BlackBerry UEM Cloud

Configuration

Contents

Configuring BlackBerry UEM Cloud for the first time

The following table summarizes the configuration tasks covered in this guide. The tasks are optional based on your organization's needs. Use this table to determine which configuration tasks you should complete.

After you complete the appropriate tasks, you are ready to set up administrators, set up device controls, create users and groups, and activate devices.

Task	Description
Connect to your organization's on-premises company directory and enable secure connectivity features	You can install, activate, and configure the BlackBerry Connectivity Node to provide access to your organization's on-premises company directory and to enable secure connectivity features.
Configure the BlackBerry Connectivity Node to send data through a proxy server	You can configure the BlackBerry Connectivity Node components to send data through a proxy server in your organization’s environment.
Connect BlackBerry UEM to Microsoft Azure	If you want to connect BlackBerry UEM to Azure Active Directory, use BlackBerry UEM to deploy iOS and Android apps managed by Microsoft Intune, or manage Windows 10 apps in BlackBerry UEM, connect BlackBerry UEM to Microsoft Azure.
Link company directory groups to BlackBerry UEM groups	If you connect BlackBerry UEM to your company directory, you can enable directory-linked groups to simplify onboarding and managing users.
Obtain and register an APNs certificate	If you want to manage and send data to iOS or macOS devices, you must obtain a signed CSR from BlackBerry, use it to obtain an APNs certificate from Apple, and register the APNs certificate with the BlackBerry UEM domain.
Configure BlackBerry UEM to support Android devices that have a work profile	To support Android devices that have a work profile, you need to configure your G Suite or Google Cloud domain to support third-party mobile device management providers and configure BlackBerry UEM to communicate with your G Suite or Google Cloud domain.
Configure BlackBerry UEM for the Apple Device Enrollment Program	If you want to use the BlackBerry UEM management console to manage iOS devices that your organization purchased from Apple for DEP, you must configure this feature.
Configure BlackBerry UEM Cloud to support BlackBerry Dynamics apps	If you want to allow users to use BlackBerry Dynamics apps, you can set up BlackBerry UEM Cloud to support the apps.
Migrate users, groups, and other data from BlackBerry UEM	You can use the management console to migrate users, devices, groups, and other data from a source on-premises BES12 or BlackBerry UEM database.

Administrator permissions required to configure BlackBerry UEM

When you perform the configuration tasks in this guide, log in to the management console using the administrator account that you created when you installed BlackBerry UEM. If you want more than one person to complete configuration tasks, you can create additional administrator accounts. For more information about creating administrator accounts, see the Administration content.

If you create additional administrator accounts to configure BlackBerry UEM, you should assign the Security Administrator role to the accounts. The default Security Administrator role has the necessary permissions to complete any configuration task.

Obtaining and activating licenses

To activate devices you must obtain the necessary licenses. You should obtain licenses before you follow the configuration instructions in this guide and before you add user accounts.

For more information about licensing options and the features and products supported by the various license types, see the Licensing content.

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 BlackBerry UEM Cloud to access your organization's on-premises company directory. You can create directory user accounts by searching for and importing user data from the company directory. User data is synchronized with the directory according to the schedule that you configure. BlackBerry 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. For more information, see Connect BlackBerry UEM to a BlackBerry Dynamics PKI connector.
BlackBerry Proxy	BlackBerry Proxy maintains a secure connection between your organization and the BlackBerry Dynamics NOC, which allows BlackBerry Dynamics apps to communicate securely with your organization's resources behind the firewall. It also supports BlackBerry Dynamics Direct Connect, which allows app data to bypass the BlackBerry Dynamics NOC. For more information, see Configuring BlackBerry UEM Cloud to support 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 the Administration content.
BlackBerry Secure Gateway	The 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 the Administration content.
BlackBerry Gatekeeping Service	The BlackBerry Gatekeeping Service makes it easier to control which devices can access Exchange ActiveSync. For more information, see the Administration content.

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

BlackBerry Connectivity Node planning information

Before you install the BlackBerry Connectivity Node, consider the following information.

Hardware

The BlackBerry Connectivity Node must be installed 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.

The computer that hosts the BlackBerry Connectivity Node must meet the following hardware 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

If you enable single-service performance mode, the computer that hosts the BlackBerry Connectivity Node must meet the following hardware requirements:

BlackBerry Connectivity Node with single-service performance mode enabled for BlackBerry Proxy only	• 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
BlackBerry Connectivity Node with single-service performance mode enabled for BlackBerry Secure Connect Plus only	• 4 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
BlackBerry Connectivity Node with single-service performance mode enabled for BlackBerry Secure Gateway only	• 8 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

Software

To verify that your environment meets the requirements for installing the BlackBerry Connectivity Node, see the Compatibility matrix.

Scalability and high availability

Each BlackBerry Connectivity Node can support up to 5000 devices. You can install additional BlackBerry Connectivity Nodes to support up to 50,000 additional devices.

You can install one or more instances of the BlackBerry Connectivity Node to provide redundancy. You must install each instance on a dedicated computer. Use the same company directory configuration for all instances.

Deploy more than one BlackBerry Connectivity Node in a server group to allow for high availability and load balancing.

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 frees

up server resources to allow fewer servers required for the same number of users or containers. Each BlackBerry Connectivity Node enabled for single-service performance mode can support up to 10,000 devices.

Steps to install and activate the BlackBerry Connectivity Node

To install and activate the BlackBerry Connectivity Node, perform the following actions:

1	Verify that your organization meets the prerequisites to install the BlackBerry Connectivity Node.
2	Download the installation and activation files for the BlackBerry Connectivity Node from the management console.
3	Install, activate, and configure the BlackBerry Connectivity Node.
4	If necessary, configure proxy settings for the BlackBerry Connectivity Node components.
5	Perform additional configuration for BlackBerry Secure Connect Plus, the BlackBerry Secure Gateway, the BlackBerry Gatekeeping Service, and BlackBerry Dynamics apps.

Prerequisites: Installing the BlackBerry Connectivity Node

- Verify that the computer is running Windows PowerShell 2.0 or later. This is required for the setup application to install RRAS for BlackBerry Secure Connect Plus and the BlackBerry Gatekeeping Service.

  Note: If the setup application cannot install RRAS on the computer, you must stop the installation, install RRAS manually, and restart the installation.
- Choose a directory account with read permissions for each configured directory connection that the BlackBerry Cloud Connector can use to access the company directories.
- Use a BlackBerry UEM Cloud account with permissions to download the BlackBerry Connectivity Node installation and activation files (for example, Security Administrator).
- Use a Windows account with permissions to install and configure software on the computer that will host the BlackBerry Connectivity Node.
- 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 (<*region*>.bbsecure.com, for example na.region.com or eu.region.com):
  - 443 (HTTPS) to activate the BlackBerry Connectivity Node
  - 3101 (TCP) for all other outbound connections

Set an environment variable for the Java location

BlackBerry UEM requires you to install a JRE 8 implementation on the servers where you will install BlackBerry UEM, and that you have an environment variable that points to the Java home location. For more information about supported JRE versions, see the Compatibility matrix. When you begin the installation, BlackBerry UEM verifies that it can find Java. If you have installed the Oracle Java SE Runtime Environment in the default location, BlackBerry UEM will find it and automatically set the environment variable. If BlackBerry UEM can't find Java, the

setup application will stop and you must set an environment variable for the Java location and ensure that the Java bin folder is included in the Path system variable.

Visit support.blackberry.com to read article 52117.

Before you begin: Verify that you have installed a supported JDK on the server where you will be installing BlackBerry UEM.

1. Open the **Windows Advanced system settings** dialog box.
2. Click **Environment Variables**.
3. Under the **System variables** list, click **New**.
4. In the **Variable name** field, type `BB_JAVA_HOME`.
5. In the **Variable value** field, type the path to the JRE (Java Runtime Environment) folder and click **OK**.
6. In the **System variables** list, select **Path** and click **Edit**.
7. If the Path doesn't include the Java bin folder, click **New** and add `%BB_JAVA_HOME%\bin` to the Path.
8. Move the %BB_JAVA_HOME%\bin entry high enough in the list that it won't be superseded by another entry and click **OK**.

Installing or upgrading the BlackBerry Connectivity Node

Follow the instructions in this section to install or upgrade the BlackBerry Connectivity Node.

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

You must install each instance on a dedicated computer.

You can configure one or more directory connections, but if you have multiple BlackBerry Connectivity Nodes, 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.

If you have more than one BlackBerry Connectivity Node, you must upgrade all of them to the same software release.

Note: If you are upgrading multiple BlackBerry Connectivity Nodes, directory services are disabled after the first node is upgraded until all the nodes are upgraded to the same version.

Download the installation and activation files for the BlackBerry Connectivity Node

1. In the 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 the installation package.
5. 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.
6. Click **Generate**.
7. Save the activation file (.txt).

   The activation file is valid for 60 minutes. If you wait longer than 60 minutes before you use the activation file, you must generate a new activation file. Only the latest activation file is valid.

After you finish: Install and configure the BlackBerry Connectivity Node.

Install and configure the BlackBerry Connectivity Node

Before you begin: Download the installation and activation files for the BlackBerry Connectivity Node.

1. Open the BlackBerry Connectivity Node installation file (.exe) that you downloaded from the management console.

   If a Windows message appears and requests permission to make changes to the computer, click **Yes**.
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 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 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 (for example na.bbsecure.com or eu.bbsecure.com). Click **Save**.
   - To send other outbound connections from the components of the BlackBerry Connectivity Node through a 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 (for example na.bbsecure.com or eu.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 that you downloaded from the management console.
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 (for example na.bbsecure.com or eu.bbsecure.com) 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 this company directory connection. **Note:** If you have a Microsoft Azure directory configured, this connection name must be different than the name of the Azure directory connection. **Note:** You cannot change the name after you save the configuration. **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 BlackBerry 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	**a.** In the **Connection name** field, type a name for this company directory connection. **Note:** If you have a Microsoft Azure directory configured, this connection name must be different than the name of the Azure directory connection. **Note:** You cannot change the name after you save the configuration. **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 port number of the LDAP computer. **e.** In the **Authorization required** drop-down list, select whether BlackBerry UEM Cloud must authenticate with the LDAP computer. If you click **Yes**, type the username and password of the LDAP account. The username must be in DN format (for example, CN=Megan Ball,OU=Sales,DC=example,DC=com). **f.** In the **Search base** field, type the search base that you want to access (for example, OU=Users,DC=example,DC=com). **g.** In the **LDAP user search filter** field, type the filter that you want to use for LDAP users. For example: (&(objectCategory=person)(objectclass=user)(memberOf=CN=Local,OU=Users,DC=example,DC=com)). **h.** 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**. **i.** In the **Unique identifier** field, type the attribute for each user's unique identifier (for example, uid). The attribute must be immutable and globally unique for every user. **j.** In the **First name** field, type the attribute for each user's first name (for example, givenName). **k.** In the **Last name** field, type the attribute for each user's last name (for example, sn). **l.** In the **Login attribute** field, type the attribute for each user's login attribute (for example, cn). This attribute is used for the value that users type to log in to BlackBerry UEM Self-Service with their directory credentials. **m.** In the **Email address** field, type the attribute for each user's email (for example, mail). **n.** In the **Display name** field, type the attribute for each user's display name (for example, displayName). **o.** 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. **p.** To enable directory-linked groups, select the **Enable directory-linked groups** check box. For more information about directory-linked groups, see Linking company directory groups to BlackBerry UEM groups. **q.** 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 a second BlackBerry Connectivity Node instance for redundancy, download another set of installation and activation files and repeat this task on a different computer. This should be done after the first instance has been activated.
- You can configure one or more directory connections, but if you have multiple BlackBerry Connectivity Nodes, 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. You can make this task easier by Copying directory connection configurations from one BlackBerry Connectivity Node to another.
- If necessary, configure proxy settings for the BlackBerry Connectivity Node. For instructions, see Configuring the BlackBerry Connectivity Node to use a TCP proxy server.
- To change the directory settings that you configured, in the BlackBerry Connectivity Node console (http:/localhost:8088), click **General settings > Company directory**. Click ✎ for the directory connection.
- If you want to send data through an HTTP proxy before it reaches the BlackBerry Dynamics NOC, in the BlackBerry Connectivity Node console (http://localhost:8088), click Click **General settings > BlackBerry Router and proxy**. Select the **Enable HTTP proxy** checkbox and configure the proxy settings.
- For instructions for enabling BlackBerry Secure Connect Plus, see "Using BlackBerry Secure Connect Plus for connections to work resources" in the Administration content.
- For more information about enabling the BlackBerry Secure Gateway, see "Protecting email data 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.

Copy directory connection configurations

If your environment has multiple BlackBerry Connectivity Nodes, the directory connections must be configured identically on all nodes. To help make this task easier, you can export the directory connection configuration from one BlackBerry Connectivity Node and import it to another.

Note: Before you can import company directory configurations to a BlackBerry Connectivity Node, you must remove any existing company directory connections from that node.

1. On the BlackBerry Connectivity Node that you want to copy the configuration from, in the **Company directory connection** screen, click **Export the directory connections in .txt file**.

   A .txt file containing information about the company directory connections is downloaded to your computer.
2. On the BlackBerry Connectivity Node that you want to copy the configuration to, on the **Company directory connection** screen, browse to the .txt file you downloaded.
3. Click **Import connections**.

   The company directory connections are added to the BlackBerry Connectivity Node.

Change the default settings for BlackBerry Connectivity Node instances

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 BlackBerry Gatekeeping Service that is installed with the primary BlackBerry UEM components, you can change the default behavior to disable the BlackBerry Gatekeeping Service in each instance. You can specify the default logging settings for all BlackBerry Connectivity Node instances. You can also enable the BlackBerry Secure Gateway settings for all BlackBerry Connectivity Node

instances and specify the discovery endpoint and mail server resource that iOS devices that run iOS 13.0 or later must use to authenticate to Microsoft Exchange Online using modern authentication.

The default settings apply to each BlackBerry Connectivity Node instance that is not in a server group. When an instance is part of a server group, it uses the default settings configured for that server group.

1. In the BlackBerry UEM management console, on the menu bar, click **Settings > External integration > BlackBerry Connectivity Node setup**.
2. Click  .
3. If you want to disable the BlackBerry Gatekeeping Service in each instance, select the **Override BlackBerry Gatekeeping Service settings** check box.
4. If you want to configure logging settings, select the **Override logging settings** check box. Perform any of the following tasks:
   - 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 specify maximum limits for log file size and age, select the **Enable local file destination** check box. Specify the size limit (in MB) and the age limit (in days).
5. If you want to specify the BlackBerry Secure Gateway in each instance, select the **Override BlackBerry Secure Gateway settings** check box. For iOS devices that run 13.0 or later and use modern authentication to the connect to Microsoft Exchange Online, complete the following steps to 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 using OAuth. 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`).
6. Click **Save**.

After you finish: If you disabled the BlackBerry Gatekeeping Service instances and you want to enable them again, select the **Enable the BlackBerry Gatekeeping Service** check box. Each instance must be able to access your organization's gatekeeping server.

Upgrade the BlackBerry Connectivity Node

When you are notified of an update to BlackBerry UEM Cloud, use the following instructions to upgrade the BlackBerry Connectivity Node components to the latest version.

1. On the computer that hosts the BlackBerry Connectivity Node, open the BlackBerry Connectivity Node console (http:/localhost:8088).
2. Record the current directory configuration settings.
3. Log in to the BlackBerry UEM Cloud management console.
4. Download the BlackBerry Connectivity Node installation and activation files. For instructions, see Download the installation and activation files for the BlackBerry Connectivity Node.
5. Install and configure the BlackBerry Cloud Connector using the information you recorded in step 2. For instructions, see Install and configure the BlackBerry Connectivity Node.

Creating server groups

You can set up regional connections for enterprise connectivity features by deploying one or more BlackBerry Connectivity Node instances in a dedicated region. This is known 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. You can associate email and enterprise connectivity profiles with a server group. Any device that is assigned those profiles uses that server group's regional connection to the BlackBerry Infrastructure when it uses any of the components of the BlackBerry Connectivity Node.

Deploying more than one BlackBerry Connectivity Node in a server group also allows for high availability and load balancing.

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

Create a server group

Before you begin: Install an additional BlackBerry Connectivity Node

1. 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 country where one or more instances of the BlackBerry Connectivity Node will be installed. The BlackBerry Connectivity Node instances that are added to the server group will use the selected country's regional connection to the BlackBerry Infrastructure.

   Note: You cannot change this setting after the server group is created.
5. By default, each BlackBerry Connectivity Node instance must be configured to the same company directories. If you want to disable the company directory connector for the BlackBerry Connectivity Node 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 that are configured at **Settings > Infrastructure > BlackBerry Secure Connect Plus**, select the **Override DNS servers** check box. Perform the following tasks:

   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.

   For more information, see "Enabling and configuring enterprise connectivity and BlackBerry Secure Connect Plus" in the Administration content.
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. Perform any of the following tasks:

   - 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 specify maximum limits for log file size and age, select the **Enable local file destination** check box. Specify the size limit (in MB) and the age limit (in days).

9. If you want to designate the BlackBerry Connectivity Node for only one connection type, select the **Enable single-service performance mode** check box. In the 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 BlackBerry Connectivity Node instance in the server group, select the **Override BlackBerry Secure Gateway settings** check box. For iOS devices running iOS 13.0 or later 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 using OAuth for authentication. 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:

- If you disabled the BlackBerry Gatekeeping Service instances in a server group and you want to enable them again, in **Settings > External integration > BlackBerry Connectivity Node setup**, select the server group and select the **Enable the BlackBerry Gatekeeping Service** check box. Each instance must be able to access your organization's gatekeeping server.
- Install and configure the BlackBerry Connectivity Node and then add the instance to a server group.

Manage server groups

You can add a BlackBerry Connectivity Node instance to a server group at any time, or remove an instance from a server group at any time. If you add an instance to a server group, that instance uses the settings that have been configured for that server group (for example, the components of that instance will use the specified regional connection to the BlackBerry Infrastructure). If you remove an instance from a server group, that instance uses the default settings that are configured on the BlackBerry Connectivity Node setup screen (see Change the default settings for BlackBerry Connectivity Node instances).

1. In the BlackBerry UEM management console, on the menu bar, click **Settings > External integration > BlackBerry Connectivity Node setup**.
2. Select a BlackBerry Connectivity Node instance.
3. Perform one of the following tasks:
    a) To add an instance to a server group, click  . Select the appropriate server group. Click **OK**.
    b) To remove an instance from a server group, click  . In the confirmation dialog box, click **OK**.

Troubleshooting BlackBerry Connectivity Node issues

When you troubleshoot issues with the BlackBerry Connectivity Node, consider the following common issues.

For more information about BlackBerry support resources, visit BlackBerry Technical Support.

The BlackBerry Connectivity Node does not activate with BlackBerry UEM Cloud

Description

After you upload the activation file and click Activate, you receive an error message that the activation was not successful.

Possible solutions

Try any of the following:

- Verify that you uploaded the latest activation file that you generated in the management console. Only the latest activation file is valid.
- Activation files expire after 60 minutes. Generate and upload a new activation file, then try to activate again.
- Visit support.blackberry.com/community to read article 38964.

The BlackBerry Connectivity Node does not connect with the company directory

Description

After you specify the information for your company directory and click Save, you receive an error message that the BlackBerry Connectivity Node cannot connect with the company directory.

Possible solutions

Try any of the following:

- If you have multiple BlackBerry Connectivity Nodes, verify that they are all at the same software version.
- Verify that you specified the correct settings for the company directory.
- Verify that all BlackBerry Connectivity Nodes have a directory connection and that the directory connections are configured identically on all enrolled BlackBerry Connectivity Nodes.
- 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 for the BlackBerry Connectivity Node are located in *<drive:>*:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs.
- If you are using Microsoft Active Directory, visit support.blackberry.com/community to read article 36955.

The BlackBerry Connectivity Node does not connect with BlackBerry UEM Cloud

Description

When you test the connection between the BlackBerry Connectivity Node and BlackBerry UEM Cloud, you receive an error message that the test was not successful.

Possible solutions

Try any of the following:

- 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 (*region*.bbsecure.com):
  - 443 (HTTPS) 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 BlackBerry UEM Cloud. By default, the log files for the BlackBerry Cloud Connector are located in <*drive:*>:\Program Files\BlackBerry\BlackBerry Connectivity Node\Logs.

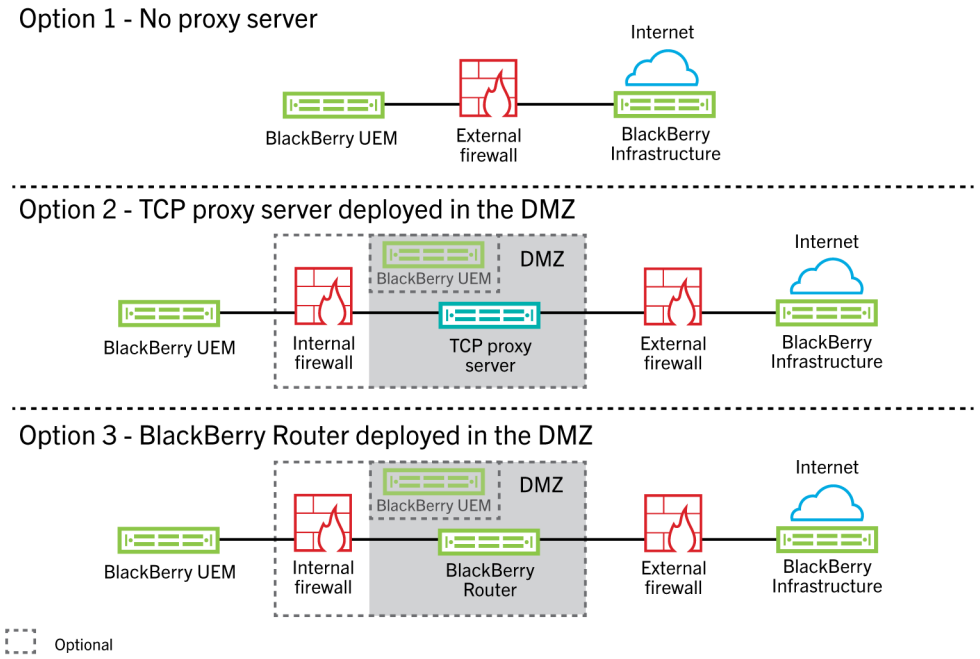
Configuring the BlackBerry Connectivity Node to use a TCP proxy server

To use a proxy server with the BlackBerry Connectivity Node, you can use a TCP proxy server that is already installed in your organization's environment.

You can install the proxy server outside your organization's firewall in a DMZ. Installing a TCP proxy server in a DMZ provides an extra level of security. Only 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. However, 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 the BlackBerry Connectivity Node and the BlackBerry Infrastructure.

This image shows the following options for sending data through a proxy server to the BlackBerry Infrastructure: no proxy server, and a TCP proxy server deployed in a DMZ.



Sending data through a TCP proxy server to the BlackBerry Infrastructure

When you activate the BlackBerry Connectivity Node, it sends data over port 443 (HTTPS) to activate with BlackBerry UEM Cloud. 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 HTTPS or TCP data through a 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 BlackBerry 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.

Comparing TCP proxies

Proxy	Description
Transparent TCP proxy	• Intercepts normal communication at the network layer without requiring any special client configuration • Requires no client browser configuration • Usually located between the client and the Internet • Performs some of the functions of a gateway or router • Often used to enforce acceptable use policy • Commonly used by ISPs in some countries to save upstream bandwidth and improve customer response times through caching
SOCKS v5 proxy	• An Internet protocol for handling Internet traffic through a proxy server • Can be handled with virtually any TCP/UDP application, including browsers and FTP clients that support SOCKS • Can be a good solution for Internet anonymity and security • Routes network packets between a client and server through a proxy server • Can provide authentication so only authorized users can access a server • Proxies TCP connections to an arbitrary IP address • Can anonymize UDP protocols and TCP protocols like HTTP

Configure BlackBerry UEM to use a transparent TCP proxy server

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

1. In the BlackBerry Connectivity Node console (http:/localhost:8088), click **General settings > Proxy**.
2. Select the **Proxy server** option.
3. Perform any of the following tasks:

Task	Steps
Route HTTPS activation data for the BlackBerry Connectivity Node through a 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 <*region*>.bbsecure.com.

Task	Steps
Route outbound connections from the components of the BlackBerry Connectivity Node through a 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 <*region*>.bbsecure.com.

4. 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 BlackBerry UEM domain.

1. In the BlackBerry Connectivity Node console (http:/localhost:8088), click **General settings > Proxy**.
2. Select the **Proxy server** option.
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 1 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**.

Connecting BlackBerry UEM to Microsoft Azure

Microsoft Azure is the Microsoft cloud computing service for deploying and managing applications and services. Connecting BlackBerry UEM to Azure provides your organization with the following features:

- Connect BlackBerry UEM to Azure Active Directory and create directory user accounts in BlackBerry UEM by searching for and importing user data from the company directory. 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.
- Use BlackBerry UEM to deploy iOS and Android apps managed by Microsoft Intune.
- Manage Windows 10 apps in BlackBerry UEM

If your organization uses Microsoft Active Directory instead of Azure Active Directory, to connect with Azure you must install the most recent version of the BlackBerry Connectivity Node to allow BlackBerry UEM Cloud to access your company directory.

BlackBerry UEM supports configuring only one Azure tenant. To connect BlackBerry UEM to Azure, you perform the following actions:

Step	Action
1	Create a Microsoft Azure account.
2	If your organization uses Azure Active Directory, configure BlackBerry UEM Cloud to synchronize with Azure Active Directory.
3	If your organization uses an on-premises Microsoft Active Directory and you want to use BlackBerry UEM to deploy apps managed by Microsoft Intune or manage Windows 10 apps, Synchronize Microsoft Active Directory with Microsoft Azure.
4	Create enterprise applications in Azure to allow BlackBerry UEM Cloud to connect to Microsoft Intune and the Windows Store for Business.
5	Configure BlackBerry UEM to synchronize with Microsoft Intune and the Windows Store for Business.
6	(Optional) Configure Azure Active Directory conditional access.

Create a Microsoft Azure account

To deploy apps protected by Microsoft Intune to iOS and Android devices or manage Windows 10 apps in BlackBerry UEM, you must have a Microsoft Azure account and authenticate BlackBerry UEM with Azure.

Complete this task if your organization doesn't have a Microsoft Azure account.

Note: To ensure you have the correct licenses and account permissions for Microsoft Intune, visit support.blackberry.com/community to read article 50341.

1. Go to https://azure.microsoft.com and click **Free account**, then follow the prompts to create the account.

You are required to provide credit card information to create the account.

2. Sign in to the Azure management portal at https://portal.azure.com and log in with the username and password you created when you signed up.

Configure BlackBerry UEM to synchronize with Azure Active Directory

If your organization uses Microsoft Azure Active Directory, you can connect it to BlackBerry UEM to create directory user accounts in BlackBerry UEM by searching for and importing user data from the company directory. Directory users can use their directory credentials to access BlackBerry UEM Self-Service.

You can connect to more than one instance of Azure Active Directory. If you install the BlackBerry Connectivity Node you can also connect to an on-premises directory.

1. Log in to the Azure portal.
2. Go to **Microsoft Azure > Azure Active Directory > App registrations**.
3. Click **+ New registration**.
4. In the **Name** field, enter a name for the app.
5. Select which account types can use the application or access the API.
6. In the **Redirect URI** section, in the drop-down list, select **Web** and enter `http://localhost`.
7. Click **Register**.
8. Copy **Application ID** of your application and paste it to a text file.
   This is the **Client ID** required in BlackBerry UEM.
9. In the **Manage** section, click **API permissions**.
10. Click **+ Add a permission** and perform the following actions:
    a) Select **Microsoft Graph**.
    b) Select **Application permissions**.
    c) Set the following permissions:
       - Group.Read.All (Application)
       - User.Read (Delegated)
       - User.Read.All (Application)
    d) Click **Add permissions**.
    e) Under **Grant consent**, click **Grant admin consent**.

       Note: You must be a global administrator to grant permissions.
    f) When you are prompted, click **Yes** to grant permissions for all accounts in the current directory.
11. In the **Management** section, click **Certificates and secrets**. Perform the following actions:
    a) Under **Client secrets**, click **New client secret**.
    b) Type a description for the client secret.
    c) Select a duration for the client secret.
    d) Click **Add**.
    e) Copy the value of the new client secret.
       This is the Client key that is required for BlackBerry UEM.
12. In the management console, click **Settings > External integration > + Company directory > Microsoft Azure Active Directory connection**.
13. Enter a **Directory connection name** and the **Domain** for your Azure Active Directory.
14. Do one of the following:

- If this is a new connection to Azure, enter the information you copied from the Azure portal when you created the enterprise application in Azure.
  - **Client ID**: The application ID generated by the Azure application registration
  - **Client key**: The client secret generated by the Azure application registration
- If this is an existing connection to Azure, click **Enable single tenant application registration** and enter the information you copied from the Azure portal when you created the enterprise application in Azure.
  - **Client ID**: The application ID generated by the Azure application registration
  - **Client key**: The client secret generated by the Azure application registration

15. Click **Continue**.

16. Click **Save**.

After you finish: Link company directory groups to BlackBerry UEM groups

Synchronize Microsoft Active Directory with Microsoft Azure

To allow Windows 10 users to install online apps or to send apps protected by Microsoft Intune to iOS and Android devices, users must exist in the Microsoft Azure Active Directory. If you are using an on-premises Active Directory, you must synchronize users and groups between your on-premises Active Directory and Azure Active Directory using Microsoft Azure Active Directory Connect. For more information, visit https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect.

1. Download Azure AD Connect from the Microsoft Download Center.
2. Install the Azure AD Connect software.
3. Configure Azure AD Connect to connect your on-premises Active Directory with the Azure Active Directory.

After you finish: Create an enterprise endpoint in Azure

Create an enterprise endpoint in Azure

To provide BlackBerry UEM access to Microsoft Azure, you must create an enterprise endpoint within Azure. The enterprise endpoint allows BlackBerry UEM to authenticate with Microsoft Azure. For more information, see https://docs.microsoft.com/en-us/azure/active-directory/active-directory-app-registration.

If you are connecting BlackBerry UEM to both Microsoft Intune and the Windows Store for Business, use a different enterprise application for each purpose due to differences in permissions and potential future changes.

Note:

Microsoft national cloud deployments (or any deployment that requires a login URL other than login.microsoftonline.com) require additional steps to connect UEM with Intune. For more information, visit support.blackberry.com/community to read article KB75773.

Before you begin:

- If your organization uses an on-premises Microsoft Active Directory, Synchronize Microsoft Active Directory with Microsoft Azure
- Make sure that you have the Reply URL. For instructions on obtaining the Reply URL for modern authentication, see Configure BlackBerry UEM to synchronize with Microsoft Intune.

1. Log in to the Azure portal.
2. Go to **Microsoft Azure > Azure Active Directory > App registrations**.
3. Click **New registration**.

4. In the **Name** field, enter a name for the app.
5. Select which account types can use the application or access the API.
6. In the **Redirect URI** section, in the drop-down list, select **Mobile Client/Desktop** and enter a valid URL. The URL format is https://<*FQDN_of_the_BlackBerry_UEM_server*>:<*port*>/admin/intuneauth
7. Click **Register**.
8. Copy the **Application ID** of your application and paste it to a text file.

   This is the **Client ID** required in BlackBerry UEM.
9. If you are creating the application to use Microsoft Intune, click **API permissions** in the **Manage** section. Perform the following steps:
   a) Click **Add a permission**.
   b) Select **Microsoft Graph**.
   c) Select **Delegated permissions**.
   d) Scroll down in the permissions list and under **Delegated Permissions**, set the following permissions for Microsoft Intune:
      - 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**)

   e) Click **Add permissions**.
   f) Under **Grant consent**, click **Grant admin consent**.

      Note: You must be a global administrator to grant permissions.
   g) When you are prompted, click **Yes** to grant permissions for all accounts in the current directory.

   You can use the default permissions if you are creating the app to connect to the Windows Store for Business.
10. Click **Certificates and secrets** in the **Manage** section. Perform the following actions:
    a) Under **Client secrets**, click **New client secret**.
    b) Type a description for the client secret.
    c) Select a duration for the client secret.
    d) Click **Add**.
    e) Copy the value of the new client secret.

       This is the **Client Key** that is required in BlackBerry UEM.

       Warning: If you do not copy the value of your key at this time, you will have to create a new key because the value is not displayed after you leave this screen.

After you finish: Configure BlackBerry UEM to synchronize with Microsoft Intune or Configure BlackBerry UEM to synchronize with the Windows Store for Business.

Configuring Azure Active Directory conditional access

If you have configured Azure AD conditional access for your organization, you can configure a BlackBerry UEM tenant as a compliance partner so that iOS and Android devices managed by UEM can connect to your cloud-based apps such as Office 365. You can configure only one UEM tenant for each Azure tenant.

You can configure connections to multiple Azure tenants. If you create multiple connections,

Note: Azure AD conditional access support is currently limited in the following situations:

- BlackBerry UEM Client does not support Azure AD conditional access policies with the "All cloud apps" option selected under "Cloud apps" or actions". You must instead select the specific apps that you want to include in the policy. For more information, visit support.blackberry.com/community to read article 90010.
- BlackBerry Work does not support the Azure AD conditional access compliance feature. For more information, visit support.blackberry.com/community to read article 89668.

To use this feature, users must meet the following requirements:

- Users must exist in Azure AD,
- If you are synchronizing your on-premises Active Directory to Azure AD, users' on-premises Active Directory UPN must match their Azure AD UPN. If these values do not match in your environment, please visit support.blackberry.com/community to read article 88208.
- Users must be added to UEM though synchronization with Active Directory.
- Users must have both the Microsoft Authenticator app and the BlackBerry UEM Client installed.

If you configure Azure AD conditional access, UEM notifies Azure AD when a device is out of compliance and conditions are enforced in the following circumstances:

- If the "Enforcement action for device" setting is set to something other than "Monitor and log," UEM notifies Azure AD after all user prompts have expired.
- If the "Enforcement action for BlackBerry Dynamics apps" setting is set to something other than "Monitor and log," UEM notifies Azure AD as soon as the compliance violation is detected.

For more information on Compliance profiles, see the UEM Administration content.

For more information on Azure AD conditional access, see the Microsoft documentation.

Configure BlackBerry UEM as a Compliance Partner in Azure

Before you begin: You must have the appropriate Microsoft Intune license to use this feature. For more information, visit support.blackberry.com to read KB91041 and KB50341. For more information about licensing, see the details from Microsoft. The administrator account that you use to complete the following steps must have an Intune license.

In the Microsoft Endpoint Manager admin center, under **Tenant Administration > Connectors and Tokens > Partner Compliance Management** add **BlackBerry UEM** as a compliance partner for iOS and Android devices and assign it to users and groups.

If you support both iOS and Android devices, you need to add BlackBerry UEM as a compliance partner for each platform. For more information, see the Microsoft documentation.

Configure Azure Active Directory conditional access

1. In the BlackBerry UEM management console, click **Settings > External integration > Azure Active Directory Conditional Access**.
2. In the table, click +.
3. Type a name for the configuration.
4. In the **Azure cloud** drop-down list, select **Global**.
5. Type your **Azure tenant ID**.

   You can enter either the tenant name, which is in FQDN format, or the unique tenant ID, which is in GUID format.
6. In the device mapping override, select **UPN** or **Email**.

   By default, UPN is selected. If UPN is used, you should verify that the Azure AD tenant and all mapped directories share the same UPN value for users before you save the connection. After you save the connection, the device mapping override cannot be changed.

7. In the **Available company directories** list, select one or more directory instances and click ➔.
8. Click **Save**.
9. Select the administrator account that you want to use to log in to your Azure tenant.

   The administrator account must be able to grant permissions to the app to access resources in your organization. such as global administrator, cloud application administrator, or application administrator.
10. Accept the Microsoft permission request.

Configure the BlackBerry Dynamics connectivity profile to support the AzureConditional Access feature

In the BlackBerry UEM management console, edit each BlackBerry Dynamics connectivity profile.

1. Under App servers, click Add.
2. Select **Feature-Azure Conditional Access** from the app list.
3. Click + to add a new app server.
4. If you are using BlackBerry UEM in a on-premises environment, specify the following server settings.

Item	Description
Server	gdas-<SRP_ID>.<region_code>.bbsecure.com
Port	443
Route	Direct

   If you have BlackBerry UEM Cloud and BEMS Cloud in your environment and you configured Email notifications or BEMS-Docs to create a BEMS tenant, the BEMS Cloud URL, port number, and priority are added automatically to the App server payload section.

Assign the Feature - Azure conditional access app to users

You can assign the app to users or groups.

Do one of the following:

Task	Steps
Assign the app to a user	a. On the menu bar, click **Users > Managed devices**. b. In the search results, click the name of a user account. c. In the **Apps** section, click **+**. d. Search for and select the Feature - Azure conditional access app. e. Click **Next**. f. Optionally, complete the **Disposition**, **Per-app VPN**, and **App configuration** fields. g. Click **Assign**.

Task	Steps
Assign the app to a group	**a.** On the menu bar, click **Groups**. **b.** On the **User groups** tab, click the name of a group. **c.** In the **Assigned apps** section, click **+**. **d.** Search for and select the Feature - Azure conditional access app. **e.** Click **Next**. **f.** Optionally, complete the **Disposition**, **Per-app VPN**, and **App configuration** fields. **g.** Click **Assign**.

Configure a BlackBerry Dynamics Profile

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > BlackBerry Dynamics**.
3. Click **+**.
4. Type a name and description for the profile.
5. Select the **Enable UEM Client to enroll in BlackBerry Dynamics** setting.
6. Configure the appropriate values for the rest of the profile settings. For more information about each profile setting, see BlackBerry Dynamics profile settings.
7. Click **Add**.

After you finish:

- The Microsoft Authenticator app must be installed on users' devices. You can download the app from the appropriate app store, and add it to UEM. For more details, see the information for iOS and the information for Android. You then assign the app to users or to groups. You can also instruct users to install the app from their app store.
- After Active Directory conditional access is configured, users activating devices are prompted to register with Active Directory conditional access during activation. Uses with activated devices are prompted to register with Active Directory conditional access the next time they open the UEM Client.

Remove devices from Azure Active Directory conditional access

When you deactivate a device from BlackBerry UEM, the device remains registered for Azure AD conditional access. Azure recognizes that the device is no longer managed, which, depending on your conditional access settings, may put the device out of compliance.

Users can remove their devices from Azure by removing their Azure AD account from the account settings in the Microsoft Authenticator app or you can remove the device from Azure.

1. In the Azure portal, in Azure AD, select the user who you want to delete the device for.
2. View the **Devices** page for the user.
3. Select the device and click **Delete**.

Linking company directory groups to BlackBerry UEM groups

You can create groups in BlackBerry UEM that are linked to groups in your company directory. By enabling directory-linked groups, you can take advantage of the following features:

- Ability to add groups in BlackBerry UEM that are linked to company directory groups for the purpose of assigning and managing the IT policies, profiles, and apps for users. These groups are called directory-linked groups.

  For information about creating directory-linked groups, see the Administration content.
- Ability to add groups in BlackBerry UEM that are linked to company directory groups for the purpose of automatically synchronizing group membership. These groups are called onboarding directory groups. See Enabling onboarding.

Enable directory-linked groups

Before you begin: 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. On the menu bar, click **Settings > External integration > Company directory**.
2. Click the company directory name that you want to edit.
3. On the **Sync settings** tab, select the **Enable directory-linked groups** check box.
4. To force the synchronization of company directory groups, select the **Force synchronization** check box.

   If selected, when a group is removed from your 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. If they are not selected, and a company directory group is not found, the synchronization process is canceled.
5. In the **Sync limit** field, type the maximum number of changes you want to allow for each synchronization process.

   The default setting is five. If the number of changes to be synchronized exceeds the synchronization limit, you can prevent the synchronization process from running. Changes are calculated by adding the following: users to add to groups, users to remove from groups, users to be onboarded, users to be offboarded.
6. In the **Maximum nesting level of directory groups** field, type the number of nested levels to synchronize for company directory groups.
7. Click **Save**.

After you finish: Create directory-linked groups. For more information, see the Administration content.

Enabling onboarding

Onboarding allows you to automatically add user accounts to BlackBerry UEM based on user membership in a universal or global company directory group. User accounts are added to BlackBerry UEM during the synchronization process.

You can also choose to automatically send onboarded users an email message and activation passwords or access keys for BlackBerry Dynamics apps.

Offboarding

If you enable onboarding, you can also choose to configure offboarding. When a user is disabled in Microsoft Active Directory or removed from all company directory groups in the onboarding directory groups, BlackBerry UEM can automatically offboard the user in any of the following ways:

- Delete work data or all data from the users' devices
- Delete the user account from BlackBerry UEM

You can use offboarding protection to delay the deletion of device data or user accounts to avoid unexpected deletions because of directory replication latency. By default, offboarding protection delays offboarding actions for two hours after the next synchronization cycle.

Note: The offboarding settings also apply to existing directory users in BlackBerry UEM. It is recommended that you click the preview icon to generate the directory synchronization report and verify the changes.

Synchronization

After you enable offboarding, during the next synchronization, the offboarding rules are applied to any users that you manually added in the management console before offboarding was turned on and that are not members of any onboarding directory-linked groups.

After you enable onboarding, you can manually add users to BlackBerry UEM even if they are already in a directory-linked group. If offboarding is enabled, users that you manually add to BlackBerry UEM will have offboarding rules applied to their devices when the next synchronization occurs if they are not members of an onboarding synchronization group at the time of the synchronization.

Enable and configure onboarding and offboarding

You can automatically onboard users that are members of universal and global groups. Onboarding is not supported for domain local groups.

Before you begin:

- 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. On the menu bar, click **Settings > External integration > Company directory**.
2. Click the company directory name that you want to edit.
3. On the **Sync settings** tab, select the **Enable directory-linked groups** check box.
4. Select the **Enable onboarding** check box.
5. Perform the following actions for each group that you want to configure for onboarding with a device activation option:
   a) Click +.
   b) Type a company directory group name. Click 🔍.
   c) Select the group. Click **Add**.
   d) Optionally, select **Link nested groups**.
   e) In the **Device activation** section, select whether you want onboarded users to receive an autogenerated activation password or no activation password. If you select the autogenerated password option, configure the activation period and select an activation email template.
6. To onboard users with BlackBerry Dynamics, select the **Onboard users with BlackBerry Dynamics apps only** check box.

7. Perform the following actions for each group that you want to onboard with activation for BlackBerry Dynamics apps only:
   a) Click +.
   b) Type a company directory group name. Click .
   c) Select the group. Click **Add**.
   d) Optionally, select **Link nested groups**.
   e) Select the number of access keys to generate per user added, the access key expiration, and the email template.
8. To delete device data when a user is offboarded, select the **Delete device data when the user is removed from all onboarding directory groups** check box. Select one of the following options:
   - Delete only work data
   - Delete all device data
   - Delete all device data for corporate owned/delete only work data for individually owed
9. To delete a user account from BlackBerry UEM when a user is removed from all onboarding groups, select **Delete user when the user is removed from all onboarding directory groups**. The first time that a synchronization cycle occurs after a user account is removed from all onboarding directory groups, the user account is deleted from BlackBerry UEM.
10. To prevent user accounts or device data from being deleted from BlackBerry UEM unexpectedly, select **Offboarding protection**.

    Offboarding protection means that users will not be deleted from BlackBerry UEM until two hours after the next synchronization cycle.
11. To force the synchronization of company directory groups, select the **Force synchronization** checkbox.

    If selected, when a group is removed from your company directory, the links to that group are removed from onboarding directory groups and directory-linked groups. If not selected, if a company directory group is not found, the synchronization process is canceled.
12. In the **Sync limit** field, type the maximum number of changes you want to allow for each synchronization process.The default setting is five.

    If the number of changes to be synchronized exceeds the synchronization limit, you can prevent the synchronization process from running. Changes are calculated by adding the following: users to add to groups, users to remove from groups, users to be onboarded, users to be offboarded.
13. In the **Maximum nesting level of directory groups** field, type the number of nested levels to synchronize for company directory groups.
14. Click **Save**.

Synchronize a company directory connection

Before you begin: Preview a synchronization report

1. On the menu bar, click **Settings > External integration > Company directory**.
2. In the **Sync** column, click .

After you finish: View a synchronization report

Preview a synchronization report

Previewing a synchronization report allows you to verify that the planned updates are what you expect before the synchronization occurs.

1. On the menu bar, click **Settings > External integration > Company directory**.
2. In the **Preview** column, click .
3. Click **Preview now**.
4. When the report finishes processing, click on the date in the **Last report** column.
5. To view synchronization reports that were generated previously, click on the drop-down menu.

View a synchronization report

1. On the menu bar, click **Settings > External integration > Company directory**.
2. In the **Last report** column, click the date.
3. To view synchronization reports that were generated previously, click on the drop-down menu.
4. To export a .csv file of the report, click .

Add a synchronization schedule

You can add a synchronization schedule to automatically synchronize BlackBerry UEM with your organization's company directory. There are three types of synchronization schedules:

- Interval: You specify the length of time between each synchronization, the time frame, and the days on which it will occur.
- Once a day: You specify the time of day that the synchronization starts and the days on which it will occur.
- No recurrence: You specify the time and day for a one time synchronization.

On the Company directory screen, you can manually synchronize BlackBerry UEM with company directory at any time.

1. On the menu bar, click **Settings > External integration > Company directory**.
2. Click the company directory name you want to edit.
3. On the **Sync schedule** tab, click +.
4. To reduce the amount of information that gets synchronized, in the **Synchronization type** drop-down list, choose one of the following options:
   - **All groups and users**: This is the default setting. If you choose this option users will be onboarded and offboarded and linked to the appropriate directory linked groups during the synchronization, users that are not onboarded or offboarded but change directory linked groups, and users with changes to their attributes will be synchronized.
   - **On-boarding group**s: If you choose this option users will be onboarded and offboarded and linked to the appropriate directory linked groups during the synchronization, and users with changes to their attributes will be synchronized. Users that are not onboarded or offboarded but change directory linked groups are not synchronized.
   - **Directory linked groups**: If you choose this option users will not be onboarded and offboarded during the synchronization. Users with changes to their directory linked groups will be linked appropriately. Users with changes to their attributes will be synchronized.
   - **User attributes**: If you choose this option users will not be onboarded and offboarded during the synchronization. Users with changes to their directory linked groups are not synchronized. Users with changes to their attributes will be synchronized.
5. In the **Recurrence** drop-down list, select one of the following options:

Option	Steps
Interval	**a.** In the **Interval** field, type the time, in minutes, between synchronizations. **b.** Specify the synchronization time frame. **c.** Select the days of the week when you want synchronizations to occur.
Once a day	**a.** Specify when you want the synchronization to start. **b.** Select the days of the week when you want the synchronizations to occur.
No recurrence	**a.** Specify when you want the synchronization to start. **b.** Select the day when you want the synchronization to occur.

6. Click **Add**.

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.

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

Note: 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 BlackBerry UEM. If you register a new APNs certificate, device users must reactivate their devices to receive data.

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

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

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

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

Obtain a signed CSR from BlackBerry

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

1. On the menu bar, click **Settings > External integration > Apple Push Notification**.
2. If you do not yet have an APNs certificate, in the **Step 1 of 3 - Download signed CSR certificate from BlackBerry** section, click **Download certificate**.

   If you want to renew the current APNs certificate, click **Renew certificate** instead.
3. Click **Save** to save the signed CSR file (.scsr) to your computer.

After you finish: Request an APNs certificate from Apple.

Request an APNs certificate from Apple

Before you begin: Obtain a signed CSR from BlackBerry.

1. On the menu bar, click **Settings > External integration > Apple Push Notification**.
2. In the **Step 2 of 3 - Request APNs certificate from Apple** section, click **Apple Push Certificate Portal**. You are directed to the Apple Push Certificates Portal.
3. Sign in to the Apple Push Certificates Portal using a valid Apple ID.
4. Follow the instructions to upload the signed CSR (.scsr). Note that if the following error displays: "You have uploaded an invalid file type. Supported file extensions are .txt, .rtf, .plist, .b64.", you can rename the .scsr file to a .txt file format, and upload the CSR again.
5. Download and save the APNs certificate (.pem) on your computer.
6. (Optional) Click to display a **Note** window.
7. In the **Note** window, type the Apple ID that you used to request the APNs certificate.

   You must use the same Apple ID to renew the certificate.
8. Click anywhere outside of the **Note** window to close it.

After you finish: Register the APNs certificate.

Register the APNs certificate

Before you begin: Request an APNs certificate from Apple.

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

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

Renew the APNs certificate

The APNs certificate is valid for one year. You must renew the APNs certificate each year before it expires. The certificate must be renewed using the same Apple ID that you used to obtain the original APNs certificate.

You can create an email event notification to remind you to renew the certificate 30 days before it expires.

Before you begin: Obtain a signed CSR from BlackBerry.

1. On the menu bar, click **Settings > External integration > Apple Push Notification**.
2. Click **Renew certificate**.
3. In the **Step 1 of 3 - Download signed CSR certificate from BlackBerry** section, click **Download certificate**.
4. Click **Save** to save the signed CSR file (.scsr) to your computer.
5. In the **Step 2 of 3 - Request APNs certificate from Apple** section, click **Apple Push Certificate Portal**. You are directed to the Apple Push Certificates Portal.
6. Sign in to the Apple Push Certificates Portal using the same Apple ID that you used to obtain the original APNs certificate.

7. Follow the instructions to renew the APNs certificate (.pem). You will need to upload the new signed CSR. Note that if the following error displays: "You have uploaded an invalid file type. Supported file extensions are .txt, .rtf, .plist, .b64.", you can rename the .scsr file to a .txt file format, and upload the CSR again.
8. Download and save the renewed APNs certificate on your computer.
9. In the **Step 3 of 3 - Register APNs certificate** section, click **Browse**. Navigate to and select the renewed APNs certificate.
10. Click **Submit**.

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

Troubleshooting APNs

This section helps you troubleshoot APNs issues.

The APNs certificate does not match the CSR. Provide the correct APNs file (.pem) or submit a new CSR.

Description

You may receive an error message when you try to register the APNs certificate if you did not upload the most recently signed CSR file from BlackBerry to the Apple Push Certificates Portal.

Possible solution

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.

I get "The system encountered an error" when I try to obtain a signed CSR

Description

When you try to obtain a signed CSR, you get the following error: "The system encountered an error. Try again."

Possible solution

Visit support.blackberry.com to read article 37266.

I cannot activate iOS or macOS devices

Possible cause

If you are unable to activate iOS or macOS devices, the APNs certificate may not be registered correctly.

Possible solution

Perform one or more of the following actions:

- In the administration 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.

Configuring BlackBerry UEM for DEP

You must configure BlackBerry UEM to use Apple's Device Enrollment Program before you can synchronize BlackBerry UEM with DEP. After you configure BlackBerry UEM, you can use the BlackBerry UEM management console to manage the activation of the iOS devices that your organization purchased for DEP.

You can use an Apple Business Manager account to synchronize BlackBerry UEM with DEP. Apple Business Manager is a web-based portal in which you can enroll and manage iOS devices in DEP, and manage Apple VPP accounts. If your organization uses DEP or VPP, you can upgrade to Apple Business Manager.

When you configure BlackBerry UEM for Apple's Device Enrollment Program, you perform the following actions:

Step	Action
1	Create a DEP account.
2	Download a public key.
3	Generate a server token.
4	Register the server token with BlackBerry UEM.
5	Add the first enrollment configuration.

Create a DEP account

1. On the menu bar, click **Settings > External integration > Apple Device Enrollment Program**.
2. In step **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.

After you finish: Download a public key.

Download a public key

Before you begin: Create a DEP account.

1. On the menu bar, click **Settings > External integration > Apple Device Enrollment Program**.
2. Click +.
3. In step **2 of 4: Download a public key**, click **Download public key**.
4. Click **Save**.

After you finish: Generate a server token.

Generate a server token

Before you begin: Download a public key.

1. On the menu bar, click **Settings > External integration > Apple Device Enrollment Program**.
2. Click +.
3. In step **3 of 4: Generate server token from Apple DEP account**, click **Open the Apple DEP portal**.
4. Sign in to your DEP account.
5. Follow the prompts to generate a server token.

After you finish: Register the server token with BlackBerry UEM.

Register the server token with BlackBerry UEM

BlackBerry UEM uses a server token for authentication when it communicates with Apple's Device Enrollment Program.

Before you begin: Generate a server token.

1. On the menu bar, click **Settings > External integration > Apple Device Enrollment Program**.
2. Click +.
3. In step **4 of 4: Register the server token with BlackBerry UEM**, click **Browse**.
4. Select the **.p7m** server token file.
5. Click **Open**.
6. Click **Next**.

After you finish: Add the first enrollment configuration.

Add the first enrollment configuration

Before you begin: Register the server token with BlackBerry UEM before you add your first enrollment configuration.

After you register a server token, BlackBerry UEM automatically displays the window where you add your first enrollment configuration.

1. Type a name for the configuration.
2. Complete one of the following tasks:
   - If you want BlackBerry UEM to automatically assign the enrollment configuration to devices when you register them in Apple's Device Enrollment Program, select the "Automatically assign all new devices to this configuration" checkbox.
   - If you want to use the BlackBerry UEM console to manually assign the enrollment configuration to specific devices, leave the "Automatically assign all new devices to this configuration" checkbox unchecked.
3. Optionally, type a department name and support phone number to be displayed on devices during setup.
4. In the **Device configuration** section, select from the following checkboxes:
   - Allow pairing - if selected, users can pair the device with a computer
   - Mandatory - if selected, users can activate devices using their company directory username and password
   - Allow removal of MDM profile - if selected, users can deactivate devices.

- Wait until device is configured - if selected, users cannot cancel the device setup until activation with BlackBerry UEM is completed.

5. In the **Skip during setup** section, select the items that you do not want to include in the device setup:
   - Passcode - if selected, users are not prompted to create a device passcode
   - Location services - if selected, location services are disabled on the device
   - Restore - if selected, users cannot restore data from a backup file
   - Move from Android - if selected, you cannot restore data from an Android device
   - Apple ID - if selected users are prevented from signing in to Apple ID and iCloud
   - Terms and conditions - if selected, users do not see the iOS terms and conditions
   - Siri - if selected, Siri is disabled on devices
   - Diagnostics - if selected, diagnostic information is not automatically sent from the device during setup
   - Biometric - if selected, users cannot setup Touch ID
   - Payment - if selected, users cannot set up Apple pay
   - Zoom - if selected, users cannot set up Zoom
   - Home button setup - if selected, users cannot adjust the Home button's click
   - Screen Time – if selected, the option to setup Screen Time is skipped during DEP enrollment
   - Software update – if selected, users do not see the mandatory software update screen on the device
   - iMessage and Face Time – if selected, users do not see the iMessage and Face Time screen on the device
   - Display tone – if selected, users do not see the Display tone screen on the device
   - Privacy – if selected, users do not see the Privacy screen on the device
   - Onboarding – if selected, users do not see the informational onboarding screen on the device
   - Watch migration – if selected, users do not see the watch migration screen on the device
   - SIM setup – if selected, users do not see the screen to set up a cellular plan on the device
   - Device-to-device migration – if selected, users do not see the device-to-device migration screen on the device
6. Click **Save**.

   If the message "An error was encountered. The server token file could not be decrypted." appears, visit support.blackberry.com/community to read article 37282.
7. 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 the Administration content.

Update the server token

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.

Before you begin: If the public key has changed, Download a new public key.

1. On the menu bar, click **Settings > External integration > Apple Device Enrollment Program**.
2. Click the name of a DEP account.
3. In the **Expiry date** section, click **Update server token**.
4. In **Step 1 of 2: Generate a Server Token from Apple DEP account**, click **Open the Apple DEP portal**.
5. Sign in to your account for DEP.
6. Follow the prompts to generate a server token.
7. In step **2 of 2: Register the Server Token with BlackBerry UEM**, click **Browse**.
8. Select the **.p7m** server token file.

9. Click **Open**.
10. Click **Save**.

Remove a DEP connection

CAUTION: If you remove all DEP connections, you cannot activate new iOS devices in Apple's Device Enrollment Program. If you assigned enrollment configurations to devices and the configurations have not been applied, BlackBerry UEM removes the enrollment configurations assigned to the devices. Removing the connection does not affect devices that are active on BlackBerry UEM.

If your organization no longer deploys iOS devices that use DEP, you can remove the BlackBerry UEM connections to DEP.

1. On the menu bar, click **Settings > External integration > Apple Device Enrollment Program**.
2. Click **Remove DEP connection**.
3. Click **Remove**.
4. Click **OK**.

Configuring BlackBerry UEM to support Android Enterprise devices

Android Enterprise devices provide additional security for organizations that want to manage Android devices. For more information about Android Enterprise devices, visit https://support.google.com/work/android/.

For detailed instructions on configuring BlackBerry UEM to support Android Enterprise devices, visit support.blackberry.com/community to read article 37748.

There are two ways to configure BlackBerry UEM to support Android Enterprise devices:

1. Connect BlackBerry UEM to a Google Cloud or G Suite domain.

   Note: You can connect only one BlackBerry UEM domain to a Google domain.
2. Allow BlackBerry UEM to manage Android Enterprise devices that have managed Google Play accounts. You don't need to have a Google domain to use this option. For more information, see https://support.google.com/googleplay/work/.

The following table summarizes the different options for configuring Android Enterprise devices:

Method to configure BlackBerry UEM to support Android Enterprise devices	When to choose this method	User account type	Supported Google services
Connect BlackBerry UEM to your G Suite domain	You have a G Suite domain in your organization	G Suite accounts (for organizations)	Supports all G Suite services such as Gmail, Google Calendar, and Drive. Supports app management through Google Play.
Connect BlackBerry UEM to your Google Cloud domain	You have a Google Cloud domain in your organization	Google Cloud accounts, also known as Managed Google accounts (for organizations)	Similar to G Suite but without access to paid products such as Gmail, Google Calendar, and Drive. Supports app management through Google Play.

Method to configure BlackBerry UEM to support Android Enterprise devices	When to choose this method	User account type	Supported Google services
Allow BlackBerry UEM to manage Android Enterprise devices as managed Google Play accounts	You don't have a Google domain in your organization or You have a Google domain that is already connected to one BlackBerry UEM domain and you want to use Android Enterprise devices on a second BlackBerry UEM domain	Android Enterprise devices that have managed Google Play accounts	Supports app management through Google Play. Google Services are not supported.

For information about configuring BlackBerry UEM and Chrome OS support, refer to Extending the management of Chrome OS devices to BlackBerry UEM.

Configure BlackBerry UEM to support Android Enterprise devices

You can connect only one BlackBerry UEM domain to your Google domain. Before you connect another BlackBerry UEM domain, you must remove the existing connection. See Remove the connection to your Google domain.

1. On the menu bar, click **Settings > External integration > Android enterprise**.
2. Perform one of the following tasks:

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 **Bring Android to Work** window, sign in using a Google account. You can use any Google or Gmail account. The account that you use will become the administrator account for the **Bring Android to Work** service. d. Click **Get Started**. e. Type the name of your organization. Click **Confirm**. f. Click **Complete registration**. You will be returned to the BlackBerry UEM management console.
Use a Google domain	a. Select **Connect BlackBerry UEM to your existing Google domain**. Note that you cannot share Google domains between multiple BlackBerry 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**. For step-by-step instructions, visit support.blackberry.com/community to read article 37748.

3. Specify how you want app configurations to be sent to a device. Any information that you added in the app configuration can be either provided using the BlackBerry Infrastructure or provided using the Google infrastructure. Do one of the following:
   - Select **Send app configuration using UEM Client** to send app configuration details using the BlackBerry Infrastructure.
   - Select **Send app configuration using Google Play** to send app configurations details using the Google infrastructure.
4. When you are prompted, click **Accept** to accept the permissions set for some or all of the following apps:
   - Google Chrome
   - BlackBerry Connectivity
   - BlackBerry Hub+ Services
   - BlackBerry Hub
   - BlackBerry Calendar
   - Contacts by BlackBerry
   - Notes by BlackBerry
   - Tasks by BlackBerry
5. Click **Done**.

After you finish: Complete the steps to activate Android Enterprise devices. For more information about device activation, see "Device activation" in the Administration content.

Remove the connection to your Google domain

You can connect only one BlackBerry UEM domain to your Google Cloud or G Suite domain. Before you connect another BlackBerry UEM domain, you must remove the existing connection.

Remove the connection to your Google domain before you complete any of the following tasks:

- Decommission a BlackBerry UEM domain
- Connect another BlackBerry UEM instance to your Google Cloud or G Suite domain

If you do not remove the connection to your Google domain, you may be unable to connect your Google Cloud or G Suite domain to a new BlackBerry UEM instance. If you remove the connection in BlackBerry UEM, all devices that are activated with an Android Enterprise activation type will be deactivated.

1. On the menu bar, click **Settings > External integration**.
2. Click **Google domain connection**.
3. Click **Remove connection**.
4. Click **Remove**.

Remove the Google domain connection using your Google account

If you configured BlackBerry UEM to support Android Enterprise devices, you can remove the connection in Google.

1. Using the Google account that you used to set up Android Enterprise devices, log in to https://play.google.com/work.
2. Click **Admin Settings**.
3. In the **Organization information** section, click ⋮.

4. Click **Delete Organization**.
5. Click **Delete**.
6. In the BlackBerry UEM console, on the menu bar, click **Settings > External integration**.
7. Click **Google domain connection**.
8. Click **Test connection**.
9. Click **Remove connection**.
10. Click **Remove**.

Edit or test the Google domain connection

You can edit the Google domain connection in BlackBerry UEM to change the type of Google domain that you use to manage Android Enterprise devices, or to test the Google domain connection. When you edit or test the connection, devices that are already activated are not affected.

1. On the menu bar, click **Settings > External integration**.
2. Click **Google domain connection**.
3. Click .
4. Complete one of the following tasks:
   - Click **Test connection** to see the current status of the connection.
   - Select the type of domain to manage Android Enterprise devices and click **Save**.

Extending the management of Chrome OS devices to BlackBerry UEM

Chrome OS support with BlackBerry UEM requires a Google managed domain. Enrollment and some management of Chrome OS devices continues to be done through the Google managed domain console. The Chrome OS integration with BlackBerry UEM extends the management of some of the Chrome OS management functionality to UEM.

In the Google Admin console, users and devices are organized into Org units, which are a hierarchical representation of groups of users, devices, and settings. BlackBerry UEM synchronizes these org units from the Google admin console into UEM Org unit groups. For more information about organizational units, see the information from Google.

After the synchronization between Google and BlackBerry UEM is complete, UEM registers with the Google domain for notifications of changes to org units, users, or devices. Then if, for example, a device is enrolled, a user's name changes, or an org unit is moved, UEM is notified immediately and updates the database accordingly.

If your organization's UEM environment is already configured for Android Enterprise, you can add another connection that you can use to manage your Chrome OS devices.

For more information visit support.blackberry.com to read article 98789.

Note: Your Google managed domain must include "Chrome Enterprise Upgrade".

Setting up management of Chrome OS devices if you have already configured BlackBerry UEM to use Android Enterprise

If you already use Android Enterprise, you need only to perform these steps to prepare to manage Chrome OS devices in BlackBerry UEM:

- Ensure your organization's Google Domain has Chrome OS enterprise enabled
- Ensure the Chrome Policy API is enabled in your organization's Google Domain, for more information see Create a service account that BlackBerry UEM uses to authenticate with your Google Cloud or Google Workspace by Google domain
- Ensure all the scopes are added, for more information see Enable additional APIs to allow BlackBerry UEM to sync the Chrome OS data
- Enable Chrome OS management in BlackBerry UEM console, see Synchronize BlackBerry UEM with the Google admin console

Create a service account that BlackBerry UEM uses to authenticate with your Google Cloud or Google Workspace by 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 using the Google account that you want to use to manage your project.
2. Click **Create Project**.
3. Type a name for the project.
4. Click **Create**.

5. After your project has been created, click on it and in the left pane, expand **IAM & Admin** and click **Service Accounts**.
6. Click **Create Service Account**.
7. Type a name for the service account and click **Create and Continue**.
8. In the **Role** list, select **Basic > Editor.**
9. Click **Continue**.
10. Click **Done**.
11. Select your service account.
12. Click the **Keys** tab.
13. Click **Add key > Create new key > P12 > Create**.
14. Copy the private key password, you will use it later.
15. You might be prompted to download the certificate, or it will be automatically downloaded. Locate and save it in a known folder.
16. Click **Close**.
17. Click ☰ > **Service Accounts**.
18. In the **Actions** column, click > ⋮ **Manage details**.
19. Copy the **Unique Client ID** and **Email Address** for the service account. Paste these in the same text file where you stored the private key password to use later in the process.
20. Click ☰ > **APIs & Services > Enabled APIs and Services**.
21. Click **Enable APIs and services**.
22. Search for and select **Admin SDK API**.
23. Click **Enable**.
24. Search for and select **Google Play EMM API**.
25. Click **Enable**.
26. Search for and select **Chrome Policy API**.
27. Click **Enable**.

Enable additional APIs to allow BlackBerry UEM to sync the Chrome OS data

You must use your organization's Google admin console to enable additional APIs which will allow UEM to synchronize the Chrome OS data.

1. Log in to the Google admin console using the administrator account for your Google domain.
2. Navigate to **Home > Devices > Mobile & endpoints > Settings > Third-party Integrations**.
3. Click **Android EMM** and ensure that **Enable third-party Android mobile management** is selected.
4. Click **Add EMM providers > Generate Token**.
5. Copy the token. Paste this in the same text file where you pasted the private key password.
6. Close the Token Windows and click **Save**.
7. Click **Save anyway**.
8. Click **Security > Access and data control > API controls**.
9. Under **Domain-wide delegation**, click **MANAGE DOMAIN-WIDE DELEGATION**.
10. Click **Add New** (near API Clients).

11. In the **Client ID** field, paste the Google service account Unique Client ID that you recorded earlier, and enter the following addresses in the OAuth scopes field, 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/admin.directory.user
    - https://www.googleapis.com/auth/chrome.management.policy
    - https://www.googleapis.com/auth/admin.reports.audit.readonly
12. Click **Authorize**.
    Note: Authorizing this API for the service account lets UEM access the user directory for your Google Cloud or Google Workspace by Google domain.

Integrate BlackBerry UEM with your Google Cloud or Google Workspace by Google domain so you can use Chrome OS devices

1. Log in to the UEM management console using a Security Administrator account.
2. On the menu bar, click **Settings > External integration > Android Enterprise**.
3. Select **Connect BlackBerry UEM to your existing Google domain**. Note that you cannot share Google domains between multiple BlackBerry UEM domains. This option supports Android Enterprise and Chrome OS Enterprise.
4. In the How app configurations are sent section, select **Send app configuration using Google Play**.
5. Click **Next**.
6. In the **Private key password** field, paste the private key password that you copied from the Google Developers Console.
7. Beside the **P12 certificate file** field, click **Browse**.
8. Navigate to the certificate file that was received from the Google Developers Console, and click **Open**.
9. In the **Service account email address** field, paste the Google service account email address that you copied from the Google Developers Console.
10. In the **Email address for Google domain administrator** field, type the email address of the administrator account used to manage the Google Cloud or Google Workspace by Google domain.
11. In the **Token** field, paste the token that you generated in the Google domain.
12. In the **Select the type of domain to manage the Android devices with a work profile** section, select if you have a Google Cloud domain or Google Workspace by Google domain.
13. If you select a 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**.

Synchronize BlackBerry UEM with the Google admin console

After you have synchronized BlackBerry UEM with your Google domain, you can perform some management actions on your organizations Chrome OS devices such as enable, disable, and unmanage.

1. Log in to the UEM management console using a Security Administrator account.
2. On the menu bar, click **Settings > External integration > Android Enterprise**.
3. In the Chrome OS Management section, click **Enable**. This button performs an initial sync of data within 10 minutes and also schedules regular synchronizations.
   Note: After the synchronization is complete, you can use the **Sync Org Units, Sync users**, and **Sync devices** buttons to perform out of schedule synchronizations.

Simplifying Windows 10 activations

You can use a Java web application from BlackBerry as a discovery service to simplify the activation process for users with Windows 10 devices. If you use the discovery service, users don't need to type a server address during the activation process. If you choose not to deploy this web application, users can still activate Windows 10 devices by typing the server address when prompted.

You can use different operating systems and web application tools to deploy a discovery service web application. This topic describes the high-level steps. See Deploy a discovery service to simplify Windows 10 activations for an example of the specific steps you would take using common operating systems and tools.

When you deploy a discovery service web application, you perform the following actions:

Step	Action
1	Create a static DNS Host A record for the Java application server. The record must specify `enterpriseenrollment.<email_domain>`, where <*email_domain*> corresponds to the email addresses of your users.
2	If you want to allow users to activate devices while they are outside of your organization's network, configure the computer that hosts the discovery service to listen externally on port 443.
3	Create and install a certificate to secure TLS connections between Windows 10 devices and the discovery service.
4	Log into *my*Account to download the Auto Discovery Proxy Tool. Run the file to extract a .war file and deploy it to the root of your Java application server.
5	Update the wdp.properties file of the discovery service web application to include a list of your organization's SRP IDs.

Integrating UEM with Azure Active Directory join

You can integrate BlackBerry UEM with Azure Active Directory join for a simplified enrollment process for Windows 10 devices. When it's configured, users can enroll their devices with UEM using their Azure Active Directory username and password. Azure Active Directory 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.

To integrate Azure Active Directory join with UEM, you do the following:

Step	Description
1	Use the value of the %ClientlessActivationURL% default variable in UEM to determine the following URLs so that you can integrate UEM with Azure Active Directory join. For example, in the user details screen of a user that uses the default activation email template, you can click **View activation email** to find the value of %ClientlessActivationURL% in the Windows 10 server name field. 1. Determine the MDM terms of use URL. The URL uses the following structure: *%ClientlessActivationURL%*/azure/termsofuse For example, if the %ClientlessActivationURL% variable resolves to `https://enrol.example.net/S123456789/win/mdm`, then use `https://enrol.example.net/S123456789/win/mdm/azure/termsofuse`. 2. Determine the MDM discovery URL. The URL uses the following structure: *%ClientlessActivationURL%*/azure/discovery For example, if the %ClientlessActivationURL% variable resolves to `https://enrol.example.net/S123456789/win/mdm`, then use `https://enrol.example.net/S123456789/win/mdm/azure/discovery`. 3. Determine the App ID URI using only the host name of the %ClientlessActivationURL% default variable. For example, if the %ClientlessActivationURL% variable resolves to `https://enrol.example.net/S123456789/win/mdm`, then use `https://enrol.example.net`.
2	Integrate UEM with Azure Active Directory join.

Integrate UEM with Azure Active Directory join

Before you begin: Determine the MDM terms of use URL, MDM discovery URL, and App ID URI. For more information, see Integrating UEM with Azure Active Directory join.

1. Sign in to the Microsoft Azure management portal at https://portal.azure.com.
2. Navigate to **Mobility (MDM and MAM)**.
3. Click **Add application**.
4. Click **On-premise MDM application**. Enter a friendly name (for example, `BlackBerry UEM`).
5. Click **Add**.
6. Click on the application that you added in the previous step to configure its settings.
7. Specify the user scope, **Some** or **All**. If applicable, select the groups.
8. In the **MDM terms of use URL** field, specify the URL.
9. In the **MDM discovery URL** field, specify the URL.
10. Click **Save**.
11. Click **On-premises MDM application settings > Properties**.
12. In the **App ID URI** field, specify the URL.
13. Click **Save**.

Configuring Windows Autopilot in Microsoft Azure

To support Windows Autopilot device activation, you do the following:

Step	Description
1	Integrate UEM with Azure Active Directory join.
2	Create a Windows Autopilot deployment profile in Azure and assign it to user groups in Azure.
3	Import Windows Autopilot devices to Azure.

Create a Windows Autopilot deployment profile in Azure

You must assign a Windows Autopilot deployment profile to the appropriate user groups in Azure to allow users to activate their device using Windows Autopilot.

1. Sign in to the Microsoft Azure management portal at https://portal.azure.com.
2. Navigate to **Device enrollment > Windows enrollment > Windows Autopilot deployment profiles**.
3. Create a Windows Autopilot deployment profile.
4. Enter a name and description for the profile.
5. Configure the out-of-box experience settings.
6. Assign the profile to the appropriate user groups.
7. Click **Save**.

Import Windows Autopilot devices to Azure

Complete these steps to import each Windows 10 device that you want to allow to be activated with Windows Autopilot.

1. Turn on the Windows 10 device to load the device out-of-the-box setup.
2. Connect to a Wi-Fi network with an internet connection.
3. On the keyboard, press **CTRL + SHIFT + F3** or **CTRL+Fn+SHIFT+F3**. The device restarts and enters audit mode.
4. Run **Windows PowerShell** as an administrator.
5. Run `Save-Script -Name Get-WindowsAutoPilotInfo -Path C:\Windows\Temp` to inspect the Windows PowerShell script.
6. Run `Install-Script -Name Get-WindowsAutoPilotInfo` to install the script.
7. Run `Get-WindowsAutoPilotInfo.ps1 -OutputFile C:\Windows\Temp\MyComputer.csv` to save the device information to a .csv file.
8. To import the .csv file into Microsoft Azure, perform the following actions:
   a) In the Azure portal, navigate to **Device enrollment > Windows enrollment > Windows Autopilot devices**.
   b) Click **Import**.
   c) Select the .csv file.
9. In the **System Preparation Tool** dialog, do the following:

a) In the **System Cleanup Action** field, select **Enter System Out-of-Box Experience (OOBE)** and deselect **Generalize**.
b) In the **Shutdown Options** field, select **Reboot**.

Deploy a discovery service to simplify Windows 10 activations

The following steps describe how to deploy the discovery service web application in the environment described below.

Before you begin: Verify that the following software is installed and running in your environment:

- Windows Server 2012 R2
- Java JRE 1.8 or later
- Apache Tomcat 8 Version 8.0 or later

1. Configure a static IP address for the computer that will host the discovery service.

   Note: If you want to allow users to activate devices when they are outside of your organization's network, the IP address must be externally accessible on port 443.
2. Create a DNS Host A record for the name **enterpriseenrollment.<*email_domain*>** that points to the static IP address that you configured in Step 1.
3. In the directory where you installed Apache Tomcat, search the server.xml file for **8080** and apply comment tags as shown in the example below:

```
<!--
    <Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
    -->
```

4. Search **server.xml** and change all instances of **8443** to **443**.
5. Search for the **<Connector port="443"** section, remove the comment tags above and below, and modify it as shown in the example below:

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS" keystoreFile="C:\Users\<account _name>
\.keystore" />
```

6. While logged in as the account you specified in the example above, generate a certificate by running the two commands shown in the example below. When asked for your first and last name, type `enterpriseenrollment.<email _domain>` as shown in the step result below:

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -genkey -alias tomcat -
keyalg RSA -keysize 2048
```

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin> keytool -certreq -alias tomcat -
keyalg RSA -file <filename>.csr
```

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -genkey -alias tomcat -
keyalg RSA -keysize 2048 Enter keystore password: changeit
    What is your first and last name?
      [Unknown]:  enterpriseenrollment.example.com
    What is the name of your organizational unit?
```

```
      [Unknown]:  IT Department
    What is the name of your organization?
      [Unknown]:  Manufacturing Co.
    What is the name of your City or Locality?
      [Unknown]:  Waterloo
    What is the name of your State or Province?
      [Unknown]:  Ontario
    What is the two-letter country code for this unit?
      [Unknown]:  CA
    Is CN=enterpriseenrollment.example.com, OU=Business Unit, O=Example
Company, L=Waterloo, ST=Ontario, C=CA correct?
     [no]:  yes

   C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -certreq -alias tomcat
-keyalg RSA -file <enterpriseenrollment.example.com>.csr
   Enter key password for <enterpriseenrollment.example.com>
           (RETURN if same as keystore password):
```

7. Send the certificate signing request to a certification authority. The certification authority will send back a .p7b file. For the example above, the certification authority would return the file `enterpriseenrollment.example.com.p7b`.
   - If you send the certificate signing request to a major external certification authority, users should not have to take any additional action to trust this certificate during the activation process.
   - If you send the certificate signing request to an internal certification authority, users must install the CA certificate on the device before starting the activation process.
8. Install the certificate using the command shown in the example below:

```
C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -import -trustcacerts -
alias tomcat -file <filename>.p7b
```

9. Stop Apache Tomcat.
10. Visit myAccount to download the Auto Discovery Proxy Tool. Extract the contents of the .zip file and run **W10AutoDiscovery-<*version*>.exe**.
    The .exe file will extract the file `W10AutoDiscovery-<version>.war` to `C:\BlackBerry`.
11. In the directory where you installed Apache Tomcat, check for the folder `\webapps\ROOT`. If it already exists, delete the `\ROOT` folder.
12. Rename `W10AutoDiscovery-<version>.war` as `ROOT.war`. Move it to the folder `\webapps` in the directory where you installed Apache Tomcat.
13. Start Apache Tomcat.
    Apache Tomcat will deploy the new webapp and create a `\webapp\ROOT folder`.
14. Run notepad.exe as an administrator. In the directory where you installed Apache Tomcat, open `\webapps\ROOT\WEB-INF\classes\config\wdp.properties`.
15. Add the Host ID for your BlackBerry UEM domain to the line `wdp.whitelisted.srpid` as shown in the example below. You can find the Host ID for your BlackBerry UEM domain in the BlackBerry UEM management console. If you have multiple BlackBerry UEM domains, specify the Host ID for each one. Perform the following actions:
    a) On the menu bar, click **Settings > Licensing > Licensing summary**.
    b) Click **Activate licenses**.
    c) In the **Licensing activation method** drop-down list, click **Host ID**.

```
wdp.whitelisted.srpid=<Host ID>, <Host ID>, <Host ID>
```

16. Restart Apache Tomcat.

Configuring BlackBerry UEM Cloud to support BlackBerry Dynamics apps

Follow the instructions in this section to configure BlackBerry UEM Cloud to support BlackBerry Dynamics apps.

For information on managing BlackBerry Dynamics apps on users devices, see "Managing BlackBerry Dynamics apps" in the administration content.

Manage BlackBerry Proxy clusters

When you install the first instance of BlackBerry Connectivity Node, 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 default; the new BlackBerry Connectivity Node instances are considered to be 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**.
2. Click **Clusters**.
3. 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 **Save**.
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 **Settings > BlackBerry Dynamics > Clusters** **b.** Click the cluster name. **c.** Click **Override global settings** See Configure BlackBerry Dynamics app proxy settings for the BlackBerry Cloud Connector for more information.
Download PAC file updates for all clusters	• Click **Refresh PAC cache**

Task	Steps
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.** Select the certificate file that you want to use. **f.** Click **Open**. **g.** Type a description for the certificate. **h.** Click **Add**.

Configure Direct Connect using port forwarding

Before you begin:

- Configure a public DNS entry for each BlackBerry Connectivity Node server (for example, bp01.mydomain.com, bp02.mydomain.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**.
2. Click **Direct Connect**.
3. Click a BlackBerry Proxy instance.
4. 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.
5. Repeat steps 3 and 4 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.
6. Click **Save**.

Connecting BlackBerry Proxy to the BlackBerry Dynamics NOC

If you plan to use BlackBerry Proxy to allow BlackBerry Dynamics apps to connect to your organization's resources, your organization's firewall must allow TCP connections to the following IP ranges so that BlackBerry Proxy can connect to the BlackBerry Dynamics NOC:

- 206.124.114.1 to 206.124.114.254 (206.124.114.0/24) on port 443
- 206.124.121.1 to 206.124.121.254 (206.124.121.0/24) on port 443
- 206.124.122.1 to 206.124.122.254 (206.124.122.0/24) on port 443

Alternatively, you can configure your organization's firewall to allow connections to the following host names:

- gdentgw.good.com on port 443
- gdrelay.good.com on port 443
- gdweb.good.com on port 443
- gdmdc.good.com on port 443

Connect BlackBerry UEM to a BlackBerry Dynamics PKI connector

If you want to use your organization's PKI software to enroll certificates for BlackBerry Dynamics apps, and your PKI software isn't supported for a direct connection with BlackBerry UEM, you can set up a BlackBerry Dynamics PKI connector to communicate with your CA and link BlackBerry UEM to the PKI connector.

Note: In a BlackBerry UEM Cloud environment, you must have a BlackBerry Connectivity Node installed to allow BlackBerry UEM to communicate with the PKI connector through the BlackBerry Cloud Connector.

A PKI connector is a set of Java programs and web services on a back-end server that allows BlackBerry UEM to send certificate requests and receive responses from the CA. BlackBerry UEM uses the BlackBerry Dynamics user certificate management protocol to communicate with the PKI connector. This protocol runs over HTTPS and defines JSON-formatted messages. For more information on setting up a BlackBerry Dynamics PKI connector, see the User Certificate Management Protocol and PKI Connector documentation.

Before you begin: Set up a BlackBerry Dynamics PKI connector.

1. On the menu bar, click **Settings > External integration > Certificate authority**.
2. Click **Add a BlackBerry Dynamics PKI connection**.
3. In the **Connection name** field, type a name for the connection.
4. In the **URL** field, type the URL of the PKI connector.
5. Select one of the following options:
   - **Authenticate with username and password**: Choose this option if BlackBerry UEM authenticates with the BlackBerry Dynamics PKI Connector using password-based authentication.
   - **Authenticate with client certificate**: Choose this option if BlackBerry UEM authenticates with the BlackBerry Dynamics PKI Connector using certificate-based authentication.
6. If you selected **Authenticate with username and password**, in the **Username** and **Password** fields, type the username and password for the BlackBerry Dynamics PKI connector.
7. If you selected **Authenticate with client certificate**, click **Browse** to select and upload a certificate that is trusted by the BlackBerry Dynamics PKI Connector. In the **Client certificate password** field, type the password for the certificate.
8. In the **Trusted certificate for the PKI connector** section you can specify the certificate that BlackBerry UEM uses to trust connections to the PKI connector, select one of the following options:
   - **CA certificate from BlackBerry Control TrustStore**
   - **CA certificate**: If you select this option you must click Browse to navigate to and select your organization's CA certificate.
   - **PKI connector server certificate**: If you select this option you must click Browse to navigate to and select your organization's PKI connector server certificate.
9. To test the connection, click **Test connection**.
10. Click **Save**.

After you finish:

- Create a user credential profile to send certificates from your PKI software to devices.

Overriding global HTTP proxy settings for a BlackBerry Connectivity Node

If you have the BlackBerry Connectivity Node installed, you can override global BlackBerry UEM Cloud proxy settings 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 and 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 BlackBerry UEM proxy settings. For more information, see the BlackBerry Access Administration Guide.

PAC file considerations

You should be aware of the following support considerations if you are using PAC files with BlackBerry Proxy.

BlackBerry UEM supports the following PAC file directives:

- DIRECT
- PROXY (treated as HTTPS proxy - connection established using HTTP CONNECT)
- HTTPS (connection established using HTTP CONNECT)

BlackBerry UEM doesn't support the following PAC file directives:

- BLOCK (treated as DIRECT)
- SOCKS (connection error will occur)
- SOCKS4 (connection error will occur)
- SOCKS5 (connection error will occur)
- HTTP (connection error will occur)
- Custom "NATIVE" directive defined by BlackBerry Access (connection error will occur)

BlackBerry UEM has the following additional limitations for PAC files:

- 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.

Note:

BlackBerry Proxy downloads and caches the PAC file to improve performance. The PAC cache is updated every 24 hours.

If a new PAC file is published and you need to update the cache immediately, you can navigate to **Settings > Infrastructure > BlackBerry Router and Proxy,** expand the **Global settings** section, and click **Update PAC cache**.

Configure BlackBerry Dynamics app proxy settings for the BlackBerry Cloud Connector

You can configure BlackBerry Cloud Connector proxy settings for BlackBerry Dynamics apps manually or using a PAC file.

1. In the BlackBerry Cloud Connector, click **General settings > BlackBerry Router and proxy**.
2. Select **Global settings**.
3. Select one of the following options.

- **Enable manual HTTP proxy**
- **Enable PAC**

PAC files are supported only for connections to application servers. If you configure both options, the PAC configuration takes precedence for connections to application servers. PAC files are supported only for apps developed with BlackBerry Dynamics SDK 7.0 and later.

4. If you selected **Enable manual HTTP proxy**, perform the following steps:
   a) Select one of the following options.
      - **Use proxy to connect only to BlackBerry Dynamics NOC servers**
      - **Use proxy to connect to all servers**
      - **Use proxy to connect only to specified servers**
   b) If you want to use the proxy to connect to specified servers, click + to specify any additional servers.
   c) In the **Address** field, type the address for the proxy server.
   d) In the **Port** field, type the port number that the proxy server listens on.
   e) If the proxy server requires authentication, select **Use authentication** and specify the **Username**, **Password**, and, if necessary, **Domain** that the app should use for authentication.
5. If you selected **Enable PAC**, perform the following steps:
   a) In the **PAC URL** field, type the URL for the PAC file.
   b) If the proxies specified in the PAC file require authentication, select **Support proxy authentication** and specify the **Username**, **Password**, and, if necessary, **Domain** that the app should use for authentication.

   End-user authentication credentials aren't supported for proxy authentication.
6. Click **Save**.

Configure email notifications for BlackBerry Work

BEMS Cloud accepts push registration requests from devices, such as iOS and Android, and then communicates with the on-premises Microsoft Exchange Server or Microsoft Office 365 server to check the user's mailbox for changes. When you specify the on-premises Microsoft Exchange Server or Microsoft Office 365 server information, you specify the settings to create the BEMS Cloud tenant for your organization.

When the tenant is created, the following services are automatically enabled:

- BlackBerry Directory Lookup: This service allows users to look up other users by first name, last name, and associated photo or avatar from the company directory.
- BlackBerry Follow-Me: This feature supports the BlackBerry Dynamics Launcher on BlackBerry Work.

A hybrid modern authentication environment (for example, on-premises Microsoft Exchange Server and Microsoft Office 365), allows the on-premises Microsoft Exchange Server to use a more secure user authentication and authorization by consuming OAuth access tokens obtained from the cloud. For more information on how to configure an on-premises Microsoft Exchange Server to use hybrid modern authentication, visit https://docs.microsoft.com/en-us/microsoft-365/enterprise/configure-exchange-server-for-hybrid-modern-authentication?view=o365-worldwide.

Before you begin: Verify that you have the following information and completed the appropriate tasks.

- Verify that the service account has application impersonation permissions applied.
- If you have a hybrid Microsoft Office 365 and on-premises Microsoft Exchange Server environment, and you enable Modern Authentication, make sure that the on-premises Microsoft Exchange Server is configured to use hybrid modern authentication. For more information, visit https://docs.microsoft.com/en-us/microsoft-365/enterprise/configure-exchange-server-for-hybrid-modern-authentication?view=o365-

worldwide. If the Microsoft Exchange Server is not configured appropriately, users won't receive email notifications.

- In a Microsoft Office 365 environment, if you plan to enable modern authentication, verify that you completed the following:
  - If you enable modern authentication using credential authentication, obtain the client application ID.
  - If you enable modern authentication using client-certificate authentication, do one of the following:
    - Obtain the client application ID with certificate-based authentication
    - Create and associate a self-signed .pfx certificate to the Azure app ID for BEMS
  - If you have configured Azure AD conditional access for your organization, make sure that the BlackBerry Connectivity Node is installed and configured in your environment.
  - Configure email notifications for BlackBerry Work
  - In an on-premises Microsoft Exchange environment, make sure that the Microsoft Exchange Server is updated to support TLS 1.2 or push notifications will fail. Weaker cipher suites such as TLSv1 or TLS 1.0 are disabled by default. Disabling the cipher suites provides enhanced security.
- If you use Passive Authentication, verify that you have the App ID for BEMS using credential authentication.
- If you use SSL for SCP lookup, verify that you exported the Microsoft Active Directory SSL certificate.

1. In the management console, click **Settings > BlackBerry Dynamics > Email notifications**.
2. In the **Authentication type** section, select an authentication type based on your environment and complete the associated tasks to allow BEMS to communicate with the Microsoft Exchange Server or Microsoft Office 365:

Authentication type	Description	Task
Credential	This option uses a defined BEMS username and password to authenticate to the Microsoft Exchange Server or Microsoft Office 365 using Basic Authentication.	**a.** In the **Service account username** field, enter the username of the BEMS service account. • For Microsoft Office 365, enter the service account's User Principal Name (UPN). • For on-premises Microsoft Exchange Server, use the format <*domain*>\<*username*>. **b.** In the **Service account password** field, enter the password for the service account.
Client Certificate	This option uses a client certificate to allow the BEMS service account to authenticate to the Microsoft Exchange Server or Microsoft Office 365.	**a.** Beside the **Certificate file (.pfx)** field, click **Browse**. Navigate to and select the client certificate file. **b.** In the **Password** field, enter the password for the client certificate.

Authentication type	Description	Task
Passive authentication	This option uses an identity provider (IDP) to authenticate the user and provide BEMS with OAuth tokens to authenticate to Microsoft Office 365. In a hybrid environment, authenticates to on-premises Microsoft Exchange Server*.	**a.** In the **Authentication Authority** field, enter the Authentication Server URL that BEMS accesses and retrieves the OAuth token for authentication with Microsoft Office 365 (for example, https://login.microsoftonline.com/common). **b.** In the **Client Application ID** field, enter the Azure app ID for the credential authentication. For instructions, see the App ID for BEMS using credential authentication. **c.** In the **Server Name** field, enter the FQDN of the Microsoft Office 365 server. By default, the the server name is https://outlook.office365.com. **d.** The **Redirect URI** field displays the URL that the IDP redirects the administrator to when the client app ID is authorized and the authentication tokens are provided. This field is prepopulated with the partition information and can't be modified. **e.** Click **Login**. **f.** Enter the credentials for the service account. **g.** Click **OK** to acknowledge that the authentication tokens were obtained. **h.** Important: BEMS Cloud doesn't automatically refresh the OAuth tokens. Repeat steps e to g to refresh the OAuth tokens. The tokens expiration time depends on your tenant policy (by default, the token expiration is 90 days). When the OAuth tokens expire, email notifications on the users' devices stop. The OAuth token expiration is displayed after you login to the IDP.

* The Microsoft Exchange Server on-premises must be configured to use hybrid modern authentication. For more information, visit https://docs.microsoft.com/en-us/microsoft-365/enterprise/configure-exchange-server-for-hybrid-modern-authentication?view=o365-worldwide.

3. If you connect to a Microsoft Office 365 environment, do the following to enable modern authentication:
   a) Select the **Enable Modern Authentication** check box.
   b) In the **Authentication authority** field, enter the Authentication Server URL that BEMS accesses to retrieve the OAuth token for authentication with Microsoft Office 365 (for example, https://login.microsoftonline.com/<*tenantname*> or or https://login.microsoftonline.com/<*tenantid*>).
   c) In the **Client application ID** field, enter one of the following Azure app IDs depending on the authentication type you selected. Do one of the following to obtain an Azure app ID:
      - Obtain an Azure app ID for BEMS with credential or passive authentication
      - Obtain an Azure app ID for BEMS with certificate-based authentication
   d) In the **Server name** field, enter the FQDN of the Microsoft Office 365 server (for example, https://outlook.office365.com).
   e) Optionally, select the **Use credentials if modern authentication fails** check box to allow BEMS to communicate with Microsoft Office 365 in the event that BEMS can't access the modern authentication source. When you select this check box, you must provide the BEMS service account credentials.

   Note: When you configure modern authentication, all nodes use the specified configuration.

4. In the **Service account username** field, enter the username that is used to log in to the Microsoft Exchange Server or Microsoft Office 365 server. The username must be in one of the following formats:
   - If your environment uses an on-premises Microsoft Exchange Server, use <*Domain*>\<*Username*> or UPN.
   - If your environment uses Microsoft Office 365, use <*username*>@<*domain*>.com.
5. In the **Service account password** field, enter the password for the service account username you provided.
6. Optionally, in the **Autodiscover URL override** field, enter the Autodiscover URL to allow BEMS to obtain user information from the Microsoft Exchange Server or Microsoft Office 365 server when it discovers users for BlackBerry Push Notifications.

   Note: If you don't enter a URL, BEMS uses Autodiscover to locate the Microsoft Exchange Server or Microsoft Office 365 server to obtain user information.
7. Select the **Allow HTTP redirection and DNS SRV record** check box to allow HTTP Redirection and DNS SRV lookups for retrieving the Autodiscover URL when discovering users for BlackBerry Push Notifications. By default, this feature is enabled.
8. Select the **Use BlackBerry Connectivity Node route** to allow BEMS Cloud to connect to the Microsoft Exchange Server or Microsoft Office 365 using the corporate network rather than using a direct connection from the BlackBerry BEMS Cloud infrastructure. This setting requires that the BlackBerry Connectivity Node is installed and configured in your environment. If your environment uses Azure AD conditional access, make sure that this option is selected.
9. If your environment uses an internal URL to access and communicate with an on-premises Microsoft Exchange Server, select the **Use internal Exchange Web Services URL** check box. This setting requires that the "Use BlackBerry Connectivity Node route" setting is enabled. This option is not available if modern authentication is enabled.
10. Optionally, select the **Enable SCP Lookup** check box to query Microsoft Active Directory using LDAP and locate Autodiscover endpoint URLs. This setting is valid only if the "Credential" authentication is selected and that a BlackBerry Connectivity Node is installed and configured in your environment. This option is not available when the "Autodiscover URL override" is specified.
11. Select the **Enable SSL for SCP** check box. This allows BEMS to communicate with the Microsoft Active Directory using SSL. This setting requires that the "Enable SCP Lookup" is selected. If you enable this feature, you must add the Microsoft Active Directory SSL certificate to the BEMS Cloud database. For information on how to add the certificate, see Create a trusted connection between BEMS Cloud and Microsoft Exchange Server.
12. If you enabled **Enable SCP Lookup** or **Enable SCP Lookup** and **Enable SSL for SCP**, specify the **Domain Controllers for SCP** to configure LDAP over SCP. If you have multiple domain controllers, separate the domain controllers using commas (for example, domaincontroller1.example.com,domaincontroller2.example.com, and so forth).
13. Optionally, in the **User email address** field, enter an email address to test the connection to the Microsoft Exchange Server or Microsoft Office 365 server. Click **Test connection**. If the test fails, resolve the issues that are identified and try the test again. You can delete the email address after you complete the test.
14. Click **Save**.

After you finish:

- Test the connection to the on-premises Microsoft Exchange Server or Microsoft Office 365 server and Autodiscover. Refresh or reopen the Email notifications screen. Click **Test connection**.
  Note: Make sure that the connection test is successful before provisioning devices to avoid any Autodiscover issues. If devices are activated prior to configuring the email notification service, have users log out of BlackBerry Work and then log in. If the test returns an error message, complete the tasks to resolve the issue and test the connection again.

- Assign the BlackBerry Cloud Enterprise Services (com.blackberry.gdservice-entitlement.cloud) entitlement to users to receive email notifications for BlackBerry Work. For instructions, see the following administration content:
  - Assign an app to a user group
  - Assign an app group to a user group
  - Assign an app to a user account
  - Assign an app group to a user account
- Optionally, create a trusted connection between the BEMS Cloud and Microsoft Exchange Server. For instructions, see Create a trusted connection between BEMS Cloud and Microsoft Exchange Server.
- Configure BlackBerry Work. For instructions, see the BlackBerry Work, Notes, and Tasks administration content.
- Optionally, configure the BEMS-Docs service. For instructions, see Enable the BEMS-Docs service.

Grant application impersonation permission to the service account

For the BlackBerry Push Notifications service to monitor mailboxes for updates, the BlackBerry Push Notifications service account, must have impersonation permissions.

Execute the following Microsoft Exchange Management Shell command to apply Application Impersonation permissions to the service account:

- Grant application impersonation permission using Exchange Administration Center
- Grant application impersonation permission using Microsoft Exchange Management Shell

Grant application impersonation permission using Exchange Administration Center

1. Depending on your environment, sign in to one of the following consoles:

Console	Steps
Microsoft Office 365 Exchange Administration Center console	**a.** Sign in to https://portal.office.com. **b.** Click the App Launcher icon in the top left hand corner. **c.** Click **Admin**. **d.** In the **Microsoft 365 admin center** console menu, click **Show all**. **e.** In the **Admin centers** section, click **All admin centers**. **f.** Click **Exchange**.
On-premises Microsoft Exchange Administration Center web console	**a.** Open a browser open `https://<url_to_on-premises_client_access_server>/ecp` and sign in with a valid account.

2. Click **permissions**.
3. Click +.
4. Type a name and description for the role group.
5. In the **Roles** section, click +. Click **ApplicationImpersonation > add > OK**.
6. In the **Members** section, click +. Click an account to add and then click **add > OK**.

Grant application impersonation permission using Microsoft Exchange Management Shell

1. Open Microsoft Exchange Management Shell.

2. Type `New-ManagementRoleAssignment -Name:<ImpersonationAssignmentName> -Role:ApplicationImpersonation -User:<ServiceAccount>`. For example, `New-ManagementRoleAssignment -Name:BlackBerryAppImpersonation -Role:ApplicationImpersonation -User:BEMSAdmin`.

After you finish:

For more information on how to restrict Application Impersonation rights to specific users, organizational units, or security groups, visit the MSDN Library to see How to: Configure impersonation.

Obtain an Azure app ID for BEMS with credential or passive authentication

1. Sign in to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for the app.
6. Select a supported account type.
7. In the **Redirect URI** section, in the drop-down list, complete one of the following tasks. The Redirect URI is the URL that the user is redirected to after they successfully authenticate to the identity provider (IDP). **Important**: Make sure that the Redirect URL matches the URL to the dashboard or authentication might not work as expected.
   - For credential authentication, select **Web** and enter `https://localhost:8443`.
   - For passive authentication, select **Public client/native (mobile & desktop)** and enter the URL that you use to access the BEMS Dashboard.
     - If you access the BEMS Dashboard from the computer that hosts the BEMS instance, enter `https://localhost:8443`.
     - If you access the BEMS Dashboard remotely, enter `https://<FQDN of the computer that hosts the BEMS instance>:8443`.
8. Click **Register**. The new registered app appears.
9. In the **Manage** section, click **API permissions**.
10. In the **Configured permissions** section, if Microsoft Graph is listed, click **Microsoft Graph**. If it is not listed, add **Microsoft Graph**.
11. Set the following permissions:
    - For Microsoft Exchange Web Services: Access mailboxes as the signed-in user via Exchange Web Services (**EWS > EWS.AccessAsUser.All**)
    - For Microsoft Graph: For Sign in and read user profile (**User > User.Read**).
12. Click one of the following:
    - If the Microsoft Graph API permission existed in the API permissions list, click **Update permissions**.
    - If you needed to add the Microsoft Graph API permission, click **Create**.
13. Click **Grant admin consent**. Click **Yes**.

    Important: This step requires tenant administrator privileges.
14. To allow autodiscovery to function as expected, set the authentication permissions.
    a) In the **Manage** section, click **Authentication**.
    b) Under the **Allow public client flows** section, select **Yes** to **Enable the following mobile and desktop flows**.
    c) Click **Save**.

15. Click **Overview**. Copy the **Application (client) ID**. The Application (client) ID is displayed in the main **Overview** page for the specified app. This is used as the **Client application ID** when you enable modern authentication and configure BEMS to communicate with Microsoft Office 365.

Obtain an Azure app ID for BEMS with certificate-based authentication

1. Sign in to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for the app.
6. Select a supported account type.
7. Optionally, in the **Redirect URI** section, in the drop-down list, select **Public/client (mobile & desktop)** and enter http://<*name of the app given in step 5*>.

   This app is a daemon, not a web app, and does not have a sign-on URL.
8. Click **Register**. The new registered app appears.
9. In the **Manage** section, click **API permissions**.
10. Click **Add a permission**.
11. In the **Select an API** section, click **APIs my organization uses**.
12. Click **Office 365 Exchange Online**.
13. Set the following permissions for Office 365 Exchange Online:
    - Application permissions: Use Exchange Web Service with full access to all mailboxes (**full_access_as_app**)
14. Click **Add permissions**.
15. Click **Microsoft Graph**. If the Microsoft Graph API permission is not listed, add it.
16. Set the following permission for Microsoft Graph.
    - Delegated permissions: Sign in and read user profile (**User > User.Read**)
17. Click **Add permissions**.
18. Click **Grant admin consent**.
19. Click **Yes**.
20. Click **Overview** to view the app that you created in step 5. Copy the **Application (client) ID**. The Application (client) ID is displayed in the main **Overview** page for the specified app. This is used as the **Client application ID** in the BEMS dashboard when you enable modern authentication and configure BEMS to communicate with Microsoft Office 365.

After you finish: Associate a certificate with the Azure app ID for BEMS

Associate a certificate with the Azure app ID for BEMS

You can use an existing certificate from your CA server or the New-SelfSignedCertificate command to create a self-signed certificate. For more information, visit docs.microsoft.com and read New-SelfSignedCertificate.

Before you begin: Verify that you have the app name you assigned in BEMS with certificate-based authentication.

1. If you have a certificate issued by a CA server, go to step 2. Create a self-signed certificate.
   a) On the computer running Microsoft Windows, open the Windows PowerShell.
   b) Enter the following command: `$cert=New-SelfSignedCertificate -Subject "CN=<app name>" -CertStoreLocation "Cert:\CurrentUser\My" -KeyExportPolicy Exportable -KeySpec Signature`.

- Where <*app name*> is the name you assigned the app in step 5 of Obtain an Azure app ID for BEMS with certificate-based authentication.

c) Press **Enter**.

2. Export the certificate from the Certificate Manager. This creates the public certificate. Make sure to save the public certificate as a .CER or .PEM.
   a) On the computer running Windows, open the Certificate Manager for the logged in user.
   b) Expand **Personal**.
   c) Click **Certificates**.
   d) Right-click the <*user*>@<*domain*> and click **All Tasks > Export**.
   e) In the **Certificate Export Wizard**, click **No, do not export private key.**.
   f) Click **Next**.
   g) Select **Base-64 encoded X.509 (.CER)**. Click **Next**.
   h) Provide a name for the certificate and save it to your desktop.
   i) Click **Next**.
   j) Click **Finish**.
   k) Click **OK**.
3. Upload the public certificate to associate the certificate credentials with the Azure app ID for BEMS.
   a) In portal.azure.com, open the <*app name*> you assigned the app in step 5 of Obtain an Azure app ID for BEMS with certificate-based authentication.
   b) Click **Settings > Keys**.
   c) Click **Upload Public Key**.
   d) Click and navigate to the location where you exported the certificate in step 2.
   e) Click **Open**.
   f) Click **Save**.

After you finish: Export the certificate in .pfx format using the Manage User Certificate MMC snap-in. Make sure to include the private key. For instructions, visit docs.microsoft.com and read Export a Certificate with the Private Key.

Create a trusted connection between BEMS Cloud and Microsoft Exchange Server

By default, BEMS is only aware of public CA certificates. If you enable email notifications for BlackBerry Work and your organization's Microsoft Exchange Server doesn't use an SSL certificate issued by a trusted CA, the connection between BEMS Cloud and Microsoft Exchange Server isn't trusted. To create a trusted connection to the Microsoft Exchange Server upload the server's SSL certificate (or the root or intermediate certificate chain) to the BEMS Cloud database. You can upload a base64-encoded or binary-encoded file that includes one or more SSL certificates. When you upload a single file that includes multiple SSL certificates, the certificates are displayed in the management console and can be deleted and replaced individually as required. BEMS Cloud supports the following file extensions: .der, .cer, .pem, and .crt.

Before you begin:

- Configure the email notifications for BlackBerry Work. For instructions, see Configure email notifications for BlackBerry Work.
- Export the SSL certificate from the Microsoft Exchange Server in a base64-encoded or binary-encoded format and store it in a network location that you can access from the management console. For more information about digital certificates and encryption in Microsoft Exchange Server, visit https://docs.microsoft.com/en-us/exchange/architecture/client-access/certificates?view=exchserver-2016

1. On the menu bar, click **Settings > BlackBerry Dynamics**.
2. Click **Email notifications**.
3. Click the **Certificates** tab.

4. Click .
5. Click **Add**.
6. Click **Browse** and navigate to the location of the certificate file that you want to upload.
7. Click **Add**.
8. If you upload individual SSL certificates, repeat steps 5 to 7 for each additional file.

Replace or delete the trusted connection SSL certificates

When you replace the SSL certificates (for example, when the certificates expire), you replace all of the existing SSL certificates in the BEMS database. You can chose to upload individual SSL certificates as required or include multiple SSL certificates in a single file. The following file types are supported: .der, .cer, .pem, and .crt.

Before you begin:

- Export the new SSL certificates from the Microsoft Exchange Server in a base64-encoded or binary-encoded format and store it in a network location that you can access from the management console. For more information about digital certificates and encryption in Microsoft Exchange Server, visit https://docs.microsoft.com/en-us/exchange/architecture/client-access/certificates?view=exchserver-2016

1. On the menu bar, click **Settings > BlackBerry Dynamics**.
2. Click **Email notifications**.
3. Click the **Certificates** tab.
4. Click .
5. Click **Remove** under the certificate that you want to delete.
6. Click **Remove** to confirm the deletion.
7. Add the new certificate. For instructions, see Create a trusted connection between BEMS Cloud and Microsoft Exchange Server.

Configure the password expiration warning message

For Active Directory users and user groups that use the PSO (Password Settings Object) method to set the maximum password age, you can configure BEMS Cloud to allow users' BlackBerry Work apps to display a warning message when their Active Directory password is about to expire.

Note: In the BlackBerry UEM management console, Email notifications for BlackBerry Work must be configured using the Credential authentication type to display the Password expiry tab.

For information on displaying a warning message for users that use the GPO (Global Policy Object) method to set the maximum password age, see the BlackBerry Work administration content.

Before you begin:

- Make sure that you have the following information:
  - Logon credentials for the service account that is used to authenticate to the domain controller.
  - LDAP server name and port number. The LDAP server name must be one of the Domain Controllers.
- Verify that the service account has READ permissions to the "Password Settings Container". For instructions, see Add Read permission to the account used to authenticate to the LDAP server.
- Verify that a BlackBerry Connectivity Node is installed and configured in your environment. For more information, see Steps to install and activate the BlackBerry Connectivity Node.
- Verify that administrators use the PSO method to set the maximum password age for the users.
- Verify that users in your environment are running BlackBerry Work 3.8 or later.

1. In the management console, click **Settings > BlackBerry Dynamics > Email notifications**.

2. Click the **Password expiry** tab.
3. Click .
4. Select the **Enable password expiry** checkbox to allow BEMS to query Active Directory for password expiry details for the users.
5. In the **LDAP server name** field, type the name of the LDAP Server (for example, ldap.<*DNS_domain_name*>).
6. In the **LDAP port** field, type the port number of the LDAP computer. The default port is 389.
7. Enter the LDAP logon account and password. You can enter the logon account in the format `domain\username` or User Principal Name (UPN) `username@domain`.
8. In the **Base DN (Domain controller)** field, enter the base DN for the LDAP search. If this entry is not set, BEMS tries to find the base DN in the namingContexts attribute.
9. Optionally, select the **Enable SSL LDAP** checkbox to tunnel data through an SSL-encrypted connection. If you enable SSL LDAP, type the port number to the LDAP computer that you used in step 6. The default port for is 636. This step requires you to import the LDAP certificate into the BEMS keystore. For instructions, see Create a trusted connection between BEMS Cloud and Microsoft Exchange Server.
10. Click **Test** to test the connection to the LDAP server.
11. Click **Save**.

Add Read permission to the account used to authenticate to the LDAP server

You can use the Windows Server ADSI Edit tool to add Read permissions to the account that is used to authenticate to the LDAP server. You must have a membership in the Domain Admins group or equivalent permissions to complete this task.

1. Start the ADSI Edit utility.
2. Right click the **ADSI Editor** icon and click **Connect to**.
3. In the **Connection Settings** screen, in the **Connection Point** section, select **Select a well known Naming Context** and from the drop-down list, select **Default naming context**.
4. Click **OK**.
5. Click your domain.
6. Navigate to and expand **CN=System**.
7. Right-click **CN=Password Settings Container** and click **Properties**.
8. On the **Security** tab, click **Add** to add the account, or the user group that the account is a member of, that is used to authenticate to the LDAP server.
9. Under **Group or user names**, with the added account or user group selected, select the **Read** checkbox in the**Allow** column.
10. Click **Apply**.
11. Click **OK**.

Configuring BlackBerry Dynamics Launcher

The BlackBerry Dynamics Launcher is a UI component that is accessed in BlackBerry Dynamics apps (for example, BlackBerry Work) with the BlackBerry Dynamics Launcher button. The BlackBerry Dynamics Launcher creates a placeholder location for app settings. The BlackBerry Dynamics Launcher is a library module with numerous functions, currently comprising of the following:

- The user's name, photo, presence, and status
- A list of BlackBerry Dynamics-powered apps and modules installed on the device.

- Quick create options to easily compose an email, create a note, schedule a calendar event, or add a contact, regardless of which app is currently open.

In the BlackBerry UEM management console, Email notifications for BlackBerry Work must be configured to display the BlackBerry Dynamics Launcher and set a customized icon for the BlackBerry Dynamics Launcher on user's devices.

Setting a customized icon for the BlackBerry Dynamics Launcher

You can specify a default customized icon for the BlackBerry Dynamics Launcher on users' devices. When you specify a customized icon, the icon replaces the BlackBerry Dynamics icon for all users managed by the BEMS instance.

When you specify a customized icon, make sure that the file meets the following requirements:

- Less than 500kb. Icons larger than 500kb are not added to the custom icons list.
- Named using the following format: <*file name*>_<*device_type*>_<*resolution*>.png. For example, Icon_iOS_2x.png.

  Where *resolution* is the supported resolution for the device. For example:

  - Android devices: ldpi, mdpi, hdpi, xhdpi, xxhdpi, and xxxhdpi
  - iOS devices: 1x, 2x, 3x, and so on
- Saved as a .png format

Specify a customized icon for the BlackBerry Dynamics Launcher

BEMS Cloud allows you to specify a custom icon for users in your environment. When you add custom icons, BEMS Cloud verifies the validity of the uploaded images. For more information about customized icon requirements, see Setting a customized icon for the BlackBerry Dynamics Launcher.

Before you begin:

- Verify that Email notifications for BlackBerry Work are configured.
- Verify that you have access to a supported customized icon for the BlackBerry Dynamics Launcher. For more information about the file requirements, see Setting a customized icon for the BlackBerry Dynamics Launcher.

1. In the BlackBerry UEM management console, on the menu bar, click **Settings > BlackBerry Dynamics > Launcher Branding**.
2. Select the **Show customized icon in launcher** checkbox.
3. Click the tab for the device for which you want to specify the launcher icon. By default, Android is selected.
4. Click +.
5. Navigate to the icon file location. Click the file and then click **Open**.
6. Click **Submit**.
7. Click **Save**.
8. Repeat steps 4 to 6 for each customized Android device icon file resolution.
9. Complete steps 3 to 6 for customized iOS device icon file resolution.

Remove a customized icon for the BlackBerry Dynamics Launcher

You can choose to remove a customized icon you specified for the BlackBerry Dynamics Launcher. If you remove all of the customized icon files, the default Launcher icon is used on the client devices for the Launcher app.

1. In the BlackBerry UEM management console, on the menu bar, click **Settings > BlackBerry Dynamics > Launcher Branding**.
2. Click the tab for the device that you want to remove the customized Launcher icon from.
3. Click ✕ beside the customized icon that you want to remove.

4. Click **Save**.

Configuring BEMS-Docs

You can use the BlackBerry UEM console to configure and maintain document and file repositories and user access policies for mobile app users of the service. When it is enabled, users can access, synchronize, and share documents using the following storage services: Microsoft SharePoint Online, Microsoft SharePoint, Microsoft OneDrive for Business, and Box. File Share and CMIS-based repository storage providers are not supported.

Note: If your environment requires users to access File Shares or CMIS-based repositories, configure BEMS-Docs in an on-premises BEMS instance. Enabling BEMS-Docs in BlackBerry UEM Cloud and in an on-premises BEMS in a BlackBerry UEM Cloud environment is not supported. For more information, see Configuring an on-premises BEMS in a BlackBerry UEM Cloud environment.

Repositories: The BEMS-Docs service provides your users with access to stored work data from their mobile devices. A Docs repository (also called a "share") exists on a work server. The repository contains files shared by authorized users. For more information about setting up and maintaining your shares in BlackBerry UEM and the associated user access, see Managing Repositories. Before you configure your repositories, enable and configure the BEMS-Docs service and configure BlackBerry Work in BlackBerry UEM to allow your users to access the repositories that you add and define from their device

Storage services: The BEMS-Docs service supports a number of storage services.

Steps to configure BEMS-Docs

When you configure BEMS-Docs, you perform the following actions:

Step	Action
1	Enable the BEMS-Docs service.
2	Configure BEMS-Docs settings.
3	Create a trusted connection between BEMS-Docs and Microsoft SharePoint.
4	Managing Repositories.
5	Assign the "Feature - Docs Service Entitlement (com.good.feature.share)" entitlement to users to allow BlackBerry Work Docs to connect to the BEMS-Docs service. For instructions, see the following administration content: • Assign an app to a user group • Assign an app group to a user group • Assign an app to a user account • Assign an app group to a user account

Enable the BEMS-Docs service

To allow users access to document and file repositories in your environment, you must enable the BEMS-Docs service. When you enable this service, a BEMS tenant is created and the BlackBerry Cloud Docs Service (com.blackberry.gdservice-entitlement.docs.cloud) entitlement is added to the BlackBerry Dynamics connectivity profile. If your environment uses both the BEMS-Docs service and email notifications for BlackBerry Work, configure the email notifications first. For instructions, see Configure email notifications for BlackBerry Work.

To enable the BEMS-Docs service, the BlackBerry Cloud Docs Service (com.blackberry.gdservice-entitlement.docs.cloud) entitlement must be present in the Organization > Entitlements in https://account.blackberry.com. This app entitlement does not need to be assigned to users in BlackBerry UEM Cloud.

1. In the management console, click **Settings > BlackBerry Dynamics > Docs**.
2. Click **Enable**.

Configure BEMS-Docs settings

Before you begin:

- Verify that the BEMS-Docs service is enabled.
- If your environment is configured for Microsoft SharePoint Online or Azure-IP, make sure that the BlackBerry Work app is registered in Azure so that it can access the BEMS-Docs Azure app. For instructions, see Obtain an Azure app ID for BlackBerry Work in the BlackBerry Work, Notes, and Tasks administration content.
- If your environment is configured for Azure-IP, have the following information available:
  - Azure tenant name
  - BEMS service Azure application ID
  - BEMS service Azure application key
- If BEMS-Docs is configured to communicate with an on-premises Microsoft SharePoint, make sure that Microsoft SharePoint repositories are using https secure ports. Using http non-secure ports is not supported.

1. In the management console, click **Settings > BlackBerry Dynamics > Docs**.
2. Click the **Settings** tab.
3. Complete one or both of the following tasks.

Environment	Steps
Your environment is configured to use Microsoft SharePoint Online or Azure-IP and Microsoft SharePoint Online	**a.** Optionally, select the **Enable Azure Information Protection** check box to allow BEMS-Docs to authenticate to Azure-IP. **b.** Enter the Azure tenant name. **c.** Enter the BEMS service Azure application ID that you obtained when you registered the BEMS-Docs component service. For instructions, see Obtain an Azure app ID for the BEMS-Docs component service. **d.** Enter the BEMS service Azure application key that you obtained when you registered the Docs app in Azure. For instructions, see Obtain an Azure app ID for the BEMS-Docs component service.

Environment	Steps
Your environment is configured to use an on-premises Microsoft SharePoint	a. Select the **Enable BlackBerry Connectivity Node** route check box to allow BEMS Cloud to connect to the BlackBerry Infrastructure instead of using an inbound port. This setting requires that the BlackBerry Connectivity Node is installed and configured in your environment. b. To allow BEMS-Docs to communicate with an on-premises Microsoft SharePoint server, extract the Microsoft SharePoint server certificate and send it to BlackBerry Support. If the on-premises Microsoft SharePoint sites use certificates that are not publicly trusted (for example, self-signed or enterprise CA certs), then send these certificates to BlackBerry Support.

4. Click **Save**.

Obtain an Azure app ID for the BEMS-Docs component service

When your environment is configured for Microsoft SharePoint Online, Microsoft OneDrive for Business, or Microsoft Azure-IP you must register the BEMS component services in Azure.

If your environment uses both Microsoft SharePoint Online and Microsoft Azure-IP or Microsoft OneDrive for Business and Microsoft Azure-IP, you must register the Microsoft SharePoint Online or Microsoft OneDrive for Business service. Microsoft Azure-IP will use the same information as the registered service.

Before you begin: To grant permissions, you must use an account with tenant administrator permissions.

1. Sign in to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for the app. For example, AzureAppIDforBEMS.
6. Select a supported account type.
7. In the **Redirect URI** drop-down list, select **Web** and enter `https://localhost:8443`.
8. Click **Register**.
9. Record the **Application (client) ID**. This is used as the **BEMS Service Azure Application ID** value in the BlackBerry UEM management console.This is used as the **BEMS Service Azure Application ID** value for the Docs > Settings service in the BEMS dashboard.
10. In the **Manage** section, click **API permissions**.
11. Click **Add a permission**.
12. Complete one or more of the following tasks:

Service	Permissions
If you configure BEMS-Docs to use Microsoft SharePoint Online or Microsoft OneDrive for Business	**a.** Search for and click **SharePoint**. **b.** Set the following permissions: • In application permissions, clear all of the permissions. **1.** Click **Application permissions**. **2.** Click expand all. Make sure that all options are cleared. • In delegated permissions, select the **Read and write items and item lists in all site collections** checkbox. None. Clear the check boxes for all options. • **Delegated permissions** Select the **Read and write items and lists in all site collections** checkbox. (**AllSite > AllSites.Manage**) **c.** Click **Add permissions**.
If you use Microsoft Azure-IP	**a.** Click **Microsoft Graph**. If Microsoft Graph is not listed, add Microsoft Graph. **b.** Set the following permissions: • In application permissions, select the **Read directory data** checkbox (**Directory > Directory.Read.All**). • In delegated permissions, select the **Read directory data** checkbox (**Directory > Directory.Read.All**). **c.** Click **Update permissions**. **d.** **Add a permission**. **e.** In the **Select an API** section, click **Azure Rights Management Services**. Set the following permissions: • In application permissions, select all of the permissions. **1.** Click **Application permissions**. **2.** Make sure that all Content options are selected. • In delegated permissions, select the **user_impersonation** checkbox. **f.** Click **Add permissions**. **g.** Click **Add a permission**. **h.** In the **Select an API** section, click **APIs my organization uses**. **i.** Search for and click **Microsoft Information Protection Sync Service**. Set the following permission: • In delegated permissions, select the **Read all unified policies a user has access to** checkbox (**UnifiedPolicy > UnifiedPolicy.User.Read**). **j.** Click **Add permissions**.

13. Wait a few minutes, then click **Grant admin consent**. Click **Yes**.

    Important: This step requires tenant administrator privileges.

14. To allow autodiscovery to function as expected, set the authentication permissions. Complete the following steps:
    a) In the **Manage** section, click **Authentication**.
    b) Under the **Allow public client flows** section, select **Yes** to **Enable the following mobile and desktop flows**.
    c) Click **Save**.
15. Define the scope and trust for this API. In the **Manage** section, click **Expose an API**. Complete the following tasks.

Task	Steps
Add a scope	The scope restricts access to data and functionality protected by the API. **a.** Click **Add a scope**. **b.** Click **Save and continue**. **c.** Complete the following fields and settings: • Scope name: Provide a unique name for the scope. • Who can consent: Click **Admins and user**. • Admin consent display name: Enter a descriptive name. • Admin consent description: Enter a description for the scope. • State: Click **Enabled**. By default, the state is enabled. **d.** Click **Add Scope**.
Add a client application	Authorizing a client application indicates that the API trusts the application and users shouldn't be prompted for consent. **a.** Click **Add a client application**. **b.** In the **Client ID** field, enter the client ID that you recorded in step 9 above. **c.** Select the **Authorized scopes** checkbox to specify the token type that is returned by the service. **d.** Click **Add application**.

16. In the **Manage** section, click **Certificates & secrets** and add a client secret. Complete the following steps:

a) Click **New client secret**.
b) In the **Description** field, enter a key description up to a maximum of 16 characters including spaces.
c) Set an expiration date (for example, In 1 year, In 2 years, Never expires).
d) Click **Add**.
e) Copy the key **Value**.

Important: The Value is available only when you create it. You cannot access it after you leave the page. This is used as the **BEMS Service Azure Application Key** value in the BlackBerry UEM console.

Allow authentication to BEMS-Docs using an alternate email address

You can configure BEMS Cloud to allow users to authenticate to Microsoft SharePoint Online and Microsoft OneDrive for Business with an email address that is different from the email address that was used to install and activate BlackBerry Work. To enable this feature, contact BlackBerry Technical Support.

Create a trusted connection between BEMS-Docs and Microsoft SharePoint

By default, BEMS Cloud is only aware of public CA certificates. If you enable the BEMS-Docs service and your organization's Microsoft SharePoint on-premises doesn't use an SSL certificate issued by a trusted CA for HTTPS sites, the connection between the BEMS-Docs service and Microsoft SharePoint on-premises isn't trusted and users won't be able to access files and documents from the BlackBerry Work Docs app. To create a trusted connection to Microsoft SharePoint, upload the server's SSL certificate if it is self-signed, or the root or intermediate certificate chain to the BEMS Cloud database. You can upload a base64-encoded or binary-encoded file that includes one or more SSL certificates. When you upload a single file that includes multiple SSL certificates, the certificates are displayed in the management console and can be deleted and replaced individually as required. BEMS Cloud supports the following file extensions: .der, .cer, .pem, and .crt.

Before you begin:

- Verify that you have enabled the BEMS-Docs service.
- Export the SSL certificate from the Microsoft SharePoint server in a base64-encoded or binary-encoded format and store it in a network location that you can access from the management console.

1. On the menu, click **Settings > BlackBerry Dynamics > Docs**.
2. Click the **Certificate** tab.
3. Click **Add** and navigate to the location of the certificate file that you want to upload.
4. Click **Add**.
5. If the upload fails, resolve the issue that is identified and try again.
6. If you upload individual SSL certificates, repeat steps 3 and 4 for each additional file.

Replace or delete the BEMS-Docs trusted connection certificate

When you replace the SSL certificates (for example, when the certificates expire), you replace the existing SSL certificates in the BEMS Cloud database. You can choose to upload individual SSL certificates as required or include multiple SSL certificates in a single file. The following file types are supported: .der, .cer, .pem, and .crt.

Before you begin: Export the new SSL certificates from Microsoft SharePoint on-premises in a base64-encoded or binary-encoded format and store it in a network location that you can access from the management console.

1. On the menu, click **Settings > BlackBerry Dynamics > Docs**.
2. Click the **Certificate** tab.
3. Click **Delete** below each certificate that you want to delete. Click **Delete**.
4. Add the new certificate files as required. For instructions, see Create a trusted connection between BEMS-Docs and Microsoft SharePoint.

Managing Repositories

BEMS Cloud has the following repository storage providers:

Storage repository	Description
SharePoint	A secure web server containing shared files which are accessed via the Internet.
SharePoint Online	If your environment is configured for Microsoft OneDrive for Business the SharePoint Online storage repository is used.
Box	A secure cloud storage account furnished by box.com containing shared files which can be accessed via the Internet.

A repository is further categorized in the BEMS-Docs service by who added and defined.

Storage repository	Description
Admin-defined	Storage provider sites added and maintained by BlackBerry UEM administrators to which individual users and user groups are granted access.
User-defined	Sites added by individual end users from their mobile devices to which you, as the BlackBerry UEM administrator, may rescind and reinstate mobile-based access in accordance with your enterprise IT acceptable-use policies.

Configuring repositories

The Repository configuration page has the following three tabs that you can configure:

Tabs	Description
Admin defined	Allows you to create and manage repositories, add and remove users and user groups, and assign users and user groups file access and use permissions.
User defined	Allows you to add and remove users and user groups, enable and disable user and user group the ability to create user-defined repositories, and grant and rescind permissions to perform a range of file-related actions on their user-defined repositories.
Users	Allows you to search for a user on the BlackBerry UEM Cloud to view the repositories permitted by path or override, and who defined the share (for example, administrator or user).

Admin-defined shares

Shares are document repositories for a particular storage provider.

When you define repositories, you perform the following actions:

Step	Action
1	Define a repository.
2	Define user and user group access permissions.

Granting user access permissions

Access permissions are defined for a single repository or inherited from an existing list of repositories. Permissions can be selectively granted to existing Microsoft Active Directory domain users and user groups. At least one user or user group must be added to the repository definition to configure access permissions.

The following table lists the access permissions and the default setting that are available.

Permission	Permissions Attributes	Default setting
List (Browse)	View and browse repository content (for example, subfolders and files) in a displayed list, and sort lists by Name, Date, Size, or Kind	Enabled
Delete Files	Remove files from the repository	Enabled
Read (Download)	Download repository files to the user's device and open them to read	Enabled
Write (Upload)	Upload files (new/modified) from user's device to the repository for storage	Enabled

Permission	Permissions Attributes	Default setting
Cache (Offline Files)	Temporarily store a cache of repository files on the device for offline access. You can designate files and folders to synchronize to users' BlackBerry Work Docs app Offline folder.	Enabled
Open In	Open a file in a format-compatible app on the device	Enabled
Create Folder	Add new folders to the repository	Enabled
Copy/Paste	Copy repository file content and paste it into a different file or app	Enabled
Check In/Check Out	When a file is checked out, the user can edit, close, reopen, and work with the file offline. Other users cannot change the file or see changes until it is checked back in	Enabled (SharePoint only)
Generate Shared Link	Users can generate a link to a file and folder and send the link to recipients The Generate Shared Link requires an updated BlackBerry Work app.	Enabled (Box only)

Change access permissions

1. In the management console, click **Settings > BlackBerry Dynamics > Docs**.
2. Click **Repositories**.
3. Click the **Admin defined** tab.
4. Click a repository.
5. Under **Access Permissions**, beside the user or user group, select or clear the permission checkbox that you want to change.
6. Click ⊗ beside a user or user groups that you want to remove.
7. Click **Save**.

Define a repository

BlackBerry UEM users and groups must be added to a repository definition before access permissions can be configured. Users and groups that are added automatically receive the default access permissions.

Before you begin: For users to access their Microsoft SharePoint repositories on their devices, make sure that they have the "Read" permission level and the "Browse Directories" permission assigned.

1. In the management console, click **Settings > BlackBerry Dynamics > Docs**.
2. Click **Repositories**.
3. Click the **Admin defined** tab.
4. Click +.
5. In the **Name** field, type the name of the repository that will be displayed to users granted mobile access to the repository.

   The repository name must be unique and can contain spaces. The following special characters cannot be used due to third-party limitations:

- Microsoft SharePoint 2010, 2013, 2016, and 2019: ~ " # % & * : < > ? / \ { | }
- Box: \ /|

6. In the **Storage** drop-down list, select a storage provider.

   If you select **SharePoint** or **SharePoint Online**, and the share is running SharePoint 2013 or later, select the **Add sites followed by users on this site** check box to make this feature available to users of this share. This setting only applies for personal (my) SharePoint or OneDrive for Business sites.

   If your environment is configured for Microsoft OneDrive for Business, select the SharePoint Online storage provider.

7. In the **Path** field, specify the path to the share. Complete one of the following tasks based on the storage type that you selected in step 6.

   The following variables are supported in the Path field:

   - username
   - sAMAccountName
   - mail
   - dnsDomain
   - If the personal site includes usernames, enter the path including these variables. For example, https://sharepoint.example.com/my/<sAMAccountName>.

Storage type	Description
Box	Enter a fully qualified URL with or without the supported variables listed above.
SharePoint SharePoint Online	If your storage provider is Microsoft OneDrive for Business, complete this task. Enter a fully qualified URL with or without the supported variables listed above. To add "my" or personal SharePoint sites, specify the URL for the "my" site. For example, • If your environment uses SharePoint and SharePoint Online, https://<*Microsoft SharePoint server*>/my. • If your environment uses Microsoft OneDrive for Business, *https://<your O365 domain>-my.sharepoint.com/personal/admin_<domain>_onmicrosoft_com/_layouts/15/onedrive.aspx* Optionally, to automatically add followed sites, complete the following steps: **a.** Add a repository for the "my" or personal SharePoint site. **b.** Select the **Add sites followed by users on this site** for the repository. **c.** On the **User-defined** tab, enable a user-defined repository permission. Make sure that you select the **Enable 'User Defined Shares'** and **Automatically add sites followed by users** check boxes. For instructions, see Enable user-defined repository permissions.

8. In the **Access permissions** section, click +.
9. Select one of the following:

   - **Users**: In the **Add a user** dialog box, field, type a full or partial search string. Click the user that you want to add.
   - **Groups**: In the **Add a group** screen, select one or more groups. Click →. Click **Add**.

10. Click **Add**.

11. Click **Save**. If the save fails and the issue is determined, the appropriate error message is displayed (for example, if you have a repository named Marketing and you create another repository with the same name, the error message **Repository already exists with name Marketing** is displayed). Resolve the issue that is specified and save again.

Add users and user groups to repositories

Microsoft Active Directory users and groups must be added to a repository definition before access permissions can be configured. Users and groups added automatically receive the default access permissions.

1. In the management console, click **Settings > BlackBerry Dynamics > Docs**.
2. Click **Repositories**.
3. Click the **Admin Defined** tab.
4. Click a repository
5. Under **Access permissions**, click +.
6. Select one of the following:
   - **Users**: In the **Add a user** dialog box, field, type a full or partial search string. Click the user that you want to add.
   - **Groups**: In the **Add a group** screen, select one or more groups. Click →. Click **Add**.
7. Click **Add**.
8. Click **Save**.

After you finish: Grant user and user groups access permissions.

Edit a repository

1. In the management console, click **Settings > BlackBerry Dynamics > Docs**.
2. Click **Repositories**.
3. Click the **Admin defined** tab.
4. Click a repository you want to edit.
5. Make the required changes.
6. Click **Save**.

Allow user-defined repositories

When you allow users to define their own repositories, you perform the following actions:

1. Enable user-defined repository permissions
2. Change user access permissions

Enable user-defined repository permissions

Before you begin: For users to access their Microsoft SharePoint repositories on their devices, make sure that they have the "Read" permission level and the "Browse Directories" permission assigned.

1. In the management console, click **Settings > BlackBerry Dynamics > Docs**
2. Click **Repositories**.
3. Click the **User Defined** tab.
4. Select the **Enable 'User Defined Shares'** checkbox to allow your mobile users to define their own data sources.

5. Optionally, select the **Automatically add sites followed by users** checkbox for authorized Microsoft SharePoint repositories with the required MySite plugin enabled.

   To automatically add followed sites, complete the following steps:

   a. On the Admin-defined tab, add a repository for the "my" or personal SharePoint site. For instructions, see Define a repository.
   b. Select the **Add sites followed by users on this site** for the repository.
   c. On the User-defined tab, make sure that you select the **Enable user-defined shares** and **Automatically add sites followed by users** check boxes.
6. In the **Storage** section, select one or more storage services.

   If you do not select at least one storage option, the user-defined option is disabled.
7. In the **Access Permissions** section, click +.
8. Select **Users** or **Groups**.
9. Select one of the following:

   - **Users**: In the **Add a user** dialog box, field, type a full or partial search string. Click the user that you want to add.
   - **Groups**: In the **Add a group** screen, select one or more groups. Click →. Click **Add**.
10. Click **Add**. The users and groups added automatically receive the default access permissions.
11. Click **Save**.

Access permissions

Permissions can be selectively granted to existing Microsoft Active Directory domain users and user groups. The most restrictive permissions (admin-defined or user-defined) are applied.

The following table lists the permissions that are provided by default when you add users and groups to the User-defined repositories.

Permission	Permissions Attributes	Default setting
List (Browse)	View and browse repository content (for example, subfolders and files) in a displayed list, and sort lists by Name, Date, Size, or Kind	Enabled
Delete Files	Remove files from the repository	Enabled
Read (Download)	Download repository files to the user's device and open them to read	Enabled
Write (Upload)	Upload files (new/modified) from user's device to the repository for storage	Enabled
Cache (Offline Files)	Temporarily store a cache of repository files on the device for offline access You can designate files and folders to synchronize to users' BlackBerry Work Docs app Offline folder.	Enabled
Open In	Open a file in a format-compatible app on the device	Enabled
Create Folder	Add new folders to the repository	Enabled

Permission	Permissions Attributes	Default setting
Copy/Paste	Copy repository file content and paste it into a different file or app	Enabled
Check In/Check Out	When a file is checked out, the user can edit, close, reopen, and work with the file offline. Other users cannot change the file or see changes until it is checked back in	Enabled (SharePoint only)
Add New Repositories	Permits new repositories to be added from the user's mobile device	Disabled
Generate Shared Link	Users can generate a link to a file and folder and send the link to recipients The Generate Shared Link requires an updated BlackBerry Work app.	Enabled (Box only)

Change user access permissions

1. In the management console, click **Settings > BlackBerry Dynamics > Docs**.
2. Click **Repositories**.
3. Click the **User defined** tab.
4. Under **Access Permissions**, beside the user or user group, select or clear the permission checkbox that you want to change.
5. Click ⊗ beside a user or user groups that you want to remove.
6. Click **Save**.

View user repository rights

In some scenarios, you may need to search for a particular user to review which repositories are configured for their access, as well as the specific permissions granted. For example, when a user is one member of a Microsoft Active Directory group configured for repositories and is not listed individually in your admin-defined or user-defined repository configurations and you want to consider making specific changes to the user's access permissions.

1. In the management console, click **Settings > BlackBerry Dynamics > Docs**.
2. Click the **Repositories** tab.
3. Click the **Users** tab.
4. In the **Search** field, begin typing the user's Microsoft Active Directory account name. If you don't see the user you want, extend or narrow the search string.
5. Click the user name. The **Defined by** column specifies if the repository is admin-defined or user-defined.
6. Click the name of the repository to view the user's access permissions. To modify the access permissions, see Change user access permissions.
7. Optionally, if the repository is admin-defined, in the**Override Path for this user** field, enter an override path.
8. Optionally, if the repository is user-defined, in the**epository name** field, enter a new repository name.

Configuring an on-premises BEMS in a BlackBerry UEM Cloud environment

You can configure an on-premises BEMS to communicate with the BlackBerry Proxy to authenticate GDAuth tokens in a BlackBerry UEM Cloud environment. When you configure your environment with an on-premises BEMS, you allow iOS and Android users to use the BEMS-Connect, BEMS-Presence, and BEMS-Docs services, in addition to the BEMS Cloud email notifications and BEMS-Docs service for BlackBerry Work.

If your environment requires users to access File Shares or CMIS- based repositories, configure BEMS-Docs in an on-premises BEMS. Enabling BEMS-Docs in BlackBerry UEM Cloud and in an on-premises BEMS in a BlackBerry UEM Cloud environment is not supported.

Note: You can configure BEMS with only one on-premises BlackBerry UEM or BlackBerry UEM Cloud environment at a time.

Steps to configure BlackBerry UEM Cloud to communicate with on-premises BEMS

When you configure BlackBerry UEM Cloud to communicate with on-premises BEMS, you perform the following actions:

Note: Some of the following tasks might have already been completed when you configured BlackBerry UEM Cloud.

Step	Action
1	Configure BlackBerry UEM Cloud in your environment.
2	In the BlackBerry UEM Cloud console, install the BlackBerry Connectivity Node or upgrade it to the latest version. 1. Verify that your organization meets the prerequisites to install the BlackBerry Connectivity Node 2. Download the installation and activation files for the BlackBerry Connectivity Node from the management console 3. Install, activate, and configure the BlackBerry Connectivity Node
3	If you are using Connect, install and configure the following on-premises BEMS services. For instructions on installing an on-premises BEMS, see the BEMS installation content and following BEMS services content: • BEMS-Connect • BEMS-Presence • BEMS-Docs

Step	Action
4	In the BEMS Dashboard, Configure the BlackBerry Dynamics server in BEMS. Optionally, configure SSL communication between the BlackBerry Connectivity Node and the on-premises BEMS on port 17433. 1. Export the BlackBerry Proxy certificate to the local computer 2. Import the certificate to the BEMS Windows keystore 3. Import the certificate into the Java keystore on BEMS **Note:** If you don't configure SSL communication, clear the **Enforce SSL Certificate Validation when communicating with BlackBerry Dynamics** check box.
5	In the BEMS Dashboard, Configure BEMS connectivity with BlackBerry Dynamics.

6	In the BlackBerry UEM Cloud console, assign BlackBerry Connect and BlackBerry Presence Service apps to users.
	• You can assign the apps using one of the following methods. For instructions, see the following BlackBerry UEM Cloud administration content:
	  • Assign an app to a user group
	  • Assign an app group to a user group
	  • Assign an app to a user account
	  • Assign an app group to a user account

7	In the BlackBerry UEM Cloud console, create a BlackBerry Dynamics Connectivity profile and add the app server that hosts the BlackBerry Connectand BlackBerry Presence Service, and Feature - Docs Service Entitlement apps.

Import the certificate to the BEMS Windows keystore

For the Connect service to trust the BlackBerry Proxy server's certificate, you must import BlackBerry Proxy certificate to the Connect service Windows keystore. Repeat this task on each BEMS instance.

Before you begin: Save a copy of the ca.cer certificate you exported to a convenient location on the computer that hosts BEMS. For instructions, see Export the BlackBerry Proxy certificate to the local computer.

1. Open the Microsoft Management Console.
2. Click **Console Root**.
3. Click **File > Add/Remove Snap-in**.
4. Click **Certificates**.
5. Select **Computer Account > Local computer > OK**.
6. Expand **Certificates (Local Computer) > Trusted Root Certification Authorities**.
7. Right-click **Certificates**, and click **All Tasks > Import**.
8. Click **Next**.
9. Browse to where you saved the certificate that you exported (for example <*drive*>:\bemscert\ca.cer). Click **Open**.
10. Click **Next**.

11. Click **Finish**. Click **OK**.

After you finish: Configure the Core BEMS service for communicating to BlackBerry Dynamics. For instructions, see Configure BEMS connectivity with BlackBerry Dynamics.

Import the certificate into the Java keystore on BEMS

For the Presence and Docs service to trust the BlackBerry Proxy server's certificate, you must import BlackBerry Connectivity Node certificate. Use the DBmanager to import the certificate into the BEMS Java keystore. By default, DBmanager is located in the installation folder at `<drive>:\GoodEnterpriseMobilityServer<version>\GoodEnterpriseMobilityServer\DBManager`.

Before you begin: Save a copy of the ca.cer certificate you exported to a convenient location on the computer that hosts BEMS. For instructions, see Export the BlackBerry Proxy certificate to the local computer.

1. On the computer that hosts the on-premises BEMS, verify that the PATH System variable includes the path to the JAVA directory.
   a) In a command prompt, type `set | findstr "Path"`.
   b) Press **Enter**.

   For more information about setting the Path system variable, see "Configure the Java Runtime Environment" in the BEMS in a BlackBerry UEM environment installation content.
2. Make a backup of the Java keystore file. The Java keystore file is located at `%JAVA_HOME%\lib\security\cacerts`, where JAVA_HOME is confirmed in Step 1.
3. Import the root BlackBerry Proxy certificate.
   a) Open a command prompt and navigate to the DBManager folder. For example, if the installation files are saved to your Downloads folder, type `C:\Users\besadmin\Downloads\GoodEnterpriseMobilityServer<version>\GoodEnterpriseMobilityServer\DBManager`
   b) Import the certificate. Type `java -jar dbmanager-<version>-jar-with-dependencies.jar -moduleName pushnotify -dbType sqlserver -dbName <SQL_server_DB_name> -dbHost <Name of the computer hosting the SQL DB> -dbPort 1433 -userName gems_sa -password <BEMS_service_account_password> -action addcertificate -pemFile "C:\<path to the pemfile location>\<certificate name>.cer" -alias gdcert`
4. Restart the Good Technology Common Services service in the Windows Service Manager.

After you finish: Configure the Core BEMS service for communicating to BlackBerry Dynamics. For instructions, see Configure the BlackBerry Dynamics server in BEMS.

Configure the BlackBerry Dynamics server in BEMS

Your BEMS environment must be configured to trust the Root CA for the BlackBerry Proxy HTTPS configuration or implement the Karaf workaround. For instructions, see "Importing and configuring certificates" in the BEMS-Core configuration content.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **BEMS Configuration**.
2. Click **BlackBerry Dynamics**.
3. Complete one of the following actions:

Task	Steps
If a BlackBerry Proxy server is not defined	**a.** Click **Add BlackBerry Proxy**. **b.** In the **Host Name** field, type the BlackBerry Proxy server host name. **c.** In the **Protocol** drop-down list, select the protocol used to communicate with the BlackBerry Proxy server. • If you select HTTPS, the **Port** field prepopulates to 17433. This is secure. • If you select HTTP, the **Port** field prepopulates to 17080. **Note:** If you configure your environment for HTTPS, you must Export the BlackBerry Proxy certificate to the local computer and then Import the certificate into the Java keystore on BEMS. **d.** Click **Test** to test the connection. **e.** Repeat steps 1 to 4 to add additional BlackBerry Proxy servers for redundancy continuity.
If one or more BlackBerry Proxy servers are defined	No action is required. Previously defined BlackBerry Proxy servers are listed.

4. Select the **Apply to other nodes in the BEMS cluster** check box to communicate the BlackBerry Proxy server information to all of the BEMS nodes in the cluster.
5. Optionally, select the **Enforce the SLL Certificate validation when communicating with BlackBerry Dynamics** check box when you use the https protocol to communicate with the BlackBerry Proxy server.
6. Click **Save**.

Configure BEMS connectivity with BlackBerry Dynamics

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Connect**.
2. Click **Service Account**.
3. Enter the service account username and password.
4. Click **Save**.
5. Click **BlackBerry Dynamics**.
6. In the **Hostname** field, type the BlackBerry Proxy server hostname.
7. In the **Port** field, the port number is prepopulated based on the communication type that you select.
   - If you select HTTP, the Port field prepopulates to 17080.
   - If you select HTTPS, the Port field prepopulates to 17433. This is secure.

   Note: If you configure your environment for HTTPS, you must Export the BlackBerry Proxy certificate to the local computer and then Import the certificate to the BEMS Windows keystore.
8. Click **Test** to verify the connection to the BlackBerry Proxy server.
9. Click **Save**.

After you finish: If you selected HTTPS, you must configure the BlackBerry Connect app to use SSL communications. For instructions, see "Configuring BlackBerry Connect app settings" for your environment in the BlackBerry Connect Administration content.

Add an app server hosting the entitlement apps to a BlackBerry Dynamics connectivity profile

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and Connections > BlackBerry Dynamics connectivity**.
3. Click + to create a new connectivity profile or click the BlackBerry Dynamics connectivity profile that you want to add an app server to.
4. If necessary, click ✎.
5. Under **App servers**, click **Add**.
6. Select the **Feature - Docs Service Entitlement** app that you want to add an app server for.
7. Click **Save**.
8. In the table for the app, click +.
9. In the **Server** field, specify the FQDN of the on-premises BEMS server.
10. In the **Port** field, specify the port of the BlackBerry Proxy cluster that is used to access the server. By default, the port is 8443.
11. In the **Priority** drop-down list, specify the priority of this or these servers as primary.
12. In the **Primary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the primary cluster.
13. In the **Secondary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
14. Click **Save**.
15. Repeat steps 5 to 14 for the following apps:
    - BlackBerry Connect
    - BlackBerry Presence Service

Export the BlackBerry Proxy certificate to the local computer

If you must configure SSL comunication to allow communication between the BlackBerry Connectivity Node and on-premises BEMS services (for example, the Connect, Docs, and Mail services), export the BlackBerry Proxy root and intermediate certificate chains and import them into the Java keystore on BEMS and the Windows keystore.

Note: The following task is not browser-specific. For specific instructions, see the documentation for the browser you are using.

Before you begin: Verify that the BlackBerry Connectivity Node is installed with a status of Running.

1. On the computer that hosts the BlackBerry Connectivity Node, export the BlackBerry Proxy certificate to your computer. In a browser, type `https://localhost:17433`. A certificate error message is displayed because the certificate was signed by a CA that is not recognized as a well-known CA.
2. To open the Certificate dialog, click the certificate icon in the URL field.
3. Click **Certificate**.
4. Click **Certificate Path**.
5. Click the root certificate. The root certificate is the first item in the Certificate hierarchy.
6. Click **View Certificate**.
7. Click the **Details** tab.

8. Click **Copy to File**.
9. Click **Next**.
10. Select **Base-64 encoded X.509 (.CER)**.
11. Click **Next**.
12. Click **Browse**.
13. Enter a name for the certificate (for example, ca.cer) and export it to the local computer.
14. Click **Save**.
15. Click **Finish**.
16. Click **OK**.

After you finish:

- If you configure the Connect service, copy the exported BlackBerry Proxy certificate to the computer that hosts BEMS and Import the certificate to the BEMS Windows keystore.
- If you configure the Presence service and Docs service, copy the exported BlackBerry Proxy certificate to the computer that hosts BEMS and Import the certificate into the Java keystore on BEMS.

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 BlackBerry UEM server.

To migrate users, devices, groups, and other data, perform the following actions:

Step	Action
1	Review the migration prerequisites.
2	Connect to a source server.
3	Optionally, migrate IT policies, profiles, and groups.
4	For migrations from a BlackBerry UEM source server with BlackBerry Dynamics apps enrolled, Complete policy and profile migration for BlackBerry Dynamics-activated users.
5	Migrate users.
6	Migrate devices.

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

Complete the following prerequisites before you begin a migration.

Prerequisite	Details
Log in	Log in to BlackBerry UEM as a Security Administrator. Only one administrator should perform migration activities at any one time.
Check the software version	To migrate data to BlackBerry UEM Cloud, the on-premises BlackBerry UEM instance you are migrating data from must be at BlackBerry UEM version 12.13 or later.
BlackBerry Connectivity Node	To use all of the migration features, activate at least one BlackBerry Connectivity Node instance running version 2.13 or later.

Prerequisite	Details
Configure the BlackBerry UEM company directory connection	Configure the destination BlackBerry UEM company directory connection in the same way that it is configured in the source. For example, if the source is configured for Active Directory integration and it is connected to the example.com domain, configure the destination BlackBerry UEM for Active Directory integration and connect it to the example.com domain. **Important:** Migration does not work if the company directory on the destination server does not match the company directory on the source server.
BlackBerry UEM Client	The BlackBerry UEM Client must be at BlackBerry Dynamics SDK version 8.0 or higher. You can find the SDK version in the release notes for the app.
Check the status of BlackBerry Dynamics apps	Check the BlackBerry Dynamics SDK version of all BlackBerry Dynamics apps you want to migrate. This includes first-party apps, BlackBerry Dynamics apps, third-party ISV apps, and internal custom apps. For migrations from an on-premises BlackBerry UEM source database, all BlackBerry Dynamics apps must be at BlackBerry Dynamics SDK version 8.0 or later. You can find the SDK version in the release notes for the app. **BlackBerry Dynamics apps that are not supported for migration are wiped from the device when the administrator starts the migration.**
Check the status of BlackBerry Dynamics app entitlements	Make sure that: • The destination BlackBerry UEM has the same list of BlackBerry Dynamics app entitlements as the source server. • All migrated user accounts are assigned the same list of BlackBerry Dynamics app entitlements on the destination BlackBerry UEM as they have on the source server. • The authentication delegate is the same on the source server and the destination server. You can change the authentication delegate after migration. • The user's BlackBerry Dynamics profile allows the BlackBerry UEM Client to be activated by BlackBerry Dynamics, if the user's BlackBerry UEM Client on the source server is also activated by BlackBerry Dynamics. **CAUTION:** Missing entitlements will result in BlackBerry Dynamics apps being disabled after migration.
Review organization IDs	Custom apps migrate only if the source and destination servers have the same organization ID. It is possible to merge two organizations. For more information, visit support.blackberry.com/community to read article 47626.
Check that the required ports are not blocked by a firewall or in use by other software	Ensure that port 8887 (TCP) is open between the on-premises BlackBerry UEM server and the BlackBerry Connectivity Node. The on-premises server listens on port 8887 for connections from the BlackBerry Connectivity Node. Ensure that the port used by the Microsoft SQL Server that hosts the on-premises BlackBerry UEM database is open and can be accessed by the BlackBerry Connectivity Node (for example, port 1433).

Connect to a source server

You must connect BlackBerry UEM to the source server that you are migrating data from.

Note: If more than one BlackBerry Connectivity Node is activated, make sure that you configure all BlackBerry Connectivity Node instances to connect to the same source database. All BlackBerry Connectivity Nodes must be running.

Note: To connect to a different source server than the one that is configured, remove the existing source configuration and then add the new one.

1. In the BlackBerry Connectivity Node management console, on the menu bar, click **General settings > Migration**.
2. Click +.
3. In the **Display name** field, type a descriptive name for the source database.
4. In the **Database server** field, type the name of the computer that hosts the source database, using the <host>\<instance> format for a dynamic port and the <host>:<port> format for a static port.
5. In the **Database authentication type** drop-down list, select the type of authentication you use to connect to the source database.
6. Do one of the following:

Option	Description
If you selected SQL authentication	a. In the **SQL username** and **SQL password** fields, type your login information to connect to the source database. b. In the **Database name** field, type the name of the source database.
If you selected Windows NT authentication	a. Change the Log On properties of the BlackBerry UEM - BlackBerry Cloud Connector service to the same account you used to install the source BlackBerry UEM. For more information about log on accounts, see the Microsoft TechNet article, Services permissions. **Note:** After the migration from this source is complete, return the Log On properties setting to Local System account. b. In the **Database name** field, type the name of the source database.

7. Click **Save**.
8. In the BlackBerry UEM management console, on the menu bar, click **Settings > Migration > Configuration**.
9. Click +.
10. Type a descriptive name for the source database.
11. To test the connection between the source and the destination, click **Test connection**.
12. Click **Save**.

After you finish:

- If you want to migrate IT policies, profiles, and groups, review the best practices and see Migrate IT policies, profiles, and groups from a source server.
- If you want to migrate users, review the considerations and see Migrate users from a source server.
- After you migrate users, see Migrate devices from a source server.

Considerations: Migrating IT policies, profiles, and groups from a source server

A migration from a BlackBerry UEM source copies the following items to the destination database:

- 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

Note: For groups migrated from BlackBerry UEM, user, role, and software configuration assignments are not migrated. You must manually recreate these assignments on the destination BlackBerry UEM server.

BlackBerry UEM

When you migrate BlackBerry UEM IT policies, profiles, and groups to another domain, consider the following guidelines:

Item	Considerations
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 BlackBerry UEM IT policies or profiles can be migrated. Deselect or update the source IT policy and restart the migration.
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.
Directory groups	To migrate directory groups, the source database and destination database must each have only one directory configured. This directory must be configured the same way on both the source and destination database. If the directories are not set up this way, directory groups are not migrated.

Apps activated with BlackBerry Dynamics

When you migrate connectivity profiles and certificate usage to BlackBerry UEM, consider the following guidelines:

Item	Considerations
Connectivity profiles	When BlackBerry Dynamics connectivity profiles are migrated, the values from the App servers tab are not migrated. The values are populated using the default values from the destination BlackBerry UEM server. When BlackBerry Dynamics connectivity profiles are migrated, 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.
Apps	If an app entitlement from the source server doesn't exist in the destination server, that app assignment is not migrated. The app group is migrated.
Certificate usage	Certificate usage is migrated, except for: • Certificate usages that already exist on the destination server • Non BlackBerry Dynamics apps

Complete policy and profile migration for BlackBerry Dynamics-activated users

After you migrate users, devices, groups, and other data to BlackBerry UEM, you must complete the following tasks on the destination BlackBerry UEM.

Rebuild the relationships between apps, policies, and users:

- Assign app configurations to BlackBerry Dynamics apps in groups.
- Assign connectivity profiles to groups.
- Assign migrated BlackBerry Dynamics policies to users.
- Set override profiles (BlackBerry Dynamics profiles and compliance profiles).

Complete the migrated connectivity profiles:

- Enter the app servers information.
- Set the BlackBerry Proxy clusters on the Infrastructure tab.

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

Optionally, you can migrate the IT policies, profiles, and groups from a source server.

1. On the menu bar, click **Settings**.
2. Click **Migration** > **IT policies, profiles, groups**.
3. Click **Next**.
4. Select the check boxes for the items that you want to migrate.

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

5. Click **Preview** to review the policies and profiles you selected.
6. Click **Migrate**.
7. To configure the IT policies, profiles, and groups, click **Configure IT policies and profiles** to go to the **Policies and Profiles** screen.

After you finish: On the destination server, create the policies and profiles that could not be migrated and assign them to users before you migrate devices.

Considerations: Migrating users from a source server

Keep the following things in mind when you migrate users to a destination BlackBerry UEM:

Item	Considerations
Maximum number to migrate	You can migrate a maximum of 1000 users at a time from a source. If you select more than the maximum number of users, only the maximum number are migrated to the destination BlackBerry UEM. The remaining users are skipped. Repeat the migration process as many times as necessary to migrate all the users from the source server. **Note:** If BlackBerry UEM times out while migrating 1000 users, try migrating fewer users.
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 BlackBerry UEM. These users do not appear in the list of users to migrate. • If two users in the source database have the same email address, only one user is displayed on the Migrate users screen.
Password	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.
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.

Migrate users from a source server

You can migrate users from a source server to the destination BlackBerry UEM. The users remain in both source and destination after the migration is complete.

1. On the menu bar, click **Settings > Migration > Users**.
2. On the **Migrate users** screen, click **Refresh cache**.

The cache can take approximately 10 minutes for each 1000 users to populate.

BlackBerry UEM caches the user data to increase the speed of searching capabilities, but the user data is migrated directly from the source. Refreshing the cache is mandatory only for the first set of users migrated and optional afterward.

3. Click **Next**.
4. Select the users to migrate.

   Only the first 20,000 users are displayed. Search on the user name or email address to locate specific users that may not be in the first 20,000. Selecting all selects only those users on the first page. Set the page size for the number of users that you want to select.

   If changes are made in the source after the cache is refreshed, those changes are not reflected in the cache data displayed. You should not make changes to the source server during migration, but if you do, refresh the cache periodically.
5. Click **Next**.
6. Assign one or more groups and assign an IT policy and one or more profiles to the selected users.

   For more information, see the Administration content.
7. Click **Preview**.
8. Click **Migrate**.

After you finish: Migrate devices from a source server.

Considerations: Migrating devices from a source server

Keep the following things in mind when migrating devices to a destination BlackBerry UEM:

Item	Considerations
Maximum number to migrate	You can migrate a maximum of 2000 devices at a time from a source server.
Destination BlackBerry UEM	Before you migrate devices verify that BlackBerry UEM supports the device type and OS.
Users	• The users must exist in the destination BlackBerry UEM domain. • You must migrate all of a user's devices at the same time.
Managed iOS devices	• iOS devices must have the latest version of the BlackBerry UEM Client installed. • iOS devices that are assigned an App lock profile can't be migrated because the BlackBerry UEM Client can't be opened for the migration • 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. **Note:** If you attempt to migrate without performing this step, the app is removed and the device may be unenrolled from BlackBerry UEM. However, even if you clear this check box, the app may still be removed during migration.
Managed Android devices	• Android Enterprise devices must have the latest version of the BlackBerry UEM Client installed. • You can't migrate Android devices that have a work profile using a Google account or Google domain.

Item	Considerations
Windows devices	You can't migrate Windows devices.
macOS devices	You can't migrate macOS devices.
MDM controls	Devices activated with "MDM controls" temporarily lose access to email when the migration begins. Email services are restored when the migration is complete.
Groups	You can't migrate a device that belongs to a shared device group. These devices do not appear in the migration list.
BlackBerry Dynamics-enabled devices	**BlackBerry Dynamics apps** • All BlackBerry Dynamics apps compatible with migration are migrated. **BlackBerry Dynamics apps that are incompatible with migration are wiped when the administrator triggers the migration.** These apps must be reactivated on the destination BlackBerry UEM. • For migrations from an on-premises BlackBerry UEM source database, all BlackBerry Dynamics apps must be at BlackBerry Dynamics SDK version 8.0 or later. • 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. • Make sure that the user has entitlements for the app on the destination BlackBerry UEM. If the app doesn't have the entitlement, after migration, the user will receive a message that the app is blocked. • BlackBerry Dynamics apps are not migrated if the destination BlackBerry UEM already has apps registered for that user. • BlackBerry Access for Windows, BlackBerry Access for macOS, and BlackBerry Enterprise BRIDGE are not supported for migration. After the migration is complete, users must re-enroll these apps in UEM. • Custom apps migrate only if the source and destination servers have the same organization ID. It is possible to merge two organizations. For more information, visit support.blackberry.com/community to read article 47626. • Devices with BlackBerry Dynamics apps activated by multiple users should not be migrated. • BlackBerry Dynamics apps that are locked due to compliance or remotely by the administrator before the migration process may no longer function after migration and may need to be reactivated. If the BlackBerry UEM Client is locked, the user may not be migrated. • The migration process does not track or guarantee migration of the BlackBerry UEM Client and apps activated on a device after that device's data is cached. Administrators should refresh the user cache before each migration. **Device authentication** • The authentication delegate must be the same on the source server and the destination BlackBerry UEM. You can change the authentication delegate after migration.

Item	Considerations
	Device management • BlackBerry Dynamics-only devices (no BlackBerry UEM Client) are visible in the source database until all apps are migrated. • BlackBerry Dynamics-enabled devices are always enrolled for BlackBerry Dynamics on the destination server. **Operating system** • Devices with an unknown operating system are not migrated. **Chat sessions** • The source BEMS server may keep stale Connect chat sessions open for up to 24 hours so the user may temporarily appear to be logged into chat from two devices. • Unread Connect chat messages are deleted during migration. Users should log out of Connect before migration. **Users** • If a user has more than one device with BlackBerry Dynamics apps, all the devices are automatically selected for migration. **Unlock keys** • 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 BlackBerry UEM source. After the migration is complete the key must be obtained from the destination BlackBerry UEM. **After the migration is started** • iOS device users must swipe up to close apps. • 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. • Not all apps will appear on the launcher until the migration is complete. • After migration, app icon arrangements in the launcher are reset to the default. • Devices upload the VIP rules, bookmarks, and user certificates to the new 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:

- Before you migrate devices, verify that the appropriate policies and entitlements are assigned to the users that you've migrated.
- Notify iOS device users that they must open the BlackBerry UEM Client to start the migration to BlackBerry UEM and that they must keep the BlackBerry UEM Client open until the migration is complete.

1. On the menu bar, click **Settings > Migration > Devices**.
2. On the **Migrate devices** screen, click **Refresh cache**.

   The cache can take approximately 10 minutes for each 1000 devices to populate.

   BlackBerry UEM caches the device data to speed searching capabilities, but the device data is migrated directly from the source. Refreshing the cache is mandatory only for the first set of devices migrated and optional afterward.
3. Click **Next**.
4. Select the devices to migrate.

   Only the first 20,000 devices are displayed. Search on the user name or email address to locate specific users that may not be in the first 20,000. Selecting all selects only those devices on the first page. Set the page size for the number of devices that you want to select.

   Note: You may see fewer line items than number of devices because the cache is displayed by user and some users may have more than one device.

   If changes are made in the source after the cache is refreshed, those changes are not reflected in the cache data displayed. You should not make changes to the source server during migration, but if you do, refresh the cache periodically.
5. Click **Preview**.
6. Click **Migrate**.
7. To view the status of the devices being migrated, click **Migration** > **Status**.

Device migration quick reference

Device type	Activation type/Configuration	Migration
Android	• MDM controls • BlackBerry 2FA • User privacy • BlackBerry Dynamics (UEM to UEM)	Supported
Android Enterprise devices that have a work profile associated with a Google domain	Any	Not supported
Android Enterprise devices that have a work profile that is not associated with a Google account or Google domain	Any	Supported
Android Samsung Knox Workspace devices that have a work profile associated with a Google account or Google domain	Any	Not supported

Device type	Activation type/Configuration	Migration
Android Samsung Knox Workspace devices that have a work profile that is not associated with a Google account or Google domain	Any	Supported
iOS	• MDM controls • Device registration for BlackBerry 2FA only • DEP devices that have the BlackBerry UEM Client installed • User privacy • BlackBerry Dynamics (UEM to UEM)	Supported
iOS	• DEP devices that don't have the BlackBerry UEM Client installed • User enrollment	Not supported
Windows	Any	Not supported
macOS	Any	Not supported

Migrating DEP devices

You can migrate iOS devices that are enrolled in Apple's Device Enrollment Program (DEP) from a source BlackBerry UEM database to another BlackBerry UEM database.

Note: The DEP enrollment configuration is not migrated and the devices will lose the enrollment configuration settings in the destination environment. For more information, visit support.blackberry.com to read KB 100525.

Migrate DEP devices that have the BlackBerry UEM Client installed

You can migrate iOS devices that are enrolled in Apple's Device Enrollment Program (DEP) and are activated with the MDM controls activation type.

Before you begin: In the app settings for the BlackBerry UEM Client, clear the **Remove the app from the device when the device is removed from BlackBerry UEM** check box.

Note: If you attempt to migrate without performing this step, the app is removed and the device may be unenrolled from BlackBerry UEM. However, even if you clear this check box, the app may still be removed during migration.

1. In the DEP portal, create a new virtual MDM server.
2. Connect the destination BlackBerry UEM instance to the new virtual MDM server. For more information, see Configuring BlackBerry UEM for DEP.

   Make sure that the DEP profile of the destination BlackBerry UEM instance matches the DEP profile of the source BES12 or BlackBerry UEM instance.
3. Move the DEP devices from the source virtual MDM server to the new virtual MDM server.

4. In the BlackBerry UEM management console, migrate the DEP devices from the source instance to the destination BlackBerry UEM instance.

After you finish:

Note: To trigger the migration on the device, the user should first open the app that is configured as the authentication delegate on the device.

Migrate DEP devices that do not have the BlackBerry UEM Client installed and are not BlackBerry Dynamics-enabled

iOS devices that are enrolled in Apple's Device Enrollment Program (DEP) and do not have BlackBerry UEM Client installed appear in the list of devices that are unsupported for migration.

1. In the DEP portal, create a new virtual MDM server.
2. Connect the destination BlackBerry UEM instance to the new virtual MDM server. For more information, see Configuring BlackBerry UEM for DEP.

   Make sure that the destination BlackBerry UEM instance has the same DEP profile as the source instance.
3. Move the DEP devices from the source virtual MDM server to the new virtual MDM server.
4. Perform a factory reset of each DEP device.
5. Reactivate each DEP device.

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