.
4. Under **How app configurations are sent**, select **Send app configuration using Google Play**.
5. Click **Next**.

6. In the **Private key password** field, paste the private key password from the Google Developers Console.
7. Click **Browse**.
8. Navigate to and select the certificate file from the Google Developers Console.
9. In the **Service account email address** field, paste the Google service account email address from the Google Developers Console.
10. In the **Google administrator email address** field, type the email address of the administrator account that is used to manage the Google Cloud or Google Workspace by Google domain.
11. In the **Token** field, paste the token that you generated.
12. Under **Select the type of domain to manage the Android devices with a work profile** section, select the appropriate type of Google domain.
13. If you selected **Google Cloud domain**, choose one of the following options:
    - **Do not allow BlackBerry UEM to create users in the domain**: If you choose this option, you must create users in your Google Cloud domain and create local users with the same email addresses in UEM.
    - **Allow BlackBerry UEM to create users in the domain**: If you choose this option, select one of the following:
      - **Do not allow BlackBerry UEM to delete users in the Google domain**
      - **Allow BlackBerry UEM to delete users in the Google domain**
14. Click **Next** and choose which applications you want to add to UEM.
15. Click **Next**.
16. Click **Next** again.

After you finish: To synchronize UEM with the Google admin console, on the menu bar, click **Settings > External integration > Android and Chrome Management**. In the **Chrome OS Management** section, click **Enable**. UEM performs an initial synchronization of data within 10 minutes and schedules regular synchronizations. After the synchronization is complete, you can use options on this screen to initiate out-of-schedule synchronizations for org units, users, and devices.

Simplifying Windows 10 activations

When a user activates a Windows 10 device with BlackBerry UEM, the user needs to specify the UEM server address. You can simplify the activation process for users using the following methods:

Method	Description
Integrate UEM with Entra ID join.	If you configure Entra ID join, users can activate their devices using only their Entra ID username and password. An Entra ID premium license is required. See Integrate UEM with Entra ID join.
Configure Windows Autopilot.	If you configure Windows Autopilot, the enrollment is part of the out-of-box setup experience and the device is automatically activated when the user completes it using only their Entra ID username and password. Integration with Entra ID join and an Entra ID premium license are required. See Configure Windows Autopilot for device activation.

Integrate UEM with Entra ID join

You can integrate BlackBerry UEM with Entra ID join for a simplified enrollment process for Windows 10 devices. When it's configured, users can enroll their devices with UEM using their Entra ID username and password. Entra ID join is also required to support Windows Autopilot, which allows Windows 10 devices to be automatically activated with UEM during the Windows 10 out-of-the-box setup experience. A UEM certificate can be installed on the device manually or administrators can deploy the certificate using SCCM.

Before you begin: You will need the MDM terms of use URL and the MDM discovery URL to complete the steps below. To determine these URLs, in the UEM management console, create a test user account and send the user an activation email using the default activation email template. The default template contains the %ClientlessActivationURL% variable that resolves to the appropriate value in the received email. Use that value for the following URLs in the steps below:

- MDM terms of use URL: *%ClientlessActivationURL%*/azure/termsofuse
- MDM discovery URL: *%ClientlessActivationURL%*/azure/discovery

1. Log in to the Microsoft Azure portal.
2. In the Mobility (MDM and WIP) section, add an application and give it a friendly name (for example, BlackBerry UEM).
3. Specify the user scope. If applicable, select groups.
4. Specify the MDM terms of use URL and the MDM discovery URL.

After you finish: Optionally, Configure Windows Autopilot for device activation.

Configure Windows Autopilot for device activation

If you configure Windows Autopilot, the device is automatically activated when the user completes out-of-the-box setup using only their Entra ID username and password.

Before you begin: Integrate UEM with Entra ID join.

1. Log in to the Microsoft Entra ID management portal.

2. In the section for Windows device enrollment, create a Windows Autopilot deployment profile.
3. Enter a name and description for the profile.
4. Configure the out-of-box experience settings.
5. Assign the profile to the appropriate user groups.
6. Save the profile.
7. Complete the following steps on each Windows 10 device that you want to activate with Windows Autopilot:
   a) Turn on the device to load the out-of-the-box setup and connect to a Wi-Fi network.
   b) Press CTRL + SHIFT + F3 to restart and enter audit mode.
   c) Run Windows PowerShell as an administrator and run the following commands:

      ```
      Save-Script -Name Get-WindowsAutoPilotInfo -Path C:\Windows\Temp
      ```

      ```
      Install-Script -Name Get-WindowsAutoPilotInfo
      ```

      ```
      Get-WindowsAutoPilotInfo.ps1 -OutputFile C:\Windows\Temp\MyComputer.csv
      ```

   d) Collect the resulting .csv file from each device.
8. In the Microsoft Entra ID management portal, in the section for Windows device enrollment and Windows Autopilot devices, import the .csv file from each device.
9. In the system preparation tool dialog, do the following:
   a) For the system cleanup action, select the option to enter system out-of-box experience (OOBE) and deselect generalize.
   b) In the shutdown options, select the option to reboot.

Migrating users, devices, groups, and other data from a source server

You can use the BlackBerry UEM management console to migrate users, devices, groups, and other data from a source on-premises UEM server.

Step	Action
1	Review the migration prerequisites and best practices and considerations.
2	Connect to a source server.
3	Migrate IT policies, profiles, and groups from a source server.
4	Migrate users from a source server.
5	Migrate devices from a source server.

Prerequisites: Migrating users, devices, groups, and other data from a source BlackBerry server

Item	Prerequisites
Security Administrator permissions	Complete the instructions in this section as a Security Administrator.
Supported versions of the source server	You can migrate from a source UEM on-premises version 12.21 or later. For UEM Cloud, you can migrate data from UEM on-premises only. The source UEM on-premises instance must be one of the three most recent major version releases. Older versions are not supported for migration.
BlackBerry Connectivity Node (UEM Cloud only)	To support all migration features, you must activate at least one BlackBerry Connectivity Node version 2.13 or later.
UEM company directory connection	Configure the destination UEM company directory connection in the same way that it is configured in the source server. Migration does not work if the company directory connection does not match.

Item	Prerequisites
Defragment the databases (UEM on-premises only)	Defragment the source and destination UEM databases before you begin migration. If you are migrating a large number of users or devices, you should defragment the destination UEM database after you migrate each set of users or devices.
BlackBerry UEM Client	• UEM on-premises: If you plan to migrate the BlackBerry Dynamics-enrolled UEM Client and BlackBerry Dynamics apps, the latest UEM Client must be installed on devices. • UEM Cloud: The UEM Client must be version 12.x or later.
BlackBerry Dynamics apps	• UEM on-premises: All BlackBerry Dynamics apps that you plan to migrate must use BlackBerry Dynamics SDK version 7.1 or later. • UEM Cloud: All BlackBerry Dynamics apps that you plan to migrate must use BlackBerry Dynamics SDK version 8.0 or later. • BlackBerry Dynamics apps that are not supported for migration are removed from the device during the migration process.
BlackBerry Dynamics app entitlements	• The destination UEM server must have the same list of BlackBerry Dynamics app entitlements as the source server. • Migrated user accounts must be assigned the same list of BlackBerry Dynamics app entitlements on the destination UEM as they have on the source server. • The authentication delegate must be the same on the source server and the destination server. You can change the authentication delegate after migration. • If the BlackBerry Dynamics profile on the source server allows the UEM Client to be activated by BlackBerry Dynamics, configure the same on the destination server. • The authentication delegate must be the same on the source server and the destination UEM server. You can change the authentication delegate after migration. If entitlements do not match between the source and destination server, BlackBerry Dynamics apps are disabled after migration.
Custom BlackBerry Dynamics apps	Custom apps migrate only if the source and destination servers have the same organization ID. For more information about merging organizations, see KB 47626.
Ports	• UEM on-premises: Verify that Port 1433 (TCP) and port 1434 (UDP) are unblocked on the Microsoft SQL Server. • UEM Cloud: Port 8887 (TCP) must be open between the on-premises UEM server and the BlackBerry Connectivity Node. Verify that the port used by the Microsoft SQL Server that hosts the on-premises UEM database is open and can be accessed by the BlackBerry Connectivity Node (for example, port 1433).

UEM migration best practices and considerations

Migrating IT policies, profiles, and groups

Item	Considerations and best practices
Items copied from a source UEM server	• Selected IT policies • Email profiles • Wi-Fi profiles • VPN profiles • Proxy profiles • BlackBerry Dynamics connectivity profiles • BlackBerry Dynamics profiles • App configuration settings • CA certificate profiles • Shared certificate profiles • Certificate retrieval • User credential profiles • SCEP profiles • CRL profiles • OSCP profiles • Certification authority settings (Entrust and PKI connector only) • Client certificates (app usage) • Any policies and profiles that are associated with the policies and profiles you select
Group migration	User, role, and software configuration assignments are not migrated. You must manually recreate these assignments on the destination UEM server.
IT policy passwords	If any of the source IT policies you selected for Android devices has a minimum password length of less than 4 or more than 16, no UEM IT policies or profiles can be migrated. Change the source IT policy accordingly.
Profile names	After migration, you must make sure that all SCEP, user credential, shared certificate, and CA certificate profiles have unique names. If two profiles of the same type have the same name, you must edit one of the profile names.
BlackBerry Dynamics connectivity profiles	The values from the App servers tab are not migrated. The values are populated using the default values from the destination UEM server. Some of the values from the Infrastructure tab are not migrated. The administrator must manually edit each migrated profile and set the values for the Primary BlackBerry Proxy cluster and the Secondary BlackBerry Proxy cluster.

Item	Considerations and best practices
Certificate usage (UEM)	Certificate usage is migrated, except for: • Certificate usages that already exist on the destination server • Non-BlackBerry Dynamics apps • Custom apps from another Good Control organization
Post-migration tasks for BlackBerry Dynamics users	After you migrate users, devices, groups, and other data from a source UEM on-premises server to UEM Cloud, complete the following tasks: • Assign app configurations to BlackBerry Dynamics apps in groups. • Assign connectivity profiles to groups. • Set override profiles (BlackBerry Dynamics profiles and compliance profiles). • In migrated connectivity profiles, specify the information for app servers and BlackBerry Proxy clusters The migration status of the listed container might display as in progress for Android devices. The UEM Client will resolve 24 hours after migration or when the users restart the device or perform a force restart of app. BlackBerry Work might require users to force quit the app and launch it again to pick up the updated BlackBerry Dynamics connectivity profiles. Alternatively, users can restart the device.

Migrating users

Item	
Maximum number of users	You can migrate a maximum of 500 users at a time from a source server. If you select more than the maximum number of users, only the maximum number are migrated and the rest are skipped. You can repeat the migration process as needed to migrate all the users from the source server.
Email address	• Only users with an associated email address can be migrated. • You can't migrate a user who already uses the same email address in the destination UEM server. • If two users in the source database have the same email address, only one user is displayed on the Migrate users screen.
Groups	• You can filter users with no group assignment to include this set of users for a migration. • You can't migrate a user who is an owner of a shared device group. The user does not appear in the list of users to migrate.

Item	
BlackBerry UEM Self-Service	• After migration, the user must use the same login information for BlackBerry UEM Self-Service that they used before migration. • After migration, local users must change their password after they log in to BlackBerry UEM Self-Service for the first time. • Users who did not have permission to access BlackBerry UEM Self-Service before migration are not automatically granted permission after migration.

Migrating devices from a source server

Item	Considerations and best practices
Validate configuration	It is a best practice to migrate one device for each unique configuration (for example, different groups, policies, app configurations, and so on) to make sure the destination server is configured correctly before migrating the rest of your devices.
Maximum number of devices	You can migrate a maximum of 2000 devices at a time from a source server.
Users	• The device users must exist in the destination UEM domain. • You must migrate all of a user's devices at the same time.
Managed iOS devices from a UEM source	• Devices must have the latest version of the UEM Client. • Devices that are assigned an App lock profile can't be migrated because the UEM Client can't be opened for the migration. • Migration of Apple DEP devices is not supported. DEP devices must be factory reset and reactivated on the new UEM instance. For more information, see KB 100525. • User enrollment devices cannot be migrated. • In the app settings for all applicable apps, clear the **Remove the app from the device when the device is removed from BlackBerry UEM** check box. If you attempt to migrate without performing this step, the app is removed and the device may be unenrolled from UEM.
Managed Android devices from a UEM source	• Android Enterprise devices must have the latest version of the UEM Client installed. • You can't migrate Android devices that have a work profile using a Google account or Google domain.
Chrome OS devices	You can migrate Chrome OS devices from a UEM source server.
Devices that are not supported for migration	• Windows • macOS
Shared device group	You can't migrate a device that belongs to a shared device group. These devices do not appear in the migration list.

Item	Considerations and best practices
BlackBerry Dynamics-enabled devices	• In the Migrate devices screen, the Incompatible containers column displays the number of BlackBerry Dynamics apps for each device that can't be migrated and the total number of BlackBerry Dynamics apps for each device. Click on the number to see the BlackBerry Dynamics apps that are incompatible with migration. • BlackBerry Access for Windows, BlackBerry Access for macOS, and BlackBerry BRIDGE are not supported for migration. After the migration is complete, users must re-enroll these apps. • The migration process does not track or guarantee migration of the UEM Client and apps activated on a device after that device's data is cached. It is a best practice to refresh the user cache before each migration. • BlackBerry Dynamics-enabled devices are always enrolled for BlackBerry Dynamics on the destination server. • If a user has more than one device with BlackBerry Dynamics apps, all the devices are automatically selected for migration. • If a user forgets the password for a BlackBerry Dynamics app after migration has been initiated, but before the container has completed migration, the unlock access key must be obtained from the UEM source server. After the migration is complete, the key must be obtained from the destination UEM server. • To trigger the migration on the device, it is a best practice to first open the app that is configured as the authentication delegate on the device.

Connect to a source server

To migrate data you must connect BlackBerry UEM to the source server. You can only have one active source server at a time.

Before you begin:

- Review the migration prerequisites and best practices and considerations.
- In UEM on-premises environments, verify that the database account associated with your login credentials has write permissions.
- In UEM Cloud environments, if more than one BlackBerry Connectivity Node is activated, configure all BlackBerry Connectivity Node instances to connect to the same source database.

Follow the steps for your type of UEM environment:

Environment	Steps
UEM on-premises	**a.** In the management console, on the menu bar, click **Settings > Migration > Configuration**. **b.** Click +. **c.** In the **Source type** drop-down list, click the appropriate type of source server. **d.** Specify the information for the source server. **e.** Click **Test connection**. **f.** Click **Save**.
UEM Cloud	**a.** In the BlackBerry Connectivity Node management console, on the menu bar, click **General settings > Migration**. **b.** Click +. **c.** Specify the information for the source server. • For the **Database server** field, use the format <*host*>\<*instance*> for a dynamic port and <*host*>:<*port*> for a static port. • If you select Windows NT authentication, change the Log On properties of the BlackBerry UEM - BlackBerry Cloud Connector service to the same account you used to install the source server. After the migration is complete, change the Log On properties back to using the Local System account. **d.** Click **Save**. **e.** In the UEM management console, click **Settings > Migration > Configuration**. **f.** Click +. **g.** Type a name for the source database. **h.** Click **Test connection**. **i.** Click **Save**.

After you finish: Do any of the following:

- Migrate IT policies, profiles, and groups from a source server.
- Migrate users from a source server.
- Migrate devices from a source server.

Migrate IT policies, profiles, and groups from a source server

Before you begin: Connect to a source server.

1. In the management console, on the menu bar, click **Settings > Migration**.

   If you configured more than one source server in a UEM on-premises environment, select the source server that you want to migrate data from.
2. Click **IT policies, profiles, groups**.
3. Click **Next**.
4. Select the items that you want to migrate.

   The name of the source server is appended to the name of each policy and profile when it is migrated to the destination server.
5. Click **Preview**.

6. Click **Migrate**.

After you finish:

- To configure the IT policies, profiles, and groups, click **Configure IT policies and profiles** to go to the **Policies and Profiles** screen.
- On the destination server, create the policies and profiles that could not be migrated and assign them to users before you migrate devices.
- Migrate users from a source server.

Migrate users from a source server

Before you begin:

- Connect to a source server.
- Migrate IT policies, profiles, and groups from a source server.

1. In the management console, on the menu bar, click **Settings > Migration > Users**.
2. Click **Refresh cache**.

   The refresh requires approximately 10 minutes for every 1000 users. Refreshing the cache is mandatory only for the first set of users that you want to migrate. If you make changes to the source server during migration, it is a best practice to refresh the cache again.
3. Click **Next**.
4. Select the users that you want to migrate.

   By default, only the first 20,000 users are displayed. You can search for specific users as needed. Note that selecting all users selects only those displayed on the first page.
5. Click **Next**.
6. Assign an IT policy, groups, and profiles to the selected users.
7. Click **Preview**.
8. Click **Migrate**.

Note that migrated user accounts are not removed from the source server.

After you finish: Migrate devices from a source server.

Migrate devices from a source server

After you migrate users from the source server to the destination BlackBerry UEM, you can migrate their devices. The devices move from the source server to the destination BlackBerry UEM and are no longer in the source after the migration.

Before you begin:

- Connect to a source server.
- Migrate IT policies, profiles, and groups from a source server.
- Migrate users from a source server.
- Notify iOS device users that they must open the BlackBerry UEM Client and that they must keep it open until the migration is complete.

1. In the management console, on the menu bar, click **Settings > Migration > Devices**.
2. Click **Refresh cache**.

The refresh requires approximately 10 minutes for every 1000 devices. Refreshing the cache is mandatory only for the first set of devices that you want to migrate. If you make changes to the source server during migration, it is a best practice to refresh the cache again.

3. Click **Next**.
4. Select the devices that you want to migrate.

   By default, only the first 20,000 devices are displayed. You can search for specific devices as needed. Note that selecting all devices selects only those displayed on the first page.
5. Click **Preview**.
6. Click **Migrate**.
7. click **Migration** > **Status**.

After you finish: To view the status of the devices that are being migrated, click **Migration > Status**.

Configuring network communication and properties for BlackBerry Dynamics apps

Follow the instructions in this section to configure network communication and other properties for BlackBerry Dynamics apps.

Task	Description
Manage BlackBerry Proxy clusters.	Create and manage BlackBerry Proxy clusters that route data for BlackBerry Dynamics apps.
Configure Direct Connect using port forwarding.	Configure Direct Connect for BlackBerry Proxy instances.
Configure BlackBerry Dynamics properties (on-premises only).	Configure properties for the BlackBerry Dynamics apps that you plan to deploy in your organization's environment.
Configure communication settings for BlackBerry Dynamics apps (on-premises only).	Configure communication settings for the BlackBerry Dynamics apps that you plan to deploy in your organization's environment, including the communication protocol the apps will use.
Sending BlackBerry Dynamics app data through an HTTP proxy.	Configure UEM to send BlackBerry Dynamics app data though an HTTP proxy between BlackBerry Proxy and an application server.
Methods for routing traffic for BlackBerry Dynamics apps.	Details of the different methods you can use to route traffic for BlackBerry Dynamics apps.
Configuring Kerberos authentication for BlackBerry Dynamics apps (on-premises only).	Configure Kerberos Constrained Delegation or Kerberos PKINIT to simplify authentication for users.

For more information about deploying and managing BlackBerry Dynamics apps, see Managing BlackBerry Dynamics apps in the Administration content.

Manage BlackBerry Proxy clusters

When you install the first instance of the BlackBerry Proxy, BlackBerry UEM creates a BlackBerry Proxy cluster named “First”. If only one cluster exists, additional instances of BlackBerry Proxy are added to the cluster by default. You can create additional clusters and move BlackBerry Proxy instances between any of the available clusters. When more than one BlackBerry Proxy cluster is available, new instances are not added to a cluster by defaulty, they are considered unassigned and must be added to one of the available clusters manually.

1. In the management console, on the menu bar, click **Settings > BlackBerry Dynamics > Clusters**.
2. Perform any of the following tasks:

Task	Steps
Create a new BlackBerry Proxy cluster.	**a.** Click +. **b.** Type a name for the cluster. **c.** Click **Save**.
Rename a BlackBerry Proxy cluster.	**a.** Click a cluster name. **b.** Change the cluster name. Each cluster must have a unique name. **c.** Click **OK**.
Move a BlackBerry Proxy instance to a different BlackBerry Proxy cluster.	**a.** In the **Servers** column, click the name of a BlackBerry Proxy instance. **b.** In the **BlackBerry Proxy cluster** drop-down list, select the cluster that you want to add the instance to. **c.** Click **Save**.
Delete an empty BlackBerry Proxy cluster.	**a.** Click × for that cluster. **b.** Click **Remove**.
Set app proxy settings for a cluster.	**a.** Click the cluster name. **b.** Click **Override global settings** **c.** See Configure BlackBerry Dynamics app proxy settings.
Download PAC file updates for all clusters.	Click **Refresh PAC cache**.
Specify a trusted root certificate to download PAC files from the server.	**a.** Verify that you have the certificate in X.509 format (*.cer, *.der) stored in a network location that you can access from the management console. **b.** On the menu bar, click **Settings > External Integration > Trusted certificates**. **c.** Click + beside **PAC server trusts**. **d.** Click **Browse**. **e.** Navigate to and select the certificate file that you want to use. **f.** Click **Open**. **g.** Type a description for the certificate. **h.** Click **Add**.
Enable a BlackBerry Proxy to be used for activation (UEM on-premises only).	Select the **Enabled for activation** option for the BlackBerry Proxy instance that you want to use for activation purposes. At least one instance must be selected.

Configure Direct Connect using port forwarding

Before you begin:

- Configure a public DNS entry for each BlackBerry Connectivity Node server (for example, bp01.example.com, bp02.example.com, and so on).

- Configure the external firewall to allow inbound connections on port 17533 and to forward that port to each BlackBerry Connectivity Node server.
- If the BlackBerry Connectivity Node instances are installed in a DMZ, ensure that the appropriate ports are open between each BlackBerry Connectivity Node and any application servers that the BlackBerry Dynamics apps need to access (for example, Microsoft Exchange, internal web servers, and the BlackBerry UEM Core).

1. In the management console, on the menu bar, click **Settings > BlackBerry Dynamics > Direct Connect**.
2. Click a BlackBerry Proxy instance.
3. To turn on Direct Connect, select the **Turn on Direct Connect** check box. In the **BlackBerry Proxy host name** field, verify that the host name is correct. If the public DNS entry you created is different from the FQDN of the server, specify the external FQDN instead.
4. Repeat for all BlackBerry Proxy instances in the cluster.

   To enable only some BlackBerry Proxy instances for Direct Connect, create a new BlackBerry Proxy cluster. All servers in a cluster must have the same configuration. For more information, see Manage BlackBerry Proxy clusters in the Configuration content.
5. Click **Save**.

Configure BlackBerry Dynamics properties

In a UEM on-premises environment, you can configure various properties related to the security, behavior, and communications of BlackBerry Dynamics apps.

1. In the management console, on the menu bar, click **Settings > BlackBerry Dynamics**.
2. Do any of the following:

Task	Steps
Change global properties for BlackBerry Dynamics apps.	• Click **Global properties**. • Configure the properties as necessary. See BlackBerry Dynamics global properties. • Click **Save**.
Change BlackBerry Dynamics properties for a specific UEM server.	• Click **Properties**. • In the **Server type** drop-down list, click **BlackBerry Control servers** and select the UEM server that you want to configure. • Configure the properties as necessary. See BlackBerry Dynamics properties. • Click **Save**.
Change the properties for a BlackBerry Proxy instance.	• Click **Properties**. • In the **Server type** drop-down list, click **BlackBerry Proxy servers** and select the BlackBerry Proxy server that you want to configure. • Configure the properties as necessary. See BlackBerry Proxy properties. • Click **Save**.

BlackBerry Dynamics global properties

The following tables describe the BlackBerry Dynamics global properties that you can configure. The Restart column indicates whether changing the property requires a restart of BlackBerry UEM.

If a property is displayed in the management console but is not documented here, it is a deprecated property that is no longer in use.

Certificate Management

Property	Description	Default	Restart
Time-to-live in seconds for the keystore for individual end-users' PKCS 12 certificates	The lifespan, in seconds, of the keystore for the PKCS 12 certificates that device users can upload to sign email messages and for client authentication. This property is read-only and cannot be changed.	86400	—

Communication

Property	Description	Default	Restart
cntmgmt.internal.port	The internal port for the container management service.	17317	Yes
cntmgmt.max.conns.above.limit	The maximum number of connections that are allowed in excess of the limit set by the cntmgmt.max.conns.persec property. **Note:** Do not change this setting without consulting BlackBerry Technical Support.	3	Yes
cntmgmt.max.conns.persec	The maximum number of connections per second for container management. **Note:** Do not change this setting without consulting BlackBerry Technical Support.	30	Yes
cntmgmt.max.active.sessions	The maximum number of active sessions for container management.	10000	Yes
cntmgmt.max.idle.count	The maximum number of idle connections that are permitted for container management. **Note:** Do not change this setting without consulting BlackBerry Technical Support.	0	Yes
cntmgmt.max.read.throughput	The maximum number of concurrent read operations for container management. **Note:** Do not change this setting without consulting BlackBerry Technical Support.	500	Yes

Property	Description	Default	Restart
cntmgmt.max.write.throughput	The maximum number of concurrent write operations for container management. **Note:** Do not change this setting without consulting BlackBerry Technical Support.	500	Yes
cntmgmt.ssl.external.enable	Controls whether SSL is enabled for external container management. This property is read-only and cannot be changed.	On	—
cntmgmt.ssl.internal.enable	Controls whether SSL is enabled for internal container management. This property is read-only and cannot be changed.	On	—

Duplicate Containers

If UEM identifies duplicate containers on devices, it schedules batch jobs to remove them. A duplicate container has the same user ID and entitlement ID (also known as the BlackBerry Dynamics App ID) as another container on the same device. When a duplicate container is removed, it is recorded in the UEM log file.

Property	Description	Default	Restart
Automatically remove older duplicate containers on same device for the user after provisioning	Specify whether UEM automatically removes duplicate containers when a new version of an app is provisioned. If this setting is selected, it takes precedence over the other Duplicate Container properties.	On	No
Enable job to automatically remove duplicate containers (on/off)	Specify whether UEM automatically schedules jobs to identify and remove duplicate containers from devices.	On	No
Inactivity timeout in seconds before duplicate container is deleted	The amount of time, in seconds, that a duplicate container must be inactive before UEM schedules a job to remove it.	259200	No
Frequency in seconds that job to remove duplicate containers will run	How often, in seconds, UEM runs a job to identify and remove duplicate containers.	86400	No
Maximum number of containers to remove in a single job	The maximum number of inactive containers that a single job can remove from devices.	100	No

Kerberos Constrained Delegation

Property	Description	Default	Restart
Use explicit UPN	Specify whether BlackBerry Dynamics apps use an explicit UPN or implicit UPN while authenticating to services integrated with Microsoft Active Directory or Exchange ActiveSync in Office 365. Your organization's Active Directory may support both options or only one of the options, depending on your environment.	Off	No
Enable KCD (gc.krb5.enabled)	Specify whether UEM supports Kerberos Constrained Delegation for BlackBerry Dynamics apps.	Off	Yes

Miscellaneous

Property	Description	Default	Restart
config.command.expiry	How long UEM waits, in seconds, before resending an unacknowledged message.	60	Yes
config.command.retry	How often, in seconds, UEM runs the task to identify and resend unacknowledged messages. If set to 0, UEM does not run the task.	900	Yes
gc.entgw.report.userinfo	Specify whether user display names are reported to the BlackBerry Dynamics NOC.	Off	No
policy.compliance.interval	How often, in minutes, UEM retrieves compliance policies for all policy sets.	1440	Yes

Purge Inactive Containers

If UEM identifies inactive containers on devices, it schedules batch jobs to remove them. UEM considers a container to be inactive if it has not connected to UEM for a default period of 90 days. When an inactive container is removed, it is recorded in the UEM log file.

Containers that have an authentication delegate configured are not purged by this process.

Property	Description	Default	Restart
Enable job to automatically remove inactive containers (on/off)	Specify whether UEM automatically schedules jobs to identify and remove inactive containers from devices.	Off	No
Container inactivity interval in seconds	The amount of time, in seconds, before UEM considers a container to be inactive.	7776000	No

Property	Description	Default	Restart
Frequency in seconds that job to remove inactive containers will run	How often, in seconds, UEM runs a job to identify and remove inactive containers.	86400	No
Maximum number of containers to remove in a single job	The maximum number of inactive containers that a single job can remove from devices.	100	No

Reporting

Property	Description	Default	Restart
Set limit for records returned in exportable reports to prevent out of memory condition	The maximum number of lines that can be included in a report. The maximum value that can be entered is 1000000.	5000	No

Retention Data Policy

Property	Description	Default	Restart
gc.purge.dbJobs Purge server jobs	Specify whether UEM automatically purges server jobs at a regular interval.	On	Yes
gc.purge.dbJobs.interval Purge server jobs interval	If “Purge server jobs” is on, how often, in days, UEM purges server jobs.	30	Yes

BlackBerry Dynamics properties

Kerberos Constrained Delegation

Property	Description	Default	Restart
Location of krb5.conf file on GC server (gc.krb5.config.file)	The location of the krb5.conf file that is required to configure KCD and to enable cross-realm authentication when there is a CAPATH trust relationship with multiple Kerberos domains.	Not set	Yes
Enable KCD debugging mode (gc.krb5.debug)	Whether UEM logs debug level data.	Off	Yes
Fully qualified name for the KDC (gc.krb5.kdc)	The FQDN of the server that hosts the Kerberos Key Distribution Center (KDC) service.	Not set	Yes

Property	Description	Default	Restart
Location of keytab file (gc.krb5.keytab.file)	The location of the Kerberos keytab file on the computer that hosts BlackBerry UEM.	Not set	Yes
Service account name under which KCD service is running (gc.krb5.principal.name)	The username of the Kerberos account. Do not include the domain or realm.	Not set	Yes
Realm - Active Directory (gc.krb5.realm)	The realm of the Kerberos account.	Not set	Yes

BlackBerry Proxy properties

The following table describe the properties that you can configure for each of your organization's BlackBerry Proxy instances.

Property	Description	Default	Restart
gp.gps.max.sessions	Maximum number of active sessions.	15000	—
gp.gps.dns.server.ttl.ms	Time to wait, in milliseconds, for the DNS server response.	1800000	—
gp.gps.server.flowcontrol	Specify whether flow control is enabled for the server.	Off	—
gp.gps.tcp.keepalive	Specify whether TCP keepalive is enabled for the server.	Off	—
gp.gps.unalias.hostname	If you select this option, BlackBerry Proxy uses reverse DNS lookup with the IP address of the app server. If you don't select this option, BlackBerry Proxy uses the app server hostname for DNS lookups.	Off	Yes
gps.directconnect.supported.ciphers	Add or change cipher suites that encrypt bridging and communications made through BlackBerry Direct Connect. You may choose to have your own proxy server configured for Direct Connect and placed between your client devices and the BlackBerry Proxy server. If you have added your own proxy server, make sure that the BlackBerry Proxy server ciphers correspond to those required by your own proxy server. All ciphers must be supported by Java.	Listed in the UI	Yes

Property	Description	Default	Restart
gp.directconnect. supported.protocols	Add or change the cryptographic protocols that you want your system's direct connect bridge to support.	TLSv1, TLSv1.1, TLSv1.2	Yes
gp.eacp.command.service.nslookup. srv.ldap	Enables LDAP over TCP for Active Directory servers. Active Directory servers offer the LDAP service over the TCP protocol. Clients find an LDAP server by querying DNS for a record of the form: _ldap._tcp.DnsDomainName. If you select this option, BlackBerry Proxy uses LDAP for nslookup of a given service hostname. If you don't select this option, BlackBerry Proxy uses reverse DNS lookup directly, using the service hostname that you provide.	Off	Yes
gc.mdc.hb.timeout	Specify the heartbeat timeout.	0	—
gp.server.secure.ciphers	Add or change cipher suites that encrypt communications made through a BlackBerry Proxy server. All ciphers must be supported by Java.	Listed in the UI	—
gp.server.secure.protocols	Add or change the cryptographic protocols that you want your BlackBerry Proxy server to support.	TLSv1.2	—

Configure communication settings for BlackBerry Dynamics apps

In UEM on-premises environments, you can configure the communication settings for BlackBerry Dynamics apps in your organization's domain. The communication settings allow you to provide secure communication in your network using the protocol of your choice. By default, only TLS v1.3 is allowed. You can also allow TLSv1, v1.1, and v1.2. You must select at least one protocol.

1. In the management console, on the menu bar, click **Settings > BlackBerry Dynamics > Communication settings**.
2. Configure the settings as necessary.
3. Click **Save**.

Sending BlackBerry Dynamics app data through an HTTP proxy

You can configure BlackBerry UEM to send BlackBerry Dynamics app data though an HTTP proxy between BlackBerry Proxy and an application server. BlackBerry Dynamics apps support both manual proxy settings and PAC files for connections to application servers. To use a PAC file, apps must be developed with BlackBerry Dynamics SDK 7.0 or later. If you configure both manual and PAC file settings, the PAC file takes precedence

for apps that support it. Apps developed using an older version of the BlackBerry Dynamics SDK use the manual settings.

BlackBerry Access also supports manual proxy and PAC file app configuration settings that apply only to browsing with BlackBerry Access. Proxy configuration settings for BlackBerry Access, or other apps that have separate proxy settings, override the UEM proxy settings. For more information, see the BlackBerry Access Administration Guide.

Considerations for using a PAC file with BlackBerry Proxy

Considerations	Details
Supported PAC file directives	• DIRECT • PROXY (treated as HTTPS proxy; connection established using HTTP CONNECT) • HTTPS (connection established using HTTP CONNECT)
Unsupported PAC file directives	A connection error will occur for the following: • SOCKS • SOCKS4 • SOCKS5 • HTTP • Custom "NATIVE" directive defined by BlackBerry Access BLOCK file directives are treated as DIRECT.
Limitations	• The dnsDomainIs function can't include the "_" and "*" characters. • The shExpMatch function can't include the expressions "[0-9]", "?", "/^d", or "d+" • The option to strip the path and query from the URI is not supported.
PAC cache	BlackBerry Proxy downloads and caches the PAC file to improve performance. The PAC cache is updated every 24 hours. If you want to update the cache manually, in the management console, go to Settings > Infrastructure > BlackBerry Router and Proxy > Global settings and click Update PAC cache.

Configure BlackBerry Dynamics app proxy settings

1. Follow the appropriate step for your UEM environment:

Environment	Task
UEM on-premises	Do one of the following in the UEM management console: • If you want to set global app proxy settings, click **Settings > Infrastructure > BlackBerry Router and proxy** and expand **Global settings**. • If you want to set app proxy settings for a cluster, click **Settings > BlackBerry Dynamics > Clusters**. Click the name of a cluster and select the **Override global settings** check box. • If you want to set manual app proxy settings for a server, click **Settings > Infrastructure > BlackBerry Router and proxy**. Expand a server and select the **Override global settings** check box. Note that PAC files are not supported when overriding global proxy settings for a server.
UEM Cloud	In the BlackBerry Connectivity Node management console, click **General settings > BlackBerry Router and proxy > Global settings**.

2. Select the appropriate option and complete the required steps:

Option	Steps
Enable manual HTTP proxy	a. Select the appropriate proxy configuration. If you want to use a proxy to connect to specified servers, click + to add servers. b. Specify the address of the proxy server and the port number that it listens on. c. If the proxy server requires authentication, select the **Use authentication** check box and specify the authentication credentials.
Enable PAC	In the **PAC URL** field, type the URL for the PAC file. If the proxies specified in the PAC file require authentication, select the **Support proxy authentication** check box and specify the authentication credentials. End-user authentication credentials aren't supported for proxy authentication.

3. Click **Save**.

Methods for routing traffic for BlackBerry Dynamics apps

BlackBerry UEM provides several options that allow you to control how BlackBerry Dynamics traffic is routed. By default, all BlackBerry Dynamics app traffic routes directly to the Internet with no web proxy server configurations. This section discusses only configurations that affect overall routing.

Routing for BlackBerry Dynamics apps can be changed by the following configurations:

Configuration	Details
Assigned BlackBerry Dynamics connectivity profile	• The only item configured in the default BlackBerry Dynamics connectivity profile is the Default allowed domain route type, which is set to Direct. • Using the default BlackBerry Dynamics connectivity profile, no internal servers or domains are accessible to BlackBerry Dynamics apps. You can change the default connectivity profile or create a new profile to allow connectivity to internal servers. • For more information, see Create a BlackBerry Dynamics connectivity profile in the Administration content.

BlackBerry Proxy web proxy server configuration	• By default, BlackBerry Proxy is not configured to use a web proxy server. Each BlackBerry Proxy server attempts to connect directly to the Internet to make connections. This applies to both app server traffic and to BlackBerry Dynamics NOC connections.
	• For information about configuring BlackBerry Proxy, see Sending BlackBerry Dynamics app data through an HTTP proxy.
	• In the BlackBerry Dynamics connectivity profile, you can specify the servers that BlackBerry Dynamics apps are allowed to access through the firewall using BlackBerry Proxy. For more information, see Create a BlackBerry Dynamics connectivity profile in the Administration content.
	• Routing traffic through BlackBerry Proxy allows web browsers and BlackBerry Dynamics apps on devices to connect to any server behind the firewall that is reachable by BlackBerry Proxy, and allows you to easily monitor data traffic between BlackBerry Dynamics apps and your organization's resources.
	• Consider the following when choosing to route data through a BlackBerry Proxy server:
	  • Establishing connections to servers on the Internet can take longer.
	  • If you are using a web proxy to allow access to external sites and have settings configured in your proxy to restrict certain sites, when you select the Route all traffic option, you also need to set the proxy properties in BlackBerry Proxy. Otherwise, apps will not be able to access external sites.
	  • BlackBerry Access can be configured with a PAC file that determines allowable sites. In this case, the PAC file determines the proxy settings. For more information, see the BlackBerry Access Administration Guide.

App-specific settings	• App-specific configuration may be required for apps to connect to specific servers (for example, for BlackBerry Work configured with the URL of the Microsoft Exchange Server). Review the documentation for the BlackBerry Dynamics apps to understand which app configurations to apply. • BlackBerry Access and some third-party apps allow app-level web proxy server configurations. The default configuration for BlackBerry Access has no web proxy server configuration applied. • An app server is a server that a BlackBerry Dynamics app connects to, such as the URL of a Microsoft Exchange Server, the URL for BEMS, the URL for Skype for Business, or any URL that BlackBerry Access browses to. The BlackBerry Dynamics NOC and the BlackBerry UEM Core server are not app servers.

If you configure and assign a BlackBerry Dynamics connectivity profile and a web proxy configuration for BlackBerry Proxy servers, the BlackBerry Dynamics connectivity profile is always checked first. When traffic arrives at the BlackBerry Proxy server, the PAC or web proxy configuration set on the BlackBerry Proxy server is evaluated for connectivity. Configuring a web proxy on the BlackBerry Proxy server controls how that BlackBerry Proxy handles sending traffic out to the Internet, it does not affect how the BlackBerry Dynamics app on the device evaluates connections.

Example routing scenarios for BlackBerry Dynamics traffic

The following scenarios are examples of common configurations:

Scenario	BlackBerry Dynamics connectivity profile	Web proxy configuration for BlackBerry Proxy	App-specific settings
Route traffic to specific servers or domains through BlackBerry Proxy. Appropriate for scenarios where some internal app servers must be accessible to BlackBerry Dynamics apps, but general traffic to public servers can remain direct.	• Default allowed domain route type: Direct • Allowed domains: Add the internal domains to route through the BlackBerry Proxy and select a cluster. • Additional servers: If needed, add specific server names and select a cluster.	No configuration necessary.	No configuration necessary.
Route all traffic through the BlackBerry Proxy and then through a web proxy server. Appropriate for organizations that require all traffic from work apps to be routed internally.	Default allowed domain route type: BlackBerry Proxy cluster	Use a manual web proxy server configuration or a PAC file.	No configuration necessary.

Scenario	BlackBerry Dynamics connectivity profile	Web proxy configuration for BlackBerry Proxy	App-specific settings
Route some traffic internally for most apps but configure a proxy server specifically for web browsing using BlackBerry Access. Appropriate for organizations that require traffic for apps to be routed internally, but require browser traffic to be routed through a web proxy server.	• Default allowed domain route type: Direct • Allowed domains: Add the internal domains to route through the BlackBerry Proxy and select a cluster. • Additional servers: If needed, add specific server names and select a cluster.	If BlackBerry Proxy servers don't have direct access to the Internet, or if a proxy is required for BlackBerry Dynamics NOC connections, configure a web proxy server as needed.	In the app configuration for BlackBerry Access, select Enable Web Proxy and Use Proxy Auto Configuration.

Configuring Kerberos authentication for BlackBerry Dynamics apps

In a BlackBerry UEM on-premises environment, BlackBerry Dynamics apps support Kerberos Constrained Delegation (KCD) and Kerberos PKINIT. You can support KCD or Kerberos PKINIT for BlackBerry Dynamics apps, but not both.

Kerberos authentication	Description
KCD	KCD allows users to access enterprise resources without having to enter their network credentials. KCD uses service tickets that are encrypted and decrypted by keys that do not contain the user's credentials. When you configure KCD, the BlackBerry Dynamics app delegates authentication to UEM to act on its behalf to request access to a work resource. You can limit the network resources that are accessible to users by configuring the account that UEM uses to be trusted only for specific services. For example, if KCD is not configured and an app requests a resource like mypage.example.com, the app prompts the user for credentials. When KCD is configured, the BlackBerry Dynamics infrastructure handles authentication and the user is not prompted for credentials. See Prerequisites for configuring KCD for BlackBerry Dynamics apps and Configure KCD for BlackBerry Dynamics apps.
KerberosPKINIT	Kerberos PKINIT authentication establishes trust directly between the BlackBerry Dynamics app and the Windows KDC. User authentication is based on certificates issued by Microsoft Active Directory Certificate Services. See Requirements to support Kerberos PKINIT for BlackBerry Dynamics apps.

Prerequisites for configuring KCD for BlackBerry Dynamics apps

Item	Description
Active Directory port	Port 88 on the Active Directory service must be accessible by all UEM servers.
Kerberos environment	The Kerberos environment must include the following components: • Microsoft Active Directory server: The directory service that authenticates and authorizes all users and computers associated with your Windows network. • Kerberos Key Distribution Center (KDC): The authentication service on the Active Directory server that supplies session tickets and keys to users and computers in the Active Directory domain. • To use KCD with Microsoft 365 resources, the on-premises Active Directory domain must be integrated with Entra. For more information, see the Microsoft article "Integrate on-premises AD with Entra".

krb5.conf file	Your UEM environment requires a krb5.conf file with values specific to your KDC. It must include the following minimum settings:
	RC4 encryption:
	`[libdefaults]`
	`allow_weak_crypto = true`
	`forwardable = true`
	AES Keytab file:
	`[libdefaults]`
	`forwardable = true`
	If you use an AES Keytab file, you must create the file with an AES flag of `/crypto AES256-SHA1`:
	`ktpass /out outfilename.keytab /mapuser kerberos_account@REALM_IN_ALL_CAPS /princ kerberos_account@REALM_IN_ALL_CAPS /pass kerberos_account_password /ptype KRB5_NT_PRINCIPAL /crypto AES256-SHA1`
	You must specify the location of the krb5.conf file in Settings > BlackBerry Dynamics > Properties (see Configure KCD for BlackBerry Dynamics apps). For more information about constructing a krb5.conf file, see the MIT Kerberos Documentation.

Service Principal Names (SPN)	Create SPNs for all HTTP services, including the BlackBerry Enterprise Mobility Server. You must set an SPN for every target resource you want devices to have access to. For more information about how to create and modify SPNs, see Register a Service Principal Name for Kerberos Connections.

Item	Description
Multi-realm Kerberos environments	• A minimum of one UEM Core must be installed in each Kerberos realm. UEM must reside in the same Kerberos realm as the resource because cross-realm resource delegation is not supported. • Ensure that single-realm KCD is working before configuring multi-realm KCD. • All trusts must be bidirectional, transitive forest trust. • Ensure a maximum of 5 ms latency between the UEM Core instances and the Microsoft SQL Server database. • For each UEM Core instance, use a separate service account with its own unique SPN set and generated keytab file (you can reuse the same account and keytab file on other UEM servers in the same realm). **Note:** If you upgrade from UEM version 12.19 or earlier to UEM 12.20 or later, you must do the following: 1. Generate a new Kerberos keytab file and copy it to each UEM server (see step 2 in Configure KCD for BlackBerry Dynamics apps). 2. In Settings > BlackBerry Dynamics > Properties, in the Service account name under which KCD service is running (gc.krb5.principal.name) field, specify the following: `GCSvc/<UEM_Core_host_machine>@<KERBEROS_REALM_IN_UPPERCASE>`

Configure KCD for BlackBerry Dynamics apps

Before you begin:

- Review the Prerequisites for configuring KCD for BlackBerry Dynamics apps.
- If you are configuring KCD for BlackBerry Docs, see Configuring Kerberos constrained delegation for the Docs service in the BlackBerry Enterprise Mobility Server content.

1. To map the Kerberos service account to an SPN, on the Active Directory server, open the command prompt as an administrator and type the following, specifying the host server name, domain, and Kerberos service account. The Kerberos service account is the service account name under which the KCD service will be configured in UEM (gc.krb5.principal.name). This account does not need to be the same as the UEM service account, but can be.

   ```
   setspn –s GCSvc/<UEM_Core_host_machine> <domain>\<Kerberos_service_account>
   ```

   For example:

   ```
   setspn –s GCSvc/uem1.example.com example.com\kcdadmin
   ```

2. Follow these steps to generate a new Kerberos keytab file and set the Kerberos account password:
   a) On the KDC server, open a command prompt.
   b) Run the following command and specify the appropriate values:

   ```
   ktpass -out <output_filename>.keytab -mapuser
    <Kerberos_account>@<KERBEROS_REALM_IN_UPPERCASE> -princ
    <Kerberos_account>@<KERBEROS_REALM_IN_UPPERCASE> -ptype KRB5_NT_PRINCIPAL -
   pass <Kerberos_account_password>
   ```

If your organization uses a multi-realm Kerberos environment, use the following command instead:

```
ktpass -out <output_filename>.keytab -mapuser
 <Kerberos_service_account>@<KERBEROS_REALM_IN_UPPERCASE> -princ
 GCSvc/<UEM_Core_host_machine>@<KERBEROS_REALM_IN_UPPERCASE> -ptype
 KRB5_NT_PRINCIPAL -pass <Kerberos_account_password>
```

c) Copy the new keytab file to every UEM server that you want to use the same KCD administrator account.

3. Enable enumeration of Active Directory user objects group membership. For more information, see Appendix B: Privileged Accounts and Groups in Active Directory.
4. On each UEM server, follow these steps to configure permissions for the UEM service account so that it can send user credentials to the Kerberos system (this is the same account that has the associated SPN):
   a) In the Microsoft Management Console, navigate to **Local Security Policy > Local Policies > User Rights Assignments**.
   b) Open the properties of **Act as part of the operating system** and click **Add User or Group**.
   c) Type the name of the service account and click **OK**.
5. In the UEM management console, on the menu bar, click **Settings > BlackBerry Dynamics > Global properties**.
6. Select the **Use explicit UPN** check box.
7. Select the **Enable KCD** check box.
8. Click **Save**.
9. On the menu bar, click **Settings > BlackBerry Dynamics > Properties** and click the server name.
10. In the **Fully qualified name for the KDC (gc.krb5.kdc)** field, type the fully qualified name for the KDC. It usually corresponds to the FQDN of an Active Directory domain controller.
11. In the **Location of keytab file (gc.krb5.keytab.file)** field, type the location of the keytab file. Use forward slashes in the path name.
12. In the **Service account name under which KCD service is running (gc.krb5.principal.name)** field, type the name of the service account used by the KCD service.

    In a multi-realm Kerberos environment, instead, specify the following:

    ```
    GCSvc/<UEM_Core_host_machine>@<KERBEROS_REALM_IN_UPPERCASE>
    ```

13. In the **Realm - Active Directory (gc.krb5.realm)** field, type the name of the Active Directory realm in all uppercase letters.
14. In the **Location of krb5.config file on GC server (gc.krb5.config.file)** field, type the location of the krb5.conf file.

    For more information about the requirements for the krb5.conf file, see Prerequisites for configuring KCD for BlackBerry Dynamics apps.
15. Click **Save**.

Requirements to support Kerberos PKINIT for BlackBerry Dynamics apps

BlackBerry UEM supports Kerberos PKINIT for BlackBerry Dynamics user authentication using PKI certificates. If you want to use Kerberos PKINIT for BlackBerry Dynamics apps, your organization must meet the following requirements:

Item	Requirements
KDC	• You must add the KDC host to the allowed domains list in the assigned BlackBerry Dynamics connectivity profile. For more information, see Create a BlackBerry Dynamics connectivity profile in the Administration content. • The KDC host must be listening on TCP port 88 (the Kerberos default port). • The KDC must have an A record (IPv4) or AAAA record (IPv6) in your DNS. • BlackBerry Dynamics doesn't support KDC over UDP. • BlackBerry Dynamics doesn't use Kerberos configuration files (such as krb5.conf) to locate the correct KDC. • The KDC can refer the client to another KDC host. BlackBerry Dynamics will follow the referral, as long as the KDC host that is referred to is added to the allowed domains list in the BlackBerry Dynamics connectivity profile. • The KDC can obtain the TGT transparently to BlackBerry Dynamics from another KDC host. • Kerberos Constrained Delegation must not be enabled.

Server certificates	• Windows KDC server certificates issued via the Active Directory certificate services must come only from the following Windows Server versions. No other server versions are supported.
	  • Internet Information Server with Windows Server 2008 R2
	  • Internet Information Server with Windows Server 2012 R2
	• Valid KDC service certificates must be located either in the BlackBerry Dynamics certificate store or the device certificate store.

Client certificates	• The minimum key length for the certificates must be 2048 bytes. • The extended key usage property of the certificate must be Microsoft Smart Card logon (1.3.6.1.4.1.311.20.2.2). • Client certificates must include the User Principal Name (for example, user@domain.com) in the Subject Alternative Name of object ID szOID_NT_PRINCIPAL_NAME 1.3.6.1.4.1.311.20.2.3. • If the user is issued more than one client certificate, the domain of the User Principal Name must match the domain of the resource that is being accessed to ensure that the correct certificate is used. • Certificates must be valid. Validate them against the servers listed above.

Encrypt the connection between BlackBerry UEM and Microsoft SQL Server

You can configure an encrypted connection between BlackBerry UEM and Microsoft SQL Server. By default, the connection is not encrypted. The steps below provide instructions for enabling the connected encryption after you install UEM. For instructions for enabling the encrypted connection when you install UEM from the command prompt, see the UEM Installation and Upgrade Guide.

Note: The encrypted connection can result in an increase in the CPU on the computer that hosts the BlackBerry UEM Core.

Before you begin: From Microsoft SQL Server, export the root certificate (.cer) that is used to sign the SQL server certificate. Copy the root certificate onto each computer that hosts a UEM Core instance. The file path where you store the certificate must not contain any spaces.

Complete these steps on every computer that hosts a UEM Core instance:

1. Open the command prompt and run the following command to import the root certificate into the Java keystore:

   ```
   keytool -importcert -keystore "<path_to_Java_CA_certs_store>" -
   storepass <CA_certs_store_password> -file <path_to_SQL_root_certificate> -alias
    root
   ```

   For example:

   ```
   keytool -importcert -keystore "c:\Program Files\Eclipse Adoptium\jre-17.0.11.9-
   hotspot\lib\security\cacerts" -storepass changeit -file c:\sqlcert\root.cer -
   alias root
   ```

2. Stop all UEM services.
3. In C:\Program Files\BlackBerry\UEM\common-settings, copy and rename **db.properties** to create a backup database properties file.
4. Open **db.properties**.
5. In the SQL Server encryption settings section, configure the following settings (you do not need to change any other settings):

   ```
   configuration.database.ng.encrypt=true
   configuration.database.ng.trustservercertificate=false
   configuration.database.ng.trustmanagerclass=mdm.contract.database.ssl.
              NiapSQLServerTrustManager
   configuration.database.ng.trustmanagerconstructorarg=<path_to_SQL_root_certificate>
   ```

6. Save and close **db.properties**.
7. Restart the UEM services.

Integrating BlackBerry UEM with Cisco ISE

Cisco Identity Services Engine (ISE) is network administration software that gives an organization the ability to control whether devices can access the work network (for example, permitting or denying Wi-Fi or VPN connections). Cisco ISE administrators can create and enforce access policies to make sure that only permitted devices can access the work network.

You can create a connection between Cisco ISE and BlackBerry UEM on-premises so that Cisco ISE can retrieve data about the devices that are activated on UEM. Cisco ISE checks device data to determine whether devices comply with access policies. For example:

- Cisco ISE checks whether a user's device is activated on UEM. If the device is not activated, an access policy can prevent the device from connecting to work Wi-Fi or VPN access points.
- Cisco ISE checks whether a user's device is compliant with UEM. If the device is not compliant (for example, the device is rooted or jailbroken), an access policy can prevent the device from connecting to work Wi-Fi or VPN access points.

Cisco ISE administrators can view, sort, and filter data about devices in the Cisco ISE management console. Administrators can also lock a device, delete the work data from a device, or delete all data from a device. For more information about network access and device controls, see Managing network access and device controls using Cisco ISE.

To integrate UEM with Cisco ISE, perform the following actions:

Step	Action
1	Verify that your organization's environment meets the requirements to integrate UEM with Cisco ISE.
2	Connect UEM to Cisco ISE and set up an authorization profile and access policies.

Managing network access and device controls using Cisco ISE

Cisco Identity Services Engine (ISE) administrators can perform the following actions.

Action	Description
View device data.	You can view information about devices that are associated with BlackBerry UEM, including the following: • MAC address • Whether the device is compliant with UEM • Whether device data is encrypted • Whether the device is activated (enrolled) on UEM • Whether the device is rooted or jailbroken • Whether the device uses a password • Manufacturer • Model • Serial number • OS version
Configure NAC policies.	Configure access policies that control whether devices can connect to work Wi-Fi or VPN access points. For example, you can set up an access policy that prevents devices that are not compliant with UEM from accessing the work network.
Lock a device.	Lock a user's device. This feature is useful if a user's device is temporarily misplaced. UEM locks the device using an IT administration command. The user must enter the device password to unlock it. Device users can also perform this action using the My Device portal.
Delete work data.	Delete the work data only and work apps from a device, leaving the user's personal data and apps intact. This feature is useful if a user's device is lost or if the user is no longer an employee. UEM deletes work data using an IT administration command. Device users can also perform this action using the My Device portal.
Delete all data.	Delete all data and apps from a device, restoring it to the factory default settings. This feature is useful if a user's device is lost or stolen, or if the device is distributed to another user. UEM deletes all device data using an IT administration command. Device users can also perform this action using the My Device portal.

Requirements: Integrating BlackBerry UEM with Cisco ISE

Item	Requirements
Cisco ISE version	BlackBerry UEM supports integration with Cisco ISE version 1.2 and later.
Supported OS	Any operating system that UEM supports, except for Windows 10 for desktop.

Item	Requirements
Listening port	Cisco ISE uses the default BlackBerry Web Services listening port, 18084, to obtain data about devices from UEM. If port 18084 was not available when UEM was installed, the setup application selected another available port for this purpose. To verify the correct port value, in the BlackBerry UEM Core log file (CORE), search for `(^/ciscoise/.*)` and record the port number that is listed just before this text.
Firewall	If a firewall exists between UEM and Cisco ISE, configure the firewall to allow HTTPS sessions between both systems.
Administrator account	Cisco ISE requires a dedicated UEM administrator account that it can use to retrieve data about devices. You can use an existing administrator account or you can create a new administrator account. It must be a local administrator account (not a directory user). The administrator account requires a role with the following permissions: • View users and activated devices • Manage devices • Lock device and set message • Delete only work data • Delete all device data The default Security Administrator and Enterprise Administrator roles have these permissions, or you can create a custom role with these permissions. For more information, see Create an administrator in the Administration content.

Connect BlackBerry UEM to Cisco ISE

If you do not have a Cisco Identity Services Engine (ISE) administrator account, send these instructions to a Cisco ISE administrator, along with the required information about UEM and the UEM administrator account. For the latest Cisco ISE documentation, visit Cisco ISE Configuration Guides.

Before you begin: In a browser, navigate to **https://<*server_name*>:<*BlackBerry_Web_Services_port*>/enterprise/admin/util/ws?wsdl** where <*server_name*> is the FQDN of the computer that hosts the BlackBerry UEM Core component. The default <*BlackBerry_Web_Services_port*> value is 18084. Use your browser to export the BlackBerry Web Services certificate and save it to your desktop.

1. Log in to the Cisco ISE management console.
2. Import the BlackBerry Web Services certificate into the Cisco ISE trusted certificate store. Select the options to trust for client authentication and syslog, and to trust for authentication of Cisco services.
3. Add an external MDM service and specify the details of the UEM instance, including the FQDN or IP address of the UEM domain, the port (default 18084), and the credentials of the UEM administrator account.
4. For the polling interval, specify how often, in minutes, you want Cisco ISE to poll UEM for device data. It is a best practice to use the default value.

   If you set this value to 60 minutes or less, you might notice a significant performance impact on your organization's environment. If you set this value to 0, Cisco ISE does not poll UEM.
5. Enable and test the connection to UEM.

After the connection is established, you can view the dictionary attributes for UEM in the Cisco ISE management console. Log entries for Cisco ISE polling are written to the BlackBerry UEM Core (CORE) log file.

After you finish: Perform the following configuration tasks in the Cisco ISE management console:

- Configure ACLs on the wireless LAN controller.
- Configure an authorization profile that will redirect devices to the BlackBerry UEM Self-Service console if they try to access the work network while the device is not activated on UEM. The user requires a UEM user account to log in to BlackBerry UEM Self-Service and activate the device. Instruct users to contact the UEM administrator when Cisco ISE directs them to the enrollment page.
- Configure authorization policy rules that determine how Cisco ISE handles devices that are not activated on UEM or compliant with UEM.

Set up VPN using Knox StrongSwan for UEM dark site environments

In a UEM dark site environment you must set up VPN access to your environment so that Samsung Knox devices can access your internal servers and resources. For more information about UEM in dark site environments, see Installing or upgrading BlackBerry UEM in a dark site environment in the Installation content.

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.

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