BlackBerry UEM

Configuration

12.18

Contents

Configuring BlackBerry UEM for the first time..... 7
Administrator permissions required to configure BlackBerry UEM.....8
Obtaining and activating licenses.....8

Changing BlackBerry UEM certificates.....9
Considerations for changing BlackBerry Dynamics certificates..... 10
Change a BlackBerry UEM certificate.....11

Configuring BlackBerry UEM to send data through a proxy server..... 13
Sending data through a TCP proxy server to the BlackBerry Infrastructure.....13
Comparing TCP proxies..... 14
Configure BlackBerry UEM to use a transparent TCP proxy server.....14
Enable SOCKS v5 on a TCP proxy server.....14

Configuring connections through internal proxy servers..... 16
Configure server-side proxy settings.....16

Connecting to your company directories.....17
Configuring Microsoft Active Directory authentication in an environment that includes Exchange linked mailboxes.....17
Connect to a Microsoft Active Directory instance..... 18
Connect to an LDAP directory..... 19
Enable directory-linked groups.....21
Enabling onboarding..... 21
Enable and configure onboarding and offboarding..... 22
Synchronize a company directory connection.....23
Preview a synchronization report.....23
View a synchronization report.....23
Add a synchronization schedule..... 24
Removing a connection to a company directory.....25

Connecting to an SMTP server to send email notifications.....26
Connect to an SMTP server to send email notifications.....26

Configuring database mirroring.....27
Steps to configure database mirroring..... 27
Prerequisites: Configuring database mirroring.....27
Create and configure the mirror database.....28
Connect BlackBerry UEM to the mirror database.....28
Configuring a new mirror database.....29

Connecting BlackBerry UEM to Microsoft Azure..... 30
Create a Microsoft Azure account..... 30
Synchronize Microsoft Active Directory with Microsoft Azure.....30
Create an app registration in Azure..... 31
Configuring Azure Active Directory conditional access.....32
Configure BlackBerry UEM as a Compliance Partner in Azure..... 32
Configure Azure Active Directory conditional access.....33
Configure the BlackBerry Dynamics connectivity profile to support the Azure Conditional Access feature.....33
Assign the Feature - Azure conditional access app to users.....33
Configure a BlackBerry Dynamics Profile.....34
Remove devices from Azure Active Directory conditional access.....34

Enable access to the BlackBerry Web Services over the BlackBerry Infrastructure.....36

Obtaining an APNs certificate to manage iOS and macOS devices..... 37
Obtain a signed CSR from BlackBerry.....37
Request an APNs certificate from Apple.....37
Register the APNs certificate.....38
Renew the APNs certificate..... 38
Troubleshooting APNs.....39
The APNs certificate does not match the CSR. Provide the correct APNs file (.pem) or submit a new CSR..... 39
I get "The system encountered an error" when I try to obtain a signed CSR.....39
I cannot activate iOS or macOS devices..... 39

Configuring BlackBerry UEM for DEP..... 40
Create a DEP account.....40
Download a public key.....40
Generate a server token..... 41
Register the server token with BlackBerry UEM..... 41
Add the first enrollment configuration..... 41
Update the server token..... 43
Remove a DEP connection.....43

Configuring BlackBerry UEM to support Android Enterprise devices.....44
Configure BlackBerry UEM to support Android Enterprise devices.....45
Remove the connection to your Google domain.....46
Remove the Google domain connection using your Google account.....46
Edit or test the Google domain connection.....47

Extending the management of Chrome OS devices to BlackBerry UEM.....48
Setting up management of Chrome OS devices if you have already configured BlackBerry UEM to use Android Enterprise..... 48

Create a service account that BlackBerry UEM uses to authenticate with your Google Cloud or Google Workspace by Google domain....48
Enable additional APIs to allow BlackBerry UEM to sync the Chrome OS data....49
Integrate BlackBerry UEM with your Google Cloud or Google Workspace by Google domain so you can use Chrome OS devices....50
Synchronize BlackBerry UEM with the Google admin console....51

Simplifying Windows 10 activations....52
Integrating UEM with Azure Active Directory join....52
Integrate UEM with Azure Active Directory join....53
Configuring Windows Autopilot in Microsoft Azure....54
Create a Windows Autopilot deployment profile in Azure....54
Import Windows Autopilot devices to Azure....54
Deploy a discovery service to simplify Windows 10 activations....55

Migrating users, devices, groups, and other data from a source server....57
Prerequisites: Migrating users, devices, groups, and other data from a source server....57
Connect to a source server....59
Export the self-signed root certificate for the Good Control server....61
Considerations: Migrating IT policies, profiles, and groups from a source server....62
Migrate IT policies, profiles, and groups from a source server....64
Complete policy and profile migration for BlackBerry Dynamics-activated users....64
Good Control features in BlackBerry UEM....65
Considerations: Migrating users from a source server....66
Migrate users from a source server....67
Considerations: Migrating devices from a source server....68
Device migration quick reference....72
Migrate devices from a source server....73
Migrating DEP devices....74
Migrate DEP devices that have the BlackBerry UEM Client installed....74
Migrate DEP devices that do not have the BlackBerry UEM Client installed and are not BlackBerry Dynamics-enabled....74

Configuring BlackBerry UEM to support BlackBerry Dynamics apps....75
Manage BlackBerry Proxy clusters....75
Configure Direct Connect using port forwarding....76
Configure BlackBerry Dynamics properties....76
BlackBerry Dynamics global properties....77
BlackBerry Dynamics properties....81
BlackBerry Proxy properties....81
Configure communication settings for BlackBerry Dynamics apps....83
Sending BlackBerry Dynamics app data through an HTTP proxy....83
PAC file considerations....83
Configure BlackBerry Dynamics app proxy settings....84
BlackBerry Dynamics connectivity and routing behavior....85
Default routing....85
Example routing scenarios....86
BlackBerry Dynamics data flow....89
Configuring Kerberos for BlackBerry Dynamics apps....89
Domains, realms, and forests....90

Prerequisites for configuring Kerberos for BlackBerry Dynamics apps..... 92
Configure Kerberos Constrained Delegation..... 93
Troubleshooting and diagnostics..... 95
Configuring Kerberos PKINIT..... 96
Connect BlackBerry UEM to a BlackBerry Dynamics PKI connector..... 96

Integrating BlackBerry UEM with Cisco ISE..... 98
Requirements: Integrating BlackBerry UEM with Cisco ISE..... 98
Create an administrator account that Cisco ISE can use..... 99
Add the BlackBerry Web Services certificate to the Cisco ISE certificate store..... 100
Connect BlackBerry UEM to Cisco ISE..... 100
Example: Authorization policy rules for BlackBerry UEM..... 101
Managing network access and device controls using Cisco ISE..... 102
Redirecting devices that are not activated on BlackBerry UEM..... 103

Legal notice..... 104

Configuring BlackBerry UEM for the first time

The following table summarizes the initial configuration tasks covered in this guide. Use this table to determine which configuration tasks you should complete. After you complete the appropriate tasks, you are ready to set up administrators, create and manage users and groups, set up device controls, and activate devices.

Task	Description
Replace default certificates with trusted certificates	You can replace the default self-signed certificates used by BlackBerry UEM to authenticate communication between various UEM components and with devices.
Configure BlackBerry UEM to send data through a proxy server	You can configure BlackBerry UEM to send data through a TCP proxy server before it reaches the BlackBerry Infrastructure. You can also configure BlackBerry UEM to send data through an HTTP proxy before it reaches the BlackBerry Dynamics NOC.
Configure connections through internal proxy servers	If your organization uses a proxy server for connections between servers inside your network, you may need to configure server-side proxy settings to allow the BlackBerry UEM Core to communicate with remote instances of the management console.
Connect BlackBerry UEM to company directories	You can connect BlackBerry UEM to one or more company directories, such as Microsoft Active Directory or an LDAP directory, so that BlackBerry UEM can access user data to create user accounts.
Connect BlackBerry UEM to an SMTP server	If you want BlackBerry UEM to send activation emails and other notifications to users, you must specify the SMTP server settings that BlackBerry UEM can use.
Configure database mirroring	To retain database service and data integrity if issues occur with the BlackBerry UEM database, you can install and configure a failover database that serves as a backup to the principal database.
Connect BlackBerry UEM to Microsoft Azure	If you want to use BlackBerry UEM to deploy iOS and Android apps managed by Microsoft Intune or if you want to manage Windows 10 apps in BlackBerry UEM, connect BlackBerry UEM to Microsoft Azure.
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 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 to support Android Enterprise devices	To support Android Enterprise devices, you need to configure your Google Workspace or Google Cloud domain to support third-party mobile device management providers and configure BlackBerry UEM to communicate with your Google Workspace or Google Cloud domain.

Task	Description
Configure your network to simplify Windows 10 activations	You can simplify the process for activating Windows 10 devices by making configuration changes to your network so that users don't need to type a server address.
Migrating users, devices, groups, and other data from a source server	You can use the management console to migrate users, devices, groups, and other data from a source on-premises BlackBerry UEM or Good Control (standalone).
Configure BlackBerry Dynamics settings	You can configure settings that are specific to BlackBerry Proxy and BlackBerry Dynamics apps.
Integrate BlackBerry UEM with Cisco ISE	You can create a connection between Cisco ISE and BlackBerry UEM so that Cisco ISE can retrieve device data from BlackBerry UEM and enforce network access control policies.

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 Using the BlackBerry UEM management console in the Administration content.

If you create additional administrator accounts to configure 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.

Changing BlackBerry UEM certificates

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

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

You can change the following certificates:

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

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

Considerations for changing BlackBerry Dynamics certificates

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

Add new certificates to any peripheral equipment

If you have added any BlackBerry Dynamics certificates to peripheral equipment on your network, add the new certificate to peripheral equipment before adding it to BlackBerry UEM

Update BlackBerry Dynamics apps

If you are replacing the BlackBerry Dynamics certificate for application management or Direct Connect, ensure that users' BlackBerry Dynamics apps are updated to the most recent versions before you replace the certificate.

Any BlackBerry Dynamics apps developed by your organization must be built with version 3.2 or later of the BlackBerry Dynamics SDK. Older apps can't receive the new certificate from BlackBerry UEM.

BlackBerry Dynamics apps must be open to receive a certificate

Users must open a BlackBerry Dynamics app for the app to receive a certificate from BlackBerry UEM. If you are replacing the BlackBerry Dynamics certificate for application management or Direct Connect and the change becomes effective before BlackBerry UEM pushes the certificate to all BlackBerry Dynamics apps, any apps that did not receive the certificate must be reactivated. Apps do not receive certificates while they are suspended on iOS devices or while Android devices are in Doze mode.

Ensure the BlackBerry Connectivity Node is accessible

If any BlackBerry Proxy instances are unreachable by BlackBerry UEM when BlackBerry Dynamics certificates are replaced, BlackBerry Dynamics apps will not be able to connect to those instances following the certificate replacement.

Schedule certificate changes appropriately

If you are replacing the certificate for BlackBerry Dynamics servers, choose a period of low activity to restart the servers.

Allow sufficient time for new certificates to propagate to BlackBerry Proxy and BlackBerry Dynamics apps. If you are replacing only the certificate for BlackBerry Dynamics servers, allow at least 10 minutes before the server restarts.

If you are replacing the BlackBerry Dynamics certificate for application management or Direct Connect, it is recommended that the time until the effective date be longer than the Connectivity verification "Last contact time" setting in the compliance profile.

If you are replacing both the BlackBerry Dynamics certificates for application management and Direct Connect, set the effective times at least 30 minutes apart. If you have a large number of users and BlackBerry Dynamics apps, you should wait longer than 30 minutes between each certificate.

Change a BlackBerry UEM certificate

Before you begin:

- Obtain a certificate signed by a trusted CA. The certificate must be in a keystore format (.pfx, .pkcs12), and must be encrypted with the TripleDES-SHA1 encryption type. For more information, visit support.blackberry.com to read KB 69494.
- If you are replacing the BlackBerry Dynamics certificate for application management or Direct Connect, ensure that users' BlackBerry Dynamics apps are updated to the most recent versions first.

1. On the menu bar, click **Settings > Infrastructure > Server certificates**.
2. In the section for the certificate that you want to replace, click **View details**.
3. Click **Replace certificate**.
4. Browse to the certificate file and select it.
5. Enter an encryption password for the certificate.
6. If you are replacing the certificate for BlackBerry Dynamics servers, specify when you want BlackBerry UEM to restart to make the change effective.

   It is recommended that you choose a period of low activity to restart the servers.
7. If you are replacing the BlackBerry Dynamics certificate for application management or Direct Connect, specify the effective date for the certificate change.

   It is recommended that the effective date be further away than the Connectivity verification "Last contact time" setting in the compliance profile. If you are changing more than one certificate, you should separate the effective times by at least 30 minutes. Note that there is no prompt for the effective date when the new certificate is issued by the same CA as the previous certificate. For more information, visit support.blackberry.com/community to read article 74167.
8. Click **Replace**.

After you finish:

- If you replaced any of the certificates on the **Server certificates** tab, restart the BlackBerry UEM Core service on all servers. It is recommended that you choose a period of low activity to restart the servers.
- For certificates on the BlackBerry Dynamics certificates tab, you can click **Revert to default** to switch back to using a self-signed certificate.
- On the BlackBerry Dynamics certificates tab, you can clear the **Trust BlackBerry UEM CA** and **Trust BlackBerry Dynamics CA** check boxes if you have no further need to trust the self-signed certificates. You can clear the

Trust BlackBerry Dynamics CA check box only if you have replaced all of the certificates on the BlackBerry Dynamics certificates tab.

- If BlackBerry Dynamics apps stop communicating after you change the certificates, ensure that the apps are up to date and then instruct users to reactivate the apps.

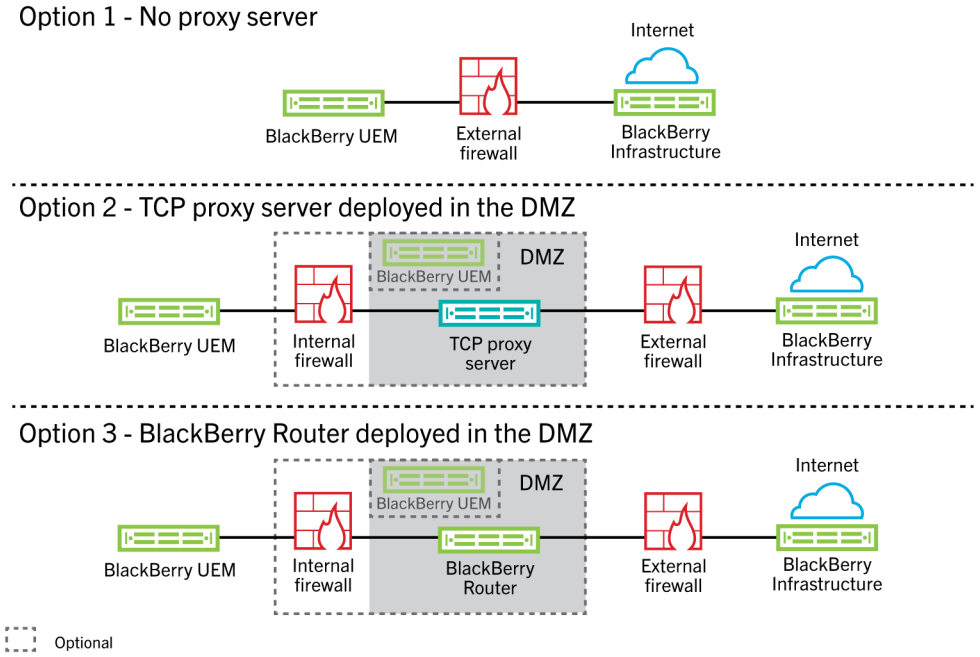
Configuring BlackBerry UEM to send data through a proxy server

You can configure BlackBerry UEM to send data through a TCP proxy server before it reaches the BlackBerry Infrastructure.

By default, BlackBerry UEM connects directly to the BlackBerry Infrastructure using port 3101. If your organization's security policy requires that internal systems cannot connect directly to the Internet, you can install a TCP proxy server. The TCP proxy server acts as an intermediary between BlackBerry UEM and the BlackBerry Infrastructure.

You can install a proxy server outside your organization's firewall in a DMZ. Installing a TCP proxy server in a DMZ provides an extra level of security for BlackBerry UEM. Only the proxy server connects to BlackBerry UEM from outside the firewall. All connections to the BlackBerry Infrastructure between BlackBerry UEM and devices go through the proxy server.

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

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

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. On the menu bar, click **Settings > Infrastructure > BlackBerry Router and proxy**.
2. Select the **Proxy server** option.
3. Perform any of the following tasks:

Task	Steps
Route TCP data through a TCP proxy server.	In the **BlackBerry UEM Core, BlackBerry Secure Gateway Service** fields, type the FQDN or IP address and the port number of the proxy server. Each field requires a single value.
Route BlackBerry Secure Connect Plus traffic through a TCP proxy server.	In the **BlackBerry Secure Connect Plus** fields, type the FQDN or IP address and the port number of the proxy server. Each field requires a single value.

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. On the menu bar, click **Settings > Infrastructure > BlackBerry Router and 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**.

Configuring connections through internal proxy servers

If your organization uses a proxy server for connections between servers inside your network, you may need to configure server-side proxy settings to allow BlackBerry UEM Core to communicate with the BlackBerry UEM management console if it is installed on a separate computer. You may also need to configure server-side proxy settings to allow BlackBerry UEM to communicate with other internal services, such as certification authorities and servers hosting push applications that push data.

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

Configure server-side proxy settings

Before you begin: Make sure you have the PAC URL or host name and port number and any other settings that you need to connect to the proxy server.

1. On the menu bar, click **Settings > Infrastructure > Server-side proxy**.
2. If most or all of the servers that are part of your BlackBerry UEM installation must connect to a proxy server, perform the following actions to set global server-side proxy settings:
   a) Under **Global server-side proxy settings**, in the **Type** list, select **PAC Configuration** or **Manual Configuration**
   b) Specify the settings required by the proxy server and click **Save**.
3. If one or more servers require proxy settings that are different from the global settings, perform the following actions to set the proxy settings for the server:
   a) Under the server name, in the **Type** list, select **None**, **PAC Configuration**, or **Manual Configuration**.
   b) If you selected **PAC Configuration** or **Manual Configuration**, specify the settings required by the proxy server.
   c) Click **Save**.

Connecting to your company directories

You can connect BlackBerry UEM to your company directory so that it can access the list of users in your organization. You can connect BlackBerry UEM to multiple directories and the directories can be a combination of both Microsoft Active Directory and LDAP.

When your company directory is connected, you can take advantage of the following features:

- You can create user accounts in BlackBerry UEM using user data from the directory, and BlackBerry UEM can authenticate administrators for the management console and users for BlackBerry UEM Self-Service.
- You can link company directory groups with BlackBerry UEM groups to organize users in BlackBerry UEM the same way that they are organized in your company directory. See Enable directory-linked groups.
- You can enable onboarding for specific groups in your company directory to create BlackBerry UEM users automatically. If you enable onboarding, you can also configure offboarding to delete device data or user accounts when users are removed from groups in your company directory. See Enabling onboarding.

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

To connect BlackBerry UEM to a company directory, perform the following actions:

Step	Action
1	Create a connection to a Microsoft Active Directory instance or to an LDAP directory. If your environment includes a resource forest, see Configuring Microsoft Active Directory authentication in an environment that includes Exchange linked mailboxes.
2	Optionally, enable directory-linked groups.
3	Optionally, enable onboarding.
4	Optionally, add a synchronization schedule.

Configuring Microsoft Active Directory authentication in an environment that includes Exchange linked mailboxes

In a resource forest model, the Microsoft Exchange server is located in one forest (the resource forest) and individual user accounts are located in account forests. If your organization's environment includes a resource forest that is dedicated to running Microsoft Exchange, you can configure Microsoft Active Directory authentication for user accounts that are located in trusted account forests.

If an Exchange resource forest exists in your organization's environment, you must configure BlackBerry UEM to connect to the resource forest. You must create a mailbox in the resource forest for each user account and then associate these mailboxes with the user accounts. When you associate the mailboxes in the resource forest with user accounts in the account forests, the user accounts obtain full access to the mailboxes and the user accounts in the account forests are connected to the Microsoft Exchange server. BlackBerry UEM uses the mailboxes to look up the user accounts in the individual domains.

To authenticate users who log in to BlackBerry UEM, BlackBerry UEM must read the user information that is stored in the global catalog servers that are part of the resource forest. You must create a Microsoft Active Directory account for BlackBerry UEM that is located in a Windows domain that is part of the resource forest. When you create the directory connection, you provide the Windows domain, username, and password for the Microsoft Active Directory account, and, if required, the names of the global catalog servers that BlackBerry UEM can use.

For more information, visit technet.microsoft.com to read *Manage linked mailboxes*.

Connect to a Microsoft Active Directory instance

Before you begin: Create a Microsoft Active Directory account that BlackBerry UEM can use. The account must meet the following requirements:

- It must be located in a Windows domain that is part of the Microsoft Exchange forest.
- It must have permission to access the user container and read the user objects stored in the global catalog servers in the Microsoft Exchange forest.
- The password must be configured not to expire and does not need to be changed at the next login.
- If you enable single sign-on, constrained delegation must be configured for the account.
- The UEM server must also be joined to the Active Directory Domain.

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

    If you want to use global groups for onboarding, you must select **Yes**. To configure a global group domain, in the **List of global group domains** section, click +. In the **Domain** field select the domain that you want

to add. The default selection for the **Specify username and password?** field is No. If you keep this default selection, the username and password for the forest connection is used. If you select Yes, you must provide valid credentials for an Active Directory account in the domain that you selected. In the **KDC selection** field, you can select Automatic to permit UEM to automatically discover the key distribution centers, or Manual to specify the list of KDCs for UEM to use for authentication. Click **Add**.

12. If your environment contains a Microsoft Exchange resource forest, to enable support for linked Microsoft Exchange mailboxes, in the **Support for linked Microsoft Exchange mailboxes** drop-down list, click **Yes**.

    To configure the Microsoft Active Directory account for each forest that you want UEM to access, in the **List of account forests** section, click +. Specify the user domain name (the user may belong to any domain in the account forest), and the username and password. If necessary, specify the KDCs that you want UEM to search. If necessary, specify the global catalog servers that you want UEM to access. Click **Add**.
13. To enable single sign-on, select the **Enable Windows single sign-on** check box. For more information about single sign-on, see Configuring single sign-on for BlackBerry UEM in the Administration content. Single-sign on is supported only in an on-premises environment.
14. To synchronize more user details from your company directory, select the **Synchronize additional user details** check box. The additional details include company name and office phone.
15. Click **Save**.
16. Click **Close**.

After you finish: If you want to add a directory synchronization schedule, see Add a synchronization schedule.

Connect to an LDAP directory

Before you begin:

- Create an LDAP account for BlackBerry UEM that is located in the relevant LDAP directory. The account must meet the following requirements:
  - The account has permission to read all users in the directory.
  - The account's password never expires and the user is not required to change the password at next login.
- If the LDAP connection is SSL encrypted, make sure that you have the server certificate for the LDAP connection and that the LDAP server supports TLS 1.2. If SSL is enabled, the LDAP connection to BlackBerry UEM must use TLS 1.2.
- Verify the LDAP attribute values that your organization uses (the steps below give examples for typical attribute values). You must specify the LDAP attribute values at step 11 and on.

1. On the menu bar, click **Settings > External integration > Company directory**.
2. Click **Add an LDAP connection**.
3. In the **Directory connection name** field, type a name for the directory connection.
4. In the **LDAP server discovery** drop-down list, perform one of the following actions:
   - To automatically discover the LDAP server, click **Automatic**. In the **DNS domain name** field, type the domain name for the server that hosts the company directory.
   - To specify a list of LDAP servers, click **Select server from list below**. In the **LDAP server** field, type the name of the LDAP server. To add more LDAP servers, click +.
5. In the **Enable SSL** drop-down list, perform one of the following actions:
   - If the LDAP connection is SSL encrypted, click **Yes**. Beside the **LDAP server SSL certificate** field, click **Browse** and select the LDAP server certificate.
   - If the LDAP connection is not SSL encrypted, click **No**.

6. In the **LDAP Port** field, type the TCP port number for communication. The default values are 636 for SSL enabled or 389 for SSL disabled.
7. In the **Authorization required** drop-down list, perform one of the following actions:
   - If authorization is required for the connection, click **Yes**. In the **Login** field, type the DN of the user that is authorized to log in to LDAP (for example, an=admin,o=Org1). In the **Password** field, type the password.
   - If authorization is not required for the connection, click **No**.
8. In the **User Search base** field, type the value to use as the base DN for user information searches.
9. In the **LDAP user search filter** field, type the LDAP search filter that is required to find user objects in your organization's directory server. For example, for an IBM Domino Directory, type `(objectClass=Person)`.

   Note: If you want to exclude disabled user accounts from search results, type `(&(objectclass=user)(logindisabled=false))`.
10. In the **LDAP user search scope** drop-down list, perform one of the following actions:
    - To search all objects following the base object, click **All levels**. This is the default setting.
    - To search objects that are one level directly following the base DN, click **One level**.
11. In the **Unique identifier** field, type the name of the attribute that uniquely identifies each user in your organization's LDAP directory (must be a string that is immutable and globally unique). For example, `dominoUNID` in IBM Domino LDAP 7 and later.
12. In the **First name** field, type the attribute for each user's first name (for example, `givenName`).
13. In the **Last name** field, type the attribute for each user's last name (for example, `sn`).
14. In the **Login attribute** field, type the login attribute to use for authentication (for example, `uid`).
15. In the **Email address** field, type the attribute for each user's email address (for example, `mail`). If you do not set the value, a default value is used.
16. In the **Display name** field, type the attribute for each user's display name (for example, `displayName`). If you do not set the value, a default value is used.
17. In the **Email profile account name** field, type the attribute for each user's email profile account name (for example, `mail`).
18. In the **User Principal Name** field, type the user principal name for SCEP (for example, `mail`).
19. To enable directory-linked groups for the directory connection, select the **Enable directory-linked groups** check box.

    Specify the following information:
    - In the **Group search base** field, type the value to use as the base DN for group information searches.
    - In the **LDAP group search filter** field, type the LDAP search filter that is required to find group objects in your company directory. For example, for IBM Domino Directory, type `(objectClass=dominoGroup)`.
    - In the **Group Unique Identifier** field, type the attribute for each group's unique identifier. This attribute must be immutable and globally unique (for example, type `cn`).
    - In the **Group Display name** field, type the attribute for each group's display name (for example, type `cn`).
    - In the **Group Membership attribute#** field, type the name of the attribute for group membership. The attribute values must be in DN format (for example, `CN=jsmith,CN=Users,DC=example,DC=com`).
    - In the **Test Group Name#** field, type an existing group name for validating the group attributes specified.
20. Click **Save**.
21. Click **Close**.

After you finish: If you want to add a directory synchronization schedule, see Add a synchronization schedule.

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 Creating directory-linked groups in 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**.

Removing a connection to a company directory

If you remove a connection to a company directory, all users that were added to BlackBerry UEM from that company directory will be converted to local users. Once users are converted to local users they can't be converted back to directory linked users, even if you later re-add the company directory connection. Users will continue to function as local users but UEM will not be able to synchronize updates from the company directory such as changes to name, email address, and other attributes.

1. On the menu bar, click **Settings > External integration > Company directory**.
2. Click **X** beside the company directory entry that you want to remove.
3. Click **Delete**.

Connecting to an SMTP server to send email notifications

To allow BlackBerry UEM to send email notifications, you must connect UEM to an SMTP server.

You can use email notifications from UEM to send activation instructions, device compliance warnings, passwords for UEM Self-Service, and messages to individual users. You cannot send this information as email messages if you don't connect to an SMTP server, but you can still configure UEM to send compliance warnings directly to devices.

Connect to an SMTP server to send email notifications

1. On the menu bar, click **Settings > External integration > SMTP server**.
2. Click ✎.
3. In the **Sender display name** field, type a name to use for BlackBerry UEM email notifications. For example, `donotreply` or `BUEM Admin`.
4. In the **Sender address** field, type the email address you want BlackBerry UEM to use to send email notifications.
5. In the **SMTP server** field, type the FQDN of the SMTP server. For example, `mail.example.com`.
6. In the **SMTP server port** field, type the SMTP server port number. The default port number is 25.
7. In the **Supported encryption type** drop-down menu, select the encryption type you want to apply to email messages.
8. If the SMTP server requires authentication, in the **Username** field, type the SMTP server login name. In the **Password** field, type the SMTP server password.
9. If necessary, import an SMTP CA certificate:
   a) Copy the SSL certificate file for your organization's SMTP server to the computer that you are using.
   b) Click **Browse**.
   c) Browse to the SSL certificate file and click **Upload**.
10. Click **Save**.

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

Configuring database mirroring

You can use database mirroring to provide high availability for the BlackBerry UEM database. Database mirroring is a Microsoft SQL Server feature that allows you to retain database service and data integrity if issues occur with the BlackBerry UEM database. For more information about using database mirroring, see the Planning content.

Note: Microsoft plans to deprecate database mirroring in future versions of Microsoft SQL Server, and recommends using the AlwaysOn feature for database high availability. Using AlwaysOn requires configuration steps before you install BlackBerry UEM. For more information about using AlwaysOn, see the Planning content.

Steps to configure database mirroring

To configure database mirroring, perform the following actions:

Step	Action
1	Review the requirements in the Planning content and verify that the BlackBerry UEM domain meets the prerequisites.
2	Create and configure the mirror database.
3	Connect BlackBerry UEM to the mirror database.

Prerequisites: Configuring database mirroring

- Configure the principal server and mirror server to permit access from remote computers.
- Configure the principal server and mirror server to have the same permissions.
- Set up a witness server that you will use to monitor the principal server.
- Configure the Microsoft SQL Server Agent to use a domain user account with the same local administrative permissions as the Windows account that runs the BlackBerry UEM services.
- Verify that the domain user account has permissions for both the principal server and mirror server.
- Verify that the DNS server is running.
- On each computer that hosts a BlackBerry UEM database instance, in the SQL Server 2012 Native Client, turn off the Named Pipes option. If you choose to not turn off the Named Pipes option, visit https://support.blackberry.com/community to read article 34373.
- To review additional prerequisites for your organization's version of Microsoft SQL Server, visit technet.microsoft.com/sqlserver to read Database Mirroring - SQL Server 2012 or Database Mirroring - SQL Server 2014.
- If the mirror database uses the default instance, the BlackBerry UEM components can connect to the mirror database using the default port 1433 only, not a custom static port. This is due to a limitation of Microsoft SQL Server 2005 and later. For more information about this issue, see SQL 2005 JDBC Driver and Database Mirroring.

Create and configure the mirror database

Before you begin: To maintain database integrity while you create and configure the mirror database, stop the BlackBerry UEM services on every computer that hosts a BlackBerry UEM instance.

1. In Microsoft SQL Server Management Studio, browse to the principal database.
2. Change the **Recovery Model** property to **FULL**.
3. In the query editor, run the **-- ALTER DATABASE** *<BUEM_db>* **SET TRUSTWORTHY ON** query, where *<BUEM_db>* is the name of the principal database.
4. Back up the principal database. Change the **Backup type** option to **Full**.
5. Copy the backup files to the mirror server.
6. On the mirror server, restore the database to create the mirror database. When you restore the database, select the **NO RECOVERY** option.
7. Verify that the name of the mirror database matches the name of the principal database.
8. On the principal server, in Microsoft SQL Server Management Studio, right-click the principal database and select the **Mirror** task. On the **Mirroring** page, click **Configure Security** to launch the Configure Database Mirroring Security wizard.
9. Start the mirroring process. For more information, see Setting Up Database Mirroring – SQL Server 2012 or Setting Up Database Mirroring – SQL Server 2014.
10. To enable automatic failover, add a witness to the mirroring session. For more information, see Database Mirroring Witness – SQL Server 2012 or Database Mirroring Witness – SQL Server 2014.

After you finish:

- To verify that failover works correctly, manually fail over service to the mirror database and back to the principal database.
- Restart the BlackBerry UEM services on every computer that hosts a BlackBerry UEM instance.
- Connect BlackBerry UEM to the mirror database.

Connect BlackBerry UEM to the mirror database

You must repeat this task on every computer that hosts a BlackBerry UEM instance.

Before you begin:

- Create and configure the mirror database.
- Verify that the mirror server is running.
- You can complete this task using the BlackBerry UEM Configuration Tool, or you can update the database properties file manually using the instructions below. If you want to use the BlackBerry UEM Configuration Tool, visit support.blackberry.com/community to read article KB36443. In the "Updating the BlackBerry UEM database properties" section, follow the instructions to enable SQL mirroring and provide the FQDN of the mirror server.

1. On the computer that hosts the BlackBerry UEM instance, navigate to *<drive>*:\Program Files\BlackBerry\UEM\common-settings.
2. In a text editor, open **DB.properties**.
3. In the section **optional settings to use failover**, after **configuration.database.ng.failover.server=**, type the FQDN of the mirror server (for example, `configuration.database.ng.failover.server=mirror_server.domain.net`).
4. If necessary, perform one of the following actions:

- If you specified a named instance for the principal database during installation, and the mirror database uses the default instance, delete the value after **configuration.database.ng.failover.instance=**.
- If the principal database uses a default instance and the mirror database uses a named instance, after **configuration.database.ng.failover.instance=**, type the named instance.

5. Save and close **DB.properties**.

After you finish:

- Restart the BlackBerry UEM services.
- Repeat this task on every computer that hosts a BlackBerry UEM instance.
- Verify that each computer that hosts a BlackBerry UEM instance can connect to the mirror server using the server shortname.

Configuring a new mirror database

If you create and configure a new mirror database after a role switch has occurred (that is, the BlackBerry UEM components failed over to the existing mirror database and the existing mirror database became the principal database), repeat Connect BlackBerry UEM to the mirror database on each computer that hosts a BlackBerry UEM instance.

Connecting BlackBerry UEM to Microsoft Azure

Microsoft Azure is the Microsoft cloud computing service for deploying and managing applications and services. You must connect UEM to Azure if you want to use UEM to deploy iOS and Android apps managed by Microsoft Intune, if you want to use Azure Active Directory conditional access, or if you want to manage Windows 10 apps in UEM.

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

Step	Action
1	Create a Microsoft Azure account.
2	Synchronize Microsoft Active Directory with Microsoft Azure.
3	Create an app registration in Azure.
4	Configure UEM to synchronize with Microsoft Intune or the Windows Store for Business.
5	Optionally, Configuring 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.

After you finish: Synchronize Microsoft Active Directory with Microsoft Azure.

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. 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 app registration in Azure

Create an app registration in Azure

To provide BlackBerry UEM access to Microsoft Azure, you must create an app registration within Azure that allows UEM to authenticate with Azure. For more information, see Register an application with the Microsoft identity platform.

If you are connecting UEM to both Microsoft Intune and the Windows Store for Business, use a different app registration 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, see KB75773.

Before you begin: Verify 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 into a text file.

   This is the **Client ID** required in UEM.
9. If you are creating the application to use Microsoft Intune, in the **Manage** section, click **API permissions**. 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**. 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. In the **Manage** 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 in UEM.

    Note: 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 UEM to synchronize with Microsoft Intune or 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 more than one UEM tenant for each Azure tenant. However, all UEM tenants will share the same Partner compliance management entry. Microsoft Azure will not be able to differentiate which UEM tenant a compliance status update originates from.

Note: BlackBerry Work does not support the Azure AD conditional access compliance feature. For more information, see KB 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, see KB 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.

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 Azure Conditional Access** 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 Azure Conditional Access feature

In the 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. Specify the following server settings.

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

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**.
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 information, see Add an iOS app to the app list and Add an Android app to the app list. 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. Users 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**.

Enable access to the BlackBerry Web Services over the BlackBerry Infrastructure

If your organization uses a web service client that is outside of the organization's firewall and the client requires access to the BlackBerry Web Services APIs (REST or legacy SOAP), the client can connect to the APIs securely over the BlackBerry Infrastructure. For more information about enabling this access in client apps, developers can see the Getting started section of the BlackBerry Web Services REST API Reference.

Web service clients can only use the BlackBerry Infrastructure to access the BlackBerry Web Services APIs if you enable this access in the management console. By default, this access is not enabled.

1. On the menu bar, click **Settings > General settings > BlackBerry Web Services access**.
2. Click **Enable**.
3. Click **Save**.

Obtaining an APNs certificate to manage iOS and macOS devices

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

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

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

It is a best practice to access the 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	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 (.plist). 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 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. Click +.
3. In the **Name** field, type a name for the account.
4. In step **1 of 4: Create an Apple DEP account**, click **Create an Apple DEP account**.
5. 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. In the preferences for your account, download the server token for the MDM server.

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. Do one of the following:
   - If you want UEM to automatically assign the enrollment configuration to devices when you register them in the Apple Device Enrollment Program, select the **Automatically assign all new devices to this configuration** checkbox.
   - If you want to use the UEM management console to manually assign the enrollment configuration to specific devices, do not select the **Automatically assign all new devices to this configuration** checkbox.
3. Optionally, type a department name and support phone number to be displayed on devices during setup.
4. In the **Device configuration** section, select any of the following options:
   - **Allow pairing**: Users can pair the device with a computer.
   - **Mandatory**: Users can activate devices using their company directory username and password.

- **Allow removal of MDM profile**: Users can deactivate devices.
- **Wait until device is configured**: Users cannot cancel the device setup until activation with UEM is complete.

5. In the **Skip during setup** section, select the items that you do not want to include in the device setup:

Option	Impact if selected
Passcode	Users are not prompted to create a device passcode.
Location services	Location services are disabled on the device.
Restore	Users cannot restore data from a backup file.
Move from Android	Data cannot be restored from an Android device.
Apple ID	Users are prevented from signing in to Apple ID and iCloud.
Terms and conditions	Users do not see the iOS terms and conditions.
Siri	Siri is disabled on devices.
Diagnostics	Diagnostic information is not automatically sent from the device during setup.
Biometric	Users cannot set up Touch ID.
Payment	Users cannot set up Apple Pay.
Zoom	Users cannot set up Zoom.
Home button setup	Users cannot adjust the Home button's click.
Screen Time	The option to set up Screen Time is skipped during DEP enrollment.
Software update	Users do not see the mandatory software update screen on the device.
iMessage and Face Time	Users do not see the iMessage and Face Time screen on the device.
Display tone	Users do not see the Display tone screen on the device.
Privacy	Users do not see the Privacy screen on the device.
Onboarding	Users do not see the informational onboarding screen on the device.
Watch migration	Users do not see the watch migration screen on the device.
SIM setup	Users do not see the screen to set up a cellular plan on the device.
Device-to-device migration	Users do not see the device-to-device migration screen on the device.

6. Click **Save**. If you selected **Automatically assign new devices to this configuration** click **Yes**.

After you finish: Activate iOS devices. For more information about activating devices that are enrolled in DEP, see Activating iOS devices that are enrolled for DEP.

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. In the preferences for your account, download the server token for the MDM server.
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 the name of a DEP account.
3. Click **Remove DEP connection**.
4. Click **Remove**.
5. 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 Google Workspace 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 Google Workspace domain	You have a Google Workspace domain in your organization	Google Workspace accounts (for organizations)	Supports all Google Workspace 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 Google Workspace 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 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 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 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, see KB 37748.

3. Do one of the following to specify how you want app configurations to be sent to a device:

- To send app configuration details using the BlackBerry Infrastructure, select **Send app configuration using UEM Client**.
- To send app configurations details using the Google infrastructure, select **Send app configuration using Google Play**.

4. When prompted, click **Accept** to accept the permissions set for some or all of the 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 Google Workspace 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 Google Workspace domain

If you do not remove the connection to your Google domain, you may be unable to connect your Google Cloud or Google Workspace 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.

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 the following source servers:

- BlackBerry UEM (on-premises)
- Good Control (standalone)

Note: If you want to migrate users, devices, groups, and other data from a BES10 source server, you must migrate to BlackBerry UEM version 12.9, then upgrade to BlackBerry UEM version 12.11, and then upgrade to version 12.14, and then upgrade to version 12.16. Direct migration from BES10 to BlackBerry UEM version 12.10 and later is not supported.

Note: For information about migrating BlackBerry Dynamics users and devices in batches using .csv files, visit support.blackberry.com/community to read article 49442.

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, or from a Good Control source server, 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: • The BlackBerry UEM instance you are migrating data from must be version 12.16 or later. • The Good Control (standalone) instance that you are migrating data from must be at version 5.0 or later.
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.
Defragment the databases (BlackBerry UEM)	Defragment the source databases and the destination BlackBerry UEM database (if one exists) before you begin migration. If you are migrating a large number of users, you should defragment the destination BlackBerry UEM database after you migrate each set of users. For more information about defragmenting a Microsoft SQL Server database, visit www.technet.microsoft.com to read the article "Reorganize and Rebuild Indexes."
BlackBerry UEM Client	For migrations of BlackBerry Dynamics-enrolled BlackBerry UEM Clients and BlackBerry Dynamics apps from an on-premises BlackBerry UEM source database, the latest BlackBerry UEM Client must be installed on the device.
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 7.1 or later. You can find the SDK version in the release notes for the app. For migrations from a Good Control (standalone) instance, all apps must be at BlackBerry Dynamics SDK version 4.0.0 or later. To determine the version of SDK used for the apps to be migrated, run the container activity report on Good Control. **BlackBerry Dynamics apps that are not supported for migration are wiped from the device when the administrator starts the migration.**

Prerequisite	Details
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 1433 (TCP) and port 1434 (UDP) are unblocked on the Microsoft SQL Server.

Connect to a source server

You must connect BlackBerry UEM to the source server that you are migrating data from. You can add multiple sources, but only one source at a time can be the active source.

Note: Make sure that the database account associated with the credentials that you use to log in to the database has write permissions.

Note: If you upgraded your source BlackBerry UEM server since the last time you performed a migration, you should delete and recreate the source server configuration before you perform another migration.

1. On the menu bar, click **Settings > Migration > Configuration**.
2. Click +.
3. In the **Source type** drop-down list, select the type of source server.
4. Depending on the type of source server that you selected, fill out the fields as follows:

Source server type	Field	Content
BlackBerry UEM	Display name	Type a descriptive name for the source server.

Source server type	Field	Content
	Database server	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.
	Database authentication type	Select the type of authentication you use to connect to the source database.
	SQL username SQL password	If you selected SQL authentication, in the SQL username and SQL password fields, type your login information to connect to the source database.
	Database name	Type the name of the source database.
	Source UEM authentication type	Select the authentication type that is used to log in to the source BlackBerry UEM management console.
	Username Password	Type your login information to log in to the source management console.
	Domain	If you selected Microsoft Active Directory authentication, type the name of the domain where the source management console is located.
Good Control (standalone)	Display name	Type a descriptive name for the source server.
	Source Good Control (standalone) host name	Type the FQDN of the Good Control management console.
	Source Good Control (standalone) certificate	Upload the Good Control CA root certificate to establish SSL connections. The certificate file must be in CER format. For instructions, see Export the self-signed root certificate for the Good Control server.

Source server type	Field	Content
	Username Password	Type your login information to log in to the administrator account for the source management console. **Note:** These credentials must correspond to a Good Control administrator with the access rights MANAGE_CONTAINERS and MANAGE_USERS_AND_GROUPS. The account can be either a Good Control service account or a regular administrator account, provided the password associated with the account allows access to the management console. You can't use an Active Directory user account with a hardware token and no password.
	Domain	Type the name of the domain where the administrator account for the source management console is located. You can leave this field blank if the administrator is a local user who does not have a domain.

5. Click **Save**.
6. To test the connection between the source and the destination, click **Test connection**.
7. 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.

Export the self-signed root certificate for the Good Control server

Complete the following task if the Good Control certificate has not been replaced with a third-party certificate. BlackBerry UEM inherently trusts certificates from third-party providers, so you do not need to export the certificate from the Good Control server and import it in to BlackBerry UEM.

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

1. In a browser, navigate to the login screen of any of your Good Control servers. You may see a certificate error message because the CA that signed the certificate was Good Control, and the browser does not recognize it as a well-known CA.
2. To open the Certificate dialog, click the certificate icon in the URL field.
3. Click **View certificate** or **Certificate information** to open the **Certificate management** menu.
4. Click the **Certification Path** tab.
5. Select the root certificate. The root certificate is the first item in the Certificate hierarchy (for example, GD12345678 CA).
6. Click **View Certificate**.
7. Click the **Details** tab.

8. Click **Copy to file** or **Export**.
9. Select either the **DER encoded binary X.509 (.CER)** or the **Base-64 encoded X.509 (.CER)** format.
10. Enter a location and file name for the certificate.
11. Click **Next** or **Save**.
12. Click **Finish**.

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 profiles
- 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)
- Any policies and profiles that are associated with the policies and profiles you select
- For migration from on-premises BlackBerry UEM version 12.12.1 and later only: App configuration settings, BlackBerry Dynamics connectivity profiles, and client certificates (app usage).

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.

A migration from a Good Control (standalone) source copies the following items to the destination database:

- Policy sets
- Connectivity profiles
- App groups
- App usage (for certificates)
- Certificates

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 security policy sets, connectivity profiles, app groups, and certificates to BlackBerry UEM, consider the following guidelines:

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

Item	Considerations
Policy sets (Good Control only)	After migration, each Good Control policy set appears as the following items in BlackBerry UEM: • an app configuration for each app in the policy set • security policy • compliance policy
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.
App groups (Good Control only)	The Everyone group is migrated but has no users assigned to it and is not related to the All Users group on the destination BlackBerry UEM server. The administrator must manually assign it to users if needed.
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.

Item	Considerations
Certificate usage (BlackBerry UEM)	Certificate usage is migrated, except for: • Certificate usages that already exist on the destination server • Non BlackBerry Dynamics apps • Custom apps from another Good Control organization

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. If you have more than one source configured, in the left pane, click **Migration > Configuration** and then select the radio button beside the name of the source server that you want to migrate data from.
3. Click **Migration** > **IT policies, profiles, groups**.
4. Click **Next**.
5. 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.
6. Click **Preview** to review the policies and profiles you selected.
7. Click **Migrate**.
8. 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.

After you finish: For specific information about what to do when you are migrating from a Good Control source server, see Complete policy and profile migration from Good Control to BlackBerry UEM.

Complete policy and profile migration for BlackBerry Dynamics-activated users

After you migrate users, devices, groups, and other data from Good Control to BlackBerry UEM, you must complete the following tasks on the destination BlackBerry UEM. For information about where to find Good Control features in BlackBerry UEM, see Good Control features in 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 and Good Control compliance policies to users.
- Set override profiles (BlackBerry Dynamics profiles and compliance profiles).
- Move .json file configurations from Good Control to BlackBerry UEM (for migrations from Good Control only).

Complete the migrated connectivity profiles:

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

Good Control features in BlackBerry UEM

The following table maps Good Control features to the location in BlackBerry UEM where you can perform the similar task.

Good Control feature	Where to find it in BlackBerry UEM
Users and Groups	Click **Users**.
Administrators	Click **Settings** > **Administrators**.
Manage BlackBerry Dynamics apps and entitlements	**Apps** and click the app that you want to manage .
Wipe, unlock, lock, and manage logs for BlackBerry Dynamics apps	**1.** On the menu bar, click **Users**. **2.** Search for a user account. **3.** In the search results, click the name of the user account. **4.** Select the device tab for the device that has installed the app that you want to manage. **5.** In the **BlackBerry Dynamics Apps** section, beside the app that you want to manage, choose the command.
Generate access keys	**1.** Click **Users**. **2.** Select the user that you want to generate an access key for. **3.** Click **Set activation password**. **4.** Select the **BlackBerry Dynamics access key generation** option.
Manage services	Click **Settings** > **BlackBerry Dynamics** > **App services**.
App groups	Click **Groups** > **User**.
Security policies	Click **Policies and profiles** > **BlackBerry Dynamics**.
Compliance policies	Click **Policies and profiles** > **Compliance (BlackBerry Dynamics)**.
Provisioning profiles	Click **Settings** > **Activation defaults**.
App specific policies	Click **Apps** and then click the BlackBerry Dynamics app that you want to manage.
Add app servers	Click **Policies and profiles** > **Connectivity (BlackBerry Dynamics)**.
Connectivity profile	Click **Policies and profiles** > **BlackBerry Dynamics connectivity**.
Device policies	Click **Policies and profiles** > **Policy** > **IT policies**

Good Control feature	Where to find it in BlackBerry UEM
Device configurations	Click **Policies and profiles** > **Networks and Connections** and choose the following profiles: • Wi-Fi • VPN • Proxy • Email • Web icon • Custom payload
Apple DEP	Click **Settings** > **External integration** > **Apple Device Enrollment Program**
APNS management	Click **Settings** > **External integration** > **Apple Push Notification**
Manage user self-service	Click **Settings** > **Self-Service**
Direct Connect settings	Click **Settings** > **BlackBerry Dynamics** > **Direct Connect**
Server properties	Click **Settings** > **BlackBerry Dynamics** > **Properties**
Good Proxy cluster configuration	Click **Settings** > **BlackBerry Dynamics** > **Clusters**
Trusted Authorities	Click **Policies and profiles** > **Certificates** > **CA certificate** Click **Settings** > **External integration** > **Certificate authority**
Certificate Definitions	Click **Policies and profiles** > **Certificates** > **User credential** Click **Settings** > **External integration** > **Certificate authority**
Uploaded certificates for users	Click **Users**>**All Users**>**User Detail**>**Summary**>**IT Policy and profiles**
App usage	**Allow BlackBerry Dynamics apps to use user certificates and user credential profiles** in corresponding application detail pages.
Reporting	Click **Settings** > **BlackBerry Dynamics** > **Reporting**
Server jobs	Click **Settings** > **BlackBerry Dynamics** > **Jobs**

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.
Device	• After migration, the user must use the same login information for BlackBerry UEM Self-Service that they used before migration.
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. In the management console, 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.

   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 Users and groups in 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
Best practice	It is a best practice to migrate one device for each unique configuration, for example, different groups, policies, app configurations, etc.) to make sure the destination server is set up correctly before migrating the rest of your devices.
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 on a BlackBerry UEM source	• 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 if the setting has not been delivered to the device. For more information on tracking commands being delivered to a device, visit support.blackberry.com/community to read article 102688.
Managed Android devices on a BlackBerry UEM source	• 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.
Chrome OS devices on a BlackBerry UEM source	You can migrate Chrome OS devices.

Item	Considerations
Windows devices	You can't migrate Windows devices.
macOS devices	You can't migrate macOS devices.
MDM controls (BlackBerry UEM)	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.

Item	Considerations
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 7.1 or later. • For migrations from a Good Control (standalone) instance, all apps must be at BlackBerry Dynamics SDK version 4.0.0 or later. To determine the version of SDK used for the apps to be migrated, run the container activity report on Good Control. • 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. • For migrations from a Good Control (standalone) instance, devices with a device authentication delegate of Good for Enterprise are not migrated. After removing Good for Enterprise as the authentication delegate, refresh the cache before continuing with the migration. It is a best practice to ensure that the user is assigned the same authentication delegate on BlackBerry UEM as they had on the source server.

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. • For migrations from a Good Control (standalone) instance, Good Dynamics MDM enrollments are not migrated. The user must unenroll from MDM. If the destination BlackBerry UEM requires MDM, the user must manually delete the old MDM profile and install and activate the BlackBerry UEM Client and re-enroll the device for MDM. **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. • You can't migrate devices for the same user from multiple Good Control source servers. You can migrate devices from multiple Good Control sources, but the users cannot already have a BlackBerry Dynamics device on the destination BlackBerry UEM. **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. **Access keys** • After migration, access keys can no longer be generated on the source server. • The device is removed from the source server at the start of migration and access keys can no longer be generated. **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.

	.json configurations (Good Control only) • For migrations from a Good Control (standalone) instance, .json configurations are not migrated. Because .json configurations are global, migrating them could overwrite .json configurations in the destination database. Ensure that any required .json configurations are reapplied in the destination server.

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
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

Device type	Activation type/Configuration	Migration
Windows	Any	Not supported
macOS	Any	Not supported

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.
- For migrations from BlackBerry UEM, 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. (Optional, for migrations from an on-premises UEM source to an on-premises UEM destination) To cancel the migration, click the check boxes beside the devices you want to cancel, and click ⊘.

   If you cancel the migration of a device, it must be wiped and then reactivated on the destination server.
8. To view the status of the devices being migrated, click **Migration** > **Status**.

   For migrations from Good Control, to determine which BlackBerry Dynamics apps have been migrated, run the container activity report on Good Control.

   Make sure that the Good Control configuration remains running until all of the users' authentication delegate apps have completed migration, even if all devices are migrated.

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.

Configuring BlackBerry UEM to support BlackBerry Dynamics apps

Follow the instructions in this section to configure BlackBerry UEM settings that are specific to BlackBerry Proxy and 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 Proxy, BlackBerry UEM creates a BlackBerry Proxy cluster named "First". If only one cluster exists, additional instances of BlackBerry Proxy are added to the cluster by default. You can create additional clusters and move BlackBerry Proxy instances between any of the available clusters. When more than one BlackBerry Proxy cluster is available, new instances are not added to a cluster by default; the new clusters 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 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**.
Enable a BlackBerry Proxy to be used for activation	Select the **Enabled for activation** option for the BlackBerry Proxy instance that you want to use for activation purposes. At least one instance must be selected.

Configure Direct Connect using port forwarding

Before you begin:

- Configure a public DNS entry for each BlackBerry Connectivity Node server (for example, bp01.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.
6. Click **Save**.

Configure BlackBerry Dynamics properties

You can configure properties specific to using BlackBerry Dynamics apps in your organization. For more information about each property and the implications of changing the default settings, see BlackBerry Dynamics global properties, BlackBerry Dynamics properties, BlackBerry Proxy properties, and Configure BlackBerry

Dynamics app proxy settings . To learn about best practices for configuring BlackBerry Proxy properties, visit support.blackberry.com/community to read article 47875.

1. In the management console, on the menu bar, click **Settings > BlackBerry Dynamics**.
2. Do one of the following:
   - To configure the global properties, click **Global properties**.
   - To configure the properties for a particular BlackBerry UEM instance, click **Properties**. In the **Server type** drop-down list, click **BlackBerry Control servers** and select the BlackBerry UEM server that you want to configure.
   - To configure the properties for a particular BlackBerry Proxy instance, click **Properties**. In the **Server type** drop-down list, click **BlackBerry Proxy servers** and select the BlackBerry Proxy server that you want to configure.
3. Configure the properties as necessary.
4. Click **Save**.

BlackBerry Dynamics global properties

The following tables describe the BlackBerry Dynamics global properties that you can configure.

The Restart column indicates whether changing the property requires a restart of BlackBerry UEM.

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

Certificate Management

Property	Description	Default	Restart
Time-to-live in seconds for the keystore for individual end-users' PKCS 12 certificates	The lifespan (time-to-live), in seconds, of the keystore for the PKCS 12 certificates that device users can upload to sign email messages and for client authentication. **Note:** This property is read-only. You cannot change it.	86400	—

Communication

Property	Description	Default	Restart
cntmgmt.internal.port	The internal port for the container management service.	Null (defaults to 17317)	Yes
cntmgmt.max.conns.above.limi	The maximum number of connections that are allowed in excess of the limit set by the cntmgmt.max.conns.persec property. **Note:** Do not change this setting without consulting BlackBerry Technical Support.	3	Yes

Property	Description	Default	Restart
cntmgmt.max.conns.persec	The maximum number of connections per second for container management. **Note:** Do not change this setting without consulting BlackBerry Technical Support.	30	Yes
cntmgmt.max.active.sessions	The maximum number of active sessions for container management.	10000	Yes
cntmgmt.max.idle.count	The maximum number of idle connections that are permitted for container management. **Note:** Do not change this setting without consulting BlackBerry Technical Support.	0	Yes
cntmgmt.max.read.throughput	The maximum number of concurrent read operations for container management. **Note:** Do not change this setting without consulting BlackBerry Technical Support.	500	Yes
cntmgmt.max.write.throughput	The maximum number of concurrent write operations for container management. **Note:** Do not change this setting without consulting BlackBerry Technical Support.	500	Yes
cntmgmt.ssl.external.enable	Controls whether SSL is enabled for external container management.	On	Yes
cntmgmt.ssl.internal.enable	Controls whether SSL is enabled for internal container management.	On	Yes

Duplicate Containers

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

Property	Description	Default	Restart
Automatically remove older duplicate containers on same device for the user after provisioning.	Specify whether BlackBerry UEM automatically removes duplicate containers when a new version of an app is provisioned. If this setting is selected, it takes precedence over the other Duplicate Container properties.	On	No
Enable job to automatically remove duplicate containers (on/off)	Specify whether BlackBerry UEM automatically schedules jobs to identify and remove duplicate containers from devices.	On	No

Property	Description	Default	Restart
Inactivity timeout in seconds before duplicate container is deleted	The amount of time, in seconds, that a duplicate container must be inactive before BlackBerry UEM schedules a job to remove it.	259200	No
Frequency in seconds that job to remove duplicate containers will run	How often, in seconds, BlackBerry UEM runs a job to identify and remove duplicate containers.	86400	No
Maximum number of containers to remove in a single job	The maximum number of inactive containers that a single job can remove from devices	100	No

Kerberos Constrained Delegation

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

Miscellaneous

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

Purge Inactive Containers

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

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

Property	Description	Default	Restart
Enable job to automatically remove inactive containers (on/off)	Specify whether BlackBerry UEM automatically schedules jobs to identify and remove inactive containers from devices.	Off	No
Container inactivity interval in seconds	The amount of time, in seconds, before BlackBerry UEM considers a container to be inactive.	7776000	No
Frequency in seconds that job to remove inactive containers will run	How often, in seconds, BlackBerry UEM runs a job to identify and remove inactive containers.	86400	No
Maximum number of containers to remove in a single job	The maximum number of inactive containers that a single job can remove from devices.	100	No

Reporting

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

Retention Data Policy

Property	Description	Default	Restart
Log read operations in the database	Whether BlackBerry Control logs read operations in the BlackBerry Control database.	On	Yes
Purge server jobs	Specify whether BlackBerry UEM automatically purges server jobs at a regular interval.	On	Yes
Purge server jobs interval (In Days)	If “Purge server jobs” is on, how often, in days, BlackBerry UEM purges server jobs.	30	Yes

BlackBerry Dynamics properties

The following tables describe the properties that you can configure for each of your organization's BlackBerry UEM Core instances.

Kerberos Constrained Delegation

Property	Description	Default	Restart
Location of krb5.config file on GC server (gc.krb5.config.file)	The krb5.conf file used for cross-realm authentication when there is a CAPATH trust relationship with multiple Kerberos domains.	Not set	Yes
Enable KCD debugging mode (gc.krb5.debug)	Whether BlackBerry UEM logs debug level data.	Off	Yes
Fully qualified name for the KDC (gc.krb5.kdc)	The FQDN of the server that hosts the Kerberos Key Distribution Center (KDC) service.	Not set	Yes
Location of keytab file (gc.krb5.keytab.file)	The location of the Kerberos keytab file on the computer that hosts BlackBerry UEM.	Not set	Yes
Service account name under which KCD service is running (gc.krb5.principal.name)	The username of the Kerberos account. Do not include the domain or realm.	Not set	Yes
Realm - Active Directory (gc.krb5.realm)	The realm of the Kerberos account.	Not set	Yes

BlackBerry Proxy properties

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

Property	Description	Default	Restart
gp.gps.max.sessions	Maximum number of active sessions.	15000	—
gp.gps.dns.server.ttl.ms	Time to wait, in milliseconds, for the DNS server response.	1800000	—
gp.gps.server.flowcontrol	Specify whether flow control is enabled for the server.	Off	—
gp.gps.tcp.keepalive	Specify whether TCP keepalive is enabled for the server.	Off	—

Property	Description	Default	Restart
gp.gps.unalias.hostname	For DNS lookups of app servers, use either IP address or hostname. If you select this option, BlackBerry Proxy uses reverse DNS lookup with IP address of app server. If you don't select this option, BlackBerry Proxy uses the app server hostname for DNS lookups.	Off	Yes
gps.directconnect.suppo	Add or change cipher suites that encrypt bridging and communications made through BlackBerry Direct Connect. You may choose to have your own proxy server configured for Direct Connect and placed between your client devices and the BlackBerry Proxy server. If you have added your own proxy server, make sure that the BlackBerry Proxy server ciphers correspond to those required by your own proxy server. **Note:** All ciphers must be supported by Java.	TLS_ECDHE_RSA_WI	Yes
gp.directconnect. supported.protocols	Add or change the cryptographic protocols that you want your system's direct connect bridge to support.	TLSv1, TLSv1.1, TLSv1.2	Yes
gp.eacp.command.servic	Enables LDAP over TCP for Active Directory servers. Active Directory servers offer the LDAP service over the TCP protocol; therefore, clients find an LDAP server by querying DNS for a record of the form: _ldap._tcp. DnsDomainName. If you select this option, BlackBerry Proxy uses LDAP for nslookup of a given service hostname. If you don't select this option, BlackBerry Proxy uses reverse DNS lookup directly, using the service hostname that you provide.	Off	Yes
gc.mdc.hb.timeout	Specify the heartbeat timeout.	0	—
gp.server.secure.ciphers	Add or change cipher suites that encrypt communications made through a BlackBerry Proxy server. **Note:** All ciphers must be supported by Java.	TLS_ECDHE_RSA_WI	—
gp.server.secure. protocols	Add or change the cryptographic protocols that you want your BlackBerry Proxy server to support.	TLSv1, TLSv1.1, TLSv1.2	—

Configure communication settings for BlackBerry Dynamics apps

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

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

Sending BlackBerry Dynamics app data through an HTTP proxy

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

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

Note: Manual proxy settings are also used for connections to the BlackBerry Dynamics NOC. The proxy must be able to access port 443. For more information about port requirements, see Outbound connections: BlackBerry UEM to the BlackBerry Dynamics NOC in the Planning content.

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

You can configure global BlackBerry Dynamics app proxy settings manually or using a PAC file. You can override the global settings for BlackBerry Proxy clusters and for individual servers; however, the level of complexity to override the settings for individual servers is not usually required and not recommended.

1. Perform one of the following actions:

Task	Steps
Set global app proxy settings	**a.** Click **Settings > Infrastructure > BlackBerry Router and proxy**. **b.** Click **Global settings**.
Set app proxy settings for a cluster	**a.** Click **Settings > BlackBerry Dynamics > Clusters** **b.** Click the cluster name. **c.** Click **Override global settings**.
Set manual app proxy settings for a server	**a.** Click **Settings > Infrastructure > BlackBerry Router and proxy**. **b.** Click **Override global settings**. **Note:** PAC files are not supported when overriding global proxy settings for a server.

2. 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.
3. 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.
4. 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.

5. Click **Save**.

BlackBerry Dynamics connectivity and routing behavior

BlackBerry UEM has several options that allow administrators to control how BlackBerry Dynamics traffic is routed. Routing for BlackBerry Dynamics apps is affected by:

- The assigned BlackBerry Dynamics connectivity profile
- The BlackBerry Proxy web proxy server configuration
- App-specific settings (for example, BlackBerry Access web proxy server configuration)

Before you configure routing, ensure that the correct ports are open and that you have network connectivity to the BlackBerry Dynamics NOC. For more information, see Port requirements in the Planning content and Sending BlackBerry Dynamics app data through an HTTP proxy.

This documentation discusses only configurations that affect overall routing. App-specific configuration may be required for apps to connect to specific servers (for example, for BlackBerry Work configured with the URL of the Microsoft Exchange Server). Review the documentation for each app to understand which app configurations to apply.

Default routing

By default, in a new installation of BlackBerry UEM, all BlackBerry Dynamics app traffic routes directly to the Internet, with no web proxy server configurations.

BlackBerry Dynamics connectivity profile configuration

The only item configured in the default BlackBerry Dynamics connectivity profile is the Default allowed domain route type, which is set to Direct.

Using the default BlackBerry Dynamics connectivity profile, no internal servers or domains are accessible to BlackBerry Dynamics apps. Administrators can modify the default connectivity profile or create a new one to allow connectivity to internal servers.

For more information, see Create a BlackBerry Dynamics connectivity profile in the Administration content.

BlackBerry Proxy web proxy server configuration

The default configuration for BlackBerry Proxy servers has no web proxy server configuration applied. In this configuration, each BlackBerry Proxy server attempts to connect directly to the Internet to make connections. This applies to both app server traffic and to BlackBerry Dynamics NOC connections.

In the BlackBerry Dynamics connectivity profile, you can specify the servers that BlackBerry Dynamics apps are allowed to access through the firewall using BlackBerry Proxy.

Routing traffic through BlackBerry Proxy has the following benefits:

- Web browsers and BlackBerry Dynamics apps on devices can connect to any server behind the firewall that is reachable by BlackBerry Proxy.
- You can easily monitor data traffic between BlackBerry Dynamics apps and your resources.

For apps developed with the BlackBerry Dynamics SDK version 6.0 and later, you can specify the BlackBerry Proxy clusters that data must route through.

If you have BlackBerry UEM in an on-premises environment, for apps developed with a version of the BlackBerry Dynamics SDK earlier than 6.0, you select the Route all traffic option to route all BlackBerry Dynamics app data, regardless of domain or subnet, through BlackBerry Proxy.

You should be aware of the following considerations when you route data through BlackBerry Proxy:

- Establishing connections to servers on the Internet can take longer.
- If you are using a web proxy to allow access to external sites and have settings configured in your proxy to restrict certain sites, when you select the Route all traffic option, you also need to set the proxy properties in BlackBerry Proxy. Otherwise, apps will not be able to access external sites. For more information on configuring BlackBerry Proxy settings, see the on-premises Configuration content or the Cloud Configuration content.
- BlackBerry Access can be configured with a PAC file that determines allowable sites. In this case, the PAC file determines the proxy settings. For more information, see the BlackBerry Access Administration Guide.

App-specific proxy configuration

BlackBerry Access and some third-party apps allow app-level web proxy server configurations.

The default configuration for BlackBerry Access has no web proxy server configuration applied. Review the documentation for third-party BlackBerry Dynamics apps to understand the default configuration for each.

Note: An app server is a server that a BlackBerry Dynamics app connects to, such as the URL of a Microsoft Exchange Server, the URL for BEMS, the URL for Skype for Business, or any URL that BlackBerry Access browses to. The BlackBerry Dynamics NOC and the BlackBerry UEM Core server are not app servers.

Example routing scenarios

The following example scenarios reflect the most common configurations. If these configurations don't meet your organization's needs or you have more complex requirements, contact BlackBerry Enterprise Consulting for assistance.

Scenario 1: Route traffic to specific servers or domains through BlackBerry Proxy

This configuration is appropriate for scenarios where some internal app servers must be accessible to BlackBerry Dynamics apps, but general traffic to public servers can remain direct.

For example, you can route connections directly to public sites like google.com and microsoft.com, but require internal routing through the BlackBerry Proxy to access internal Microsoft Exchange Servers and SharePoint servers.

This configuration assumes that a web proxy server connection to the Internet is not required, either because no Internet-based servers will ever be routed through the BlackBerry Proxy server or because the BlackBerry Proxy server itself has direct access to the Internet without requiring a web proxy server connection.

BlackBerry Dynamics connectivity profile

1. Set the **Default allowed domain route type** to **Direct**.
2. Under **Allowed domains**, add the internal domains that you want to route through the BlackBerry Proxy and select a BlackBerry Proxy cluster.
3. (Optional) Add specific server names under **Additional servers** and select a BlackBerry Proxy cluster. This is required only if the servers are not already covered by the **Allowed domains** rules.

BlackBerry Proxy server web proxy server

No web proxy server configuration is necessary.

Note: If your organization has special requirements to access the internet from internal servers, or requires all traffic to be routed through a web proxy server, see the configuration examples below that include proxy configurations.

App-specific web proxy server

No app-specific web proxy server configurations are necessary.

Scenario 2: Route all traffic through the BlackBerry Proxy and then through a web proxy server

This configuration is appropriate for organizations that require all traffic from work apps to be routed internally. A web proxy server is required for internal servers to connect to the internet.

For example, connections to public sites like google.com and microsoft.com as well as internal Microsoft Exchange Servers and SharePoint servers must all be routed internally through the BlackBerry Proxy.

In this configuration, it is assumed that a web proxy server connection to the Internet is also required, because most organizations that require all traffic to be routed internally also require that traffic be routed through a web proxy server for filtering or monitoring.

BlackBerry Dynamics connectivity profile

1. Set the **Default allowed domain route type** to **BlackBerry Proxy cluster**.
2. (Optional) Add internal domains to the **Allowed domains** list. This is not necessary when the **Default allowed domain route type** is set to route through the BlackBerry Proxy.
3. (Optional) Add specific server names under **Additional servers** and select a BlackBerry Proxy cluster. This is not necessary when the **Default allowed domain route type** is set to route through the BlackBerry Proxy.
4. (Optional) If you want specific servers to be exempt from the default routing through the BlackBerry Proxy, you can specify specific domains (either under **Allowed domains** or **Additional servers**) and select **Direct**. This allows you to route most traffic through BlackBerry Proxy but exempt some traffic (for example, to improve performance to certain trusted public sites).

BlackBerry Proxy server web proxy server

Depending on the complexity of your environment, you can configure the BlackBerry Proxy server to route traffic through a web proxy server rather than directly to the destination server.

You can either use a manual web proxy server configuration or a PAC file.

Note: You can select both manual HTTP proxy and PAC. This may be necessary for scenarios where NOC traffic should use a different proxy server than app traffic. Avoid this level of complexity where possible.

Manual HTTP proxy: Manual web proxy server configuration is sufficient if there are no complex rules governing which URLs should use a web proxy server and which should go direct. If all traffic should use a web proxy server, then configuring a manual web proxy server is the easiest way to accomplish this.

1. Enable the manual HTTP proxy:

In an on-premises environment	**a.** Go to **Settings > Infrastructure > BlackBerry Router and proxy**. **b.** Expand **Global Settings**, and select **Enable manual HTTP proxy**.
In a Cloud environment	**a.** Go to **Settings > BlackBerry Dynamics > Clusters**. **b.** Click on the cluster you want to edit. **c.** Enable **Override Global Settings**, and select **Enable manual HTTP proxy**.

2. Select **Use proxy to connect to all servers**.
3. Type the address and port for the web proxy server.

Proxy auto-configuration (PAC) file: If your organization requires more complex rules about which servers should use a proxy and which should connect directly, BlackBerry recommends using a PAC file because it is much easier to manage.

For example, if you want all connections to the public internet to use the web proxy server, but all internal domains to connect directly, the best practice is to use a PAC file.

Note: PAC file configuration is not part of the BlackBerry product and should be completed by the appropriate network or proxy team in your organization.

1. Open the proxy settings:

In an on-premises environment	Go to **Settings > Infrastructure > BlackBerry Router and proxy**.
In a Cloud environment	Go to **General Settings > BlackBerry Router and proxy**.

2. Expand **Global Settings**, select **Enable PAC**.
3. Enter the PAC URL and authentication information as required.

App-specific web proxy server

No app-specific proxy configurations are necessary. This configuration assumes that all traffic is routed internally and either a manual proxy or PAC is configured at the BlackBerry Proxy server.

Scenario 3: Route some traffic internally for most apps but configure a proxy server specifically for web browsing using BlackBerry Access

This configuration is appropriate for organizations that require traffic for apps to be routed internally, but require more complex routing through a web proxy server specifically for browser traffic.

For example, your organization might decide that it is acceptable for BlackBerry Work to connect to Microsoft Office 365 servers directly. SharePoint is still internal, though, so some traffic must route through the BlackBerry Proxy. However, browsing is more tightly controlled, and any traffic from BlackBerry Access should route through a web proxy server for monitoring and logging.

This configuration can also include a web proxy server configuration at the BlackBerry Proxy server level, but for this example we assume direct connectivity is available from the BlackBerry Proxy.

BlackBerry Dynamics connectivity profile

1. Set the **Default allowed domain route type** to **Direct**.
2. Under **Allowed domains**, add all internal domains that you want to route through the BlackBerry Proxy and select a BlackBerry Proxy cluster.
3. (Optional) Add specific servers that are not already included under **Additional servers** and select a BlackBerry Proxy cluster.

Important: If you plan to specify an internally hosted web proxy server in the app-specific configuration, you must include that web proxy server URL either in the Allowed domains list or the Additional servers list. If the web proxy server URL is not set to route through the BlackBerry Proxy, then connections to the web proxy server will fail. If the web proxy server is accessible publicly, this step is not required.

BlackBerry Proxy server web proxy server

This example assumes that the BlackBerry Proxy servers have direct access to the Internet. If not, or if you need to specifically configure a proxy for BlackBerry Dynamics NOC connections, configure a web proxy server as needed.

App-specific web proxy server

If a web proxy server is required for a specific app (for example, BlackBerry Access for browsing, or other third-party apps), you must use the App configuration for that app. Consult third-party vendors for specifics on whether an app-specific proxy is supported and how to configure it.

If an app-specific web proxy server is configured, the BlackBerry Dynamics app evaluates the proxy and PAC rules locally on the device before BlackBerry Dynamics connectivity profile rules are evaluated. It is important,

therefore, that any proxy URLs configured using the manual proxy, or that can be returned by the PAC file, must be appropriately configured in the BlackBerry Dynamics connectivity profile.

1. Go to **Apps**, then click on the app you want to configure (for example, BlackBerry Access).
2. Under **App configuration**, create a new configuration or edit an existing one.
3. For BlackBerry Access, on the **Network** tab, select **Enable Web Proxy** and **Use Proxy Auto Configuration** as required.

For more information, see Troubleshoot routing issues in the BlackBerry Access content.

BlackBerry Dynamics data flow

It is important for administrators to understand the effects of certain combinations of settings. The table in this section describes the interaction between the BlackBerry Dynamics connectivity profile and the HTTP proxy server configured for the BlackBerry Proxy service.

How BlackBerry UEM evaluates connections to hosts

The BlackBerry Dynamics connectivity profile is always checked first. After traffic arrives at the BlackBerry Proxy server, the PAC or web proxy server configuration set on the BlackBerry Proxy server is evaluated for connectivity. Configuring a web proxy server on the BlackBerry Proxy server controls how that BlackBerry Proxy handles sending traffic out to the Internet. It does not affect how the BlackBerry Dynamics app on the device evaluates connections.

	Host in connectivity profile resolves to BlackBerry Proxy	Host in connectivity profile resolves to Direct	Host in connectivity profile is blocked
Proxy/PAC = Proxy URL	BlackBerry Dynamics app > BlackBerry Proxy cluster > Web proxy server URL > Destination	BlackBerry Dynamics app > Destination	Content blocked by BlackBerry Dynamics SDK
Proxy/PAC = Direct	BlackBerry Dynamics app > BlackBerry Proxy cluster > Destination	BlackBerry Dynamics app > Destination	Content blocked by BlackBerry Dynamics SDK
Proxy/PAC = Block	Content blocked by web proxy server	BlackBerry Dynamics app > Destination	Content blocked by BlackBerry Dynamics SDK

Note: Some apps allow a web proxy server or PAC to be configured specifically for that app. For example, BlackBerry Access allows administrators to configure a web proxy server or PAC specifically for BlackBerry Access to use. In these scenarios, the app evaluates the app-specific web proxy server configuration before it evaluates the BlackBerry Dynamics connectivity profile.

For more information, see Troubleshoot routing issues in the BlackBerry Access Administration content.

Configuring Kerberos for BlackBerry Dynamics apps

BlackBerry Dynamics apps support both Kerberos Constrained Delegation and Kerberos PKINIT. Kerberos Constrained Delegation (KCD) and Kerberos PKINIT are distinct implementations of Kerberos. You can support one or the other for BlackBerry Dynamics apps, but not both.

Kerberos Constrained Delegation (KCD) allows users to access enterprise resources without having to enter their network credentials. KCD uses service tickets that are encrypted and decrypted by keys that do not contain the user's credentials.

When *delegation* is configured, the BlackBerry Dynamics app delegates authentication to BlackBerry UEM to act on its behalf to request access to a work resource. KCD *constrains* the accessed resources: administrators can limit the network resources that are accessible. This is accomplished by configuring the account under which the delegate (BlackBerry UEM) runs as trusted only for specific services.

For example, if KCD is not configured and an app requests a resource like mypage.mydomain.com, the app prompts the user for credentials. When KCD is configured, the BlackBerry Dynamics infrastructure handles authentication and the user is not prompted for credentials for the resource.

Kerberos is a part of Microsoft Active Directory. Before configuring Kerberos Constrained Delegation in BlackBerry UEM, ensure your Kerberos environment is functioning properly and that you understand the implications involved in configuring Constrained Delegation for internal resources. Consult the appropriate Microsoft documentation if you require information on Kerberos in general or Constrained Delegation.

Kerberos PKINIT authentication establishes trust directly between the BlackBerry Dynamics app and the Windows KDC. User authentication is based on certificates issued by Microsoft Active Directory Certificate Services. To use PKINIT, Kerberos Constrained Delegation must not be enabled in the app settings in BlackBerry UEM.

The information in this section is a guideline. If you require more information about Kerberos and BlackBerry UEM, contact BlackBerry Technical Support.

Domains, realms, and forests

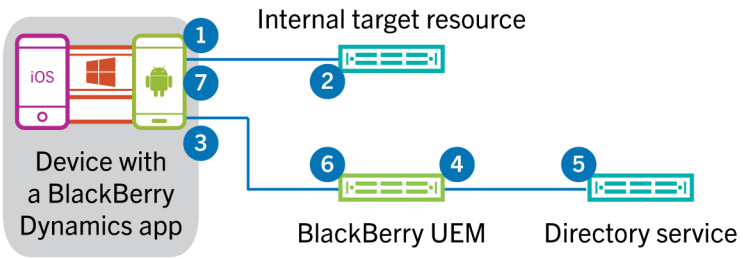
BlackBerry UEM operating in a *single-realm* Kerberos environment consists of one core, or multiple cores that are configured identically. BlackBerry UEM operating in a *multi-realm* Kerberos environment consists of multiple cores that are configured separately.

A *realm* is a collection of entities, either user realms or resource realms. A resource realm is any realm other than a user realm. In Kerberos, the realm name must always be typed in uppercase characters.

A *domain* is a directory service domain, most frequently from Active Directory.

The terms realm and domain are interchangeable in KCD.

Single-realm Kerberos environment

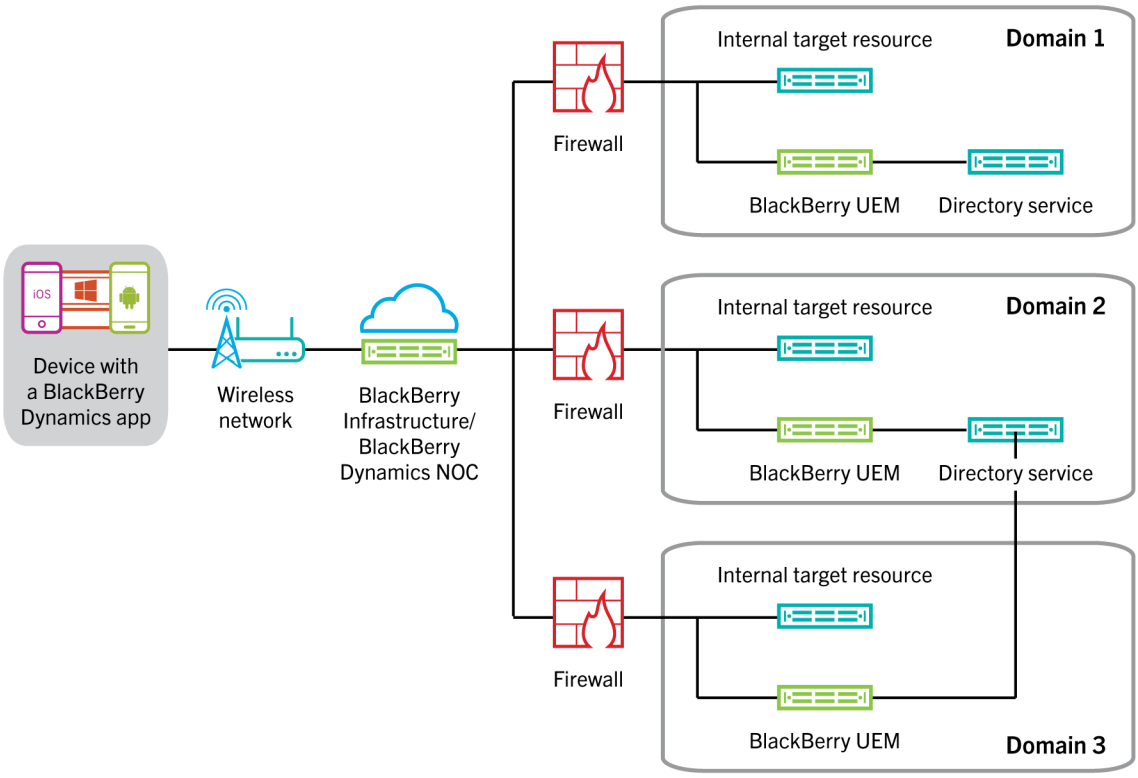


1. A BlackBerry Dynamics app makes a request to an internal server or service (the *target)*.

   The target can be either a host name (server name) or an account that is to be protected by Kerberos and BlackBerry Dynamics. For example, if IIS is running on a server as the Network service, the target is the server running IIS as Network. On the other hand, if IIS is running as a user (for example, IISSrvUser), then the target is that user name, IISSrvUser.
2. The target replies with an authentication challenge that BlackBerry Dynamics intercepts.
3. The BlackBerry Dynamics SDK sends a request to BlackBerry UEM for a service ticket to access the target.

4. BlackBerry UEM authenticates the user or app (through internal BlackBerry Dynamics protocols) and asks for a service ticket on behalf of the user (delegation) for the service on the target.
5. Active Directory checks its local policy. If the user has permission to access the resource on the target and if the resource on the target is allowed (constrained), Active Directory returns to BlackBerry UEM a service ticket for the resource.
6. BlackBerry UEM sends the necessary information from the returned service ticket to the BlackBerry Dynamics SDK.
7. The BlackBerry Dynamics app uses the information from BlackBerry UEM to complete the authentication to the target.

Multi-realm Kerberos environment, single-forest configuration



In a multi-realm KCD environment, the BlackBerry Dynamics client selects a BlackBerry UEM Core to process the KCD request based upon the DNS domain of the target server. Once the target is determined to be a KCD target, the BlackBerry Dynamics client determines the list of BlackBerry UEM Core servers that are within the same DNS domain as the target, then randomly selects from this list (based on priorities) a BlackBerry UEM Core to process the request.

If there is no such DNS match (no BlackBerry UEM Core servers are within the same DNS domain as the target), the client randomly selects from the list of all BlackBerry UEM Core servers.

Note: When a resource (for example, Microsoft Exchange) has an FQDN name that doesn't accurately reflect the Kerberos realm the resource is in, then BlackBerry UEM may not be able to properly authenticate the resource. For example, if the resource has a DNS pool name of cas.domain.com but the actual servers behind that DNS pool name are server1.alternatedomain.domain.com and server2.alternatedomain.domain.com, then the SDK will not be able to find a BlackBerry UEM Core server within the correct realm.

The SDK compares the target host DNS domain to the DNS domain of all the BlackBerry UEM Core servers so that the comparison can be done offline on the device as soon as the Kerberos request occurs, with no additional

fetches. If the list of Core servers in the same DNS domain as the target is empty, the SDK returns the full list of servers. Otherwise, it uses the previously generated list. The list is then randomised and further sorted to ensure this also meets the priority as well (the primaries first). The SDK selects the top two entries and initiates the KCD request to the top-listed Core server. If that request fails, the SDK sends the request to the second Core server.

For more information, visit support.blackberry.com/community to read article 49304.

DNS for BlackBerry UEM and BlackBerry Connectivity Node in separate domains

The BlackBerry UEM server and the BlackBerry Connectivity Node server are often installed in the same Kerberos domain but they do not have to be. You can install the BlackBerry Connectivity Node in a DMZ or "sacrificial" workgroup. If you choose this configuration, you must set up some required network configurations, as detailed below.

BlackBerry Dynamics operates differently between normal Kerberos (or Kerberos authentication) and Kerberos Constrained Delegation (KCD), which affects the network configuration.

- In KCD, the BlackBerry UEM Core service requests authentication tickets from the ticketing server (the domain controller) on behalf of the client apps.
- In Kerberos without constrained delegation, the client apps make the ticketing requests, and the requests pass through the BlackBerry Proxy. This means that the BlackBerry Proxy must be able to discover the name of the Kerberos domain controller (server). In the domain name system (DNS), you must add an SRV record specifying the Kerberos service that enables this discovery. This SRV record must be associated with an A or AAAA record, not a CNAME record. The syntax below is for a Kerberos domain controller in an internet domain named example.com:

  ```
  _kerberos._tcp.example.com. 86400 IN SRV 0 5 88 kerberos.example.com
  ```

  This points to a server named kerberos.example.com listening on TCP port 88 for Kerberos requests. The priority is 0 and the weight is 5.

Prerequisites for configuring Kerberos for BlackBerry Dynamics apps

- Port 88 on the Active Directory service must be accessible by all BlackBerry UEM servers.
- The Kerberos environment must include the following components:
  - Microsoft Active Directory server: The directory service that authenticates and authorizes all users and computers associated with your Windows network.
  - Kerberos Key Distribution Center (KDC): The authentication service on the Active Directory server that supplies session tickets and keys to users and computers in the Active Directory domain.
- Create service principal names (SPN) for all HTTP services (including BlackBerry Enterprise Mobility Server and other services). You must set an SPN for every target resource you want devices to have access to. For example:

  ```
  setspn –S HTTP/SPHOST.FQDN:PORT domain\AppPoolUser
  ```

  For more information on how to create and modify SPNs, see Register a Service Principal Name for Kerberos Connections. SPNs should be configured by the owners of the app servers or the Active Directory server.

For multi-realm Kerberos environments:

- A minimum of one BlackBerry UEM Core server must be installed in each Kerberos realm. UEM must reside in the same Kerberos realm as the resource because cross-realm resource delegation is not supported.
- Ensure that single-realm KCD is working before configuring multi-realm KCD.
- All trusts must be bidirectional, transitive forest trust.

- Ensure a maximum of 5 ms latency between the BlackBerry UEM Core servers and the Microsoft SQL Server database.

Configure Kerberos Constrained Delegation

For multi-realm configuration, always start by configuring and testing a single realm first, then proceed to adding the other realms or forests.

Before you begin:

- If you are configuring KCD for BlackBerry Docs, see Configuring Kerberos constrained delegation for the Docs service.
- For additional information about the keytab file, see KB 42712.

1. Map the Kerberos service account to a service principal name (SPN). Open an administrator command prompt on the Active Directory server and type `setspn –s GCSvc/UEM_Core_host_machine DOMAIN\Kerberos_service_account`.

   Replace the host server name, domain, and service account variables with values appropriate to your environment. The Kerberos service account is the service account name under which the KCD service will be configured in UEM (gc.krb5.principal.name). This account does not need to be the same as the UEM service account, but can be.

   For example:

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

2. Create the Kerberos keytab file. You must generate a new keytab file and copy it to the UEM server when you change the Kerberos account password.

   Creating the Kerberos keytab file also sets the Kerberos account password. The password set in this command sets the password for the account that you specify in the command. If you have already been given a password, ensure you use the same one. If you use a different password, it resets the password. This includes the UEM service account password, if you use the UEM service account to create the keytab file. To create the keytab file, perform the following actions:

   a) Open a command prompt window on the KDC server.
   b) Use the ktpass command. For more information about the ktpass command, visit docs.microsoft.com.

   ```
   ktpass -out outfilename.keytab -mapuser kerberos_account@REALM_IN_ALL_CAPS
   -princ kerberos_account@REALM_IN_UPPERCASE/ptype KRB5_NT_PRINCIPAL -pass
   kerberos_account_password
   ```

outfilename	This is the name of the output file.
kerberos_account	This is the name of the Kerberos account.
REALM_IN_UPPERCASE	This is the Kerberos realm. The name must use only uppercase letters.
-pass kerberos_account_password	This is the existing password for the reused Kerberos account. If the kerberos_account_password contains special characters, such as ^, enclose it in double quotation marks.

For example:

```
ktpass -out outfilename.keytab -mapuser kerberos_account@REALM_IN_UPPERCASE
 -princ kerberos_account@REALM_IN_UPPERCASE /ptype KRB5_NT_PRINCIPAL -pass
 kerberos_account_password
```

or

```
ktpass /out outfilename.keytab /mapuser kerberos_account@REALM_IN_UPPERCASE /
princ kerberos_account@REALM_IN_UPPERCASE /ptype KRB5_NT_PRINCIPAL /pass
 kerberos_account_password
```

c) Copy the new keytab file (kcdadmin.keytab in the examples) saved in this directory to the UEM server. If you have multiple BlackBerry UEM Core servers that are configured to use the same KCD admin account, you must copy the keytab file to every UEM server.

   You can copy the keytab file to any location on the servers, for example, c:\keytab. You will reference this location later on, so make a note of it.

3. Enable enumeration of AD user objects group membership. For more information, see Appendix B: Privileged Accounts and Groups in Active Directory.
4. On the UEM server, configure permissions for the UEM service account so it can send user credentials to the Kerberos system. This is the same account that has the associated service principal name (SPN). To configure permissions, perform the following actions:
   a) Open the **Local Security Policy** pane in the Windows console.
   b) Under **Local Policies**, select **User Rights Assignments**, then right-click **Act** as part of the operating system in the right panel and select **Properties**.
   c) In the **Properties** window, click on **Add User or Group**, then type the name of the service account and click **OK**.
5. Configure Kerberos-related properties in UEM.

   You can specify only one KDC (domain controller) in the UEM configuration for each BlackBerry UEM Core server. This means that all KCD-related calls to the domain controller will always go to that single KCD. This could mean that if that one KDC goes down, all KCD calls will fail.

   - In **Settings > BlackBerry Dynamics > Global properties**, the following settings are required to enable KCD in UEM.

Property	Description
Use explicit UPN	Enable this property to force UEM to perform authentication using the explicit UPN stored in Active Directory instead of the implicit UPN that is generated by combining a user's alias and domain."
Enable KCD (gc.krb5.enabled)	Select this check box to enable KCD.

   - In **Settings > BlackBerry Dynamics > Properties** (click on the server name), the following settings are required to enable KCD in UEM.

Property	Example	Description
gc.krb5.kdc=<kdc_host_name>	UEM1.EXAMPLE.COM	The fully qualified name for the KDC. It usually corresponds to the FQDN of an Active Directory domain controller.

Property	Example	Description
gc.krb5.keytab.file= <keytab_file_location>	c:/keytab/kcdadmin.keytab	The location of the keytab file. Use forward slashes in the path name.
gc.krb5.principal.name= <kcd_service_account>	kcdadmin@EXAMPLE.COM	The name of the service account used by the KCD service.
gc.krb5.realm=<REALM>	EXAMPLE.COM	The name of the Active Directory realm. The value must be in all uppercase letters.

6. Optionally, create a krb5.conf file if there is a CAPATH trust. Consult your Active Directory team if you need to create this file.

   The krb5.conf file is required to establish the CAPATH trust relationships of multiple Kerberos domains. The location of the krb5.conf file on the UEM server must be specified in the server property gc.krb5.config.file.

   Sample krb5.conf file:

```
[libdefaults] default_realm = NA.POD1.COM [realms] NA.POD1.COM = { kdc
 = pod1-na-ad.na.pod1.com } [ capaths] NA.POD1.COM = { APAC.POD2.COM =
 POD2.COM POD2.COM = POD1.COM POD1.COM = . } POD2.COM = { NA.POD1.COM =
 POD1.COM POD1.COM = . } APAC.POD2.COM = { NA.POD1.COM = POD1.COM POD1.COM =
 POD2POD2.COM POD2.COM = .}
```

Troubleshooting and diagnostics

Use the log files to help you detect issues that your system administrator can either fix or else send to BlackBerry Technical Support for investigation and resolution. You can also search the BlackBerry Knowledge Base for information.

Enable debug logging to see the logs.

Kerberos and KCD log file error codes

Information captured in the BlackBerry UEM server logs can often help to explain Kerberos authentication and KCD issues and errors. Following is an example of a Kerberos error log:

```
2019-06-26T13:23:19.424-0500 - CORE {ContainerMgmtServerThread#1}
 none|none [{{externalTenantId,S12345678}}] - ERROR KRB u=
 B32F95DF-4338-499A-A06D-7EAC36852A21 while requesting KRB ServiceTicket
 for serviceClass= HTTP server= uem1.example.com port= 443 serviceName=
 httpcom.rim.platform.mdm.dynamics.kerberos.KerberosException: Failed to
 impersonate userPrincipal KCDADMIN@UEM1.EXAMPLE.COM;
            krbErrCode: 63;
            krbErrText: Fail to create credential.
```

The two most important parameters in the error messages are krbErrCode and krbErrText, which furnish a description of possible error conditions detected.

For a complete list of Kerberos error messages, visit docs.microsoft.com to read "Kerberos and LDAP error messages".

Configuring Kerberos PKINIT

BlackBerry UEM supports Kerberos PKINIT for BlackBerry Dynamics user authentication using PKI certificates.

If you want to use Kerberos PKINIT for BlackBerry Dynamics apps, your organization must meet the following requirements:

Key points

- Kerberos Constrained Delegation must not be enabled.
- The KDC host must be added to the Allowed Domains list in the BlackBerry Dynamics Connectivity Profile.
- The KDC host must be listening on TCP port 88 (the Kerberos default port).
- BlackBerry Dynamics doesn't support KDC over UDP.
- The KDC must have an `A` record (IPv4) or `AAAA` record (IPv6) in your DNS.
- BlackBerry Dynamics doesn't use Kerberos configuration files (such as `krb5.conf`) to locate the correct KDC.
- The KDC can refer the client to another KDC host. BlackBerry Dynamics will follow the referral, as long as the KDC host that is referred to is added to the Allowed Domains list in the BlackBerry Dynamics Connectivity Profile.
- The KDC can obtain the TGT transparently to BlackBerry Dynamics from another KDC host.

Server certificates

- Windows KDC server certificates issued via the Active Directory Certificate Services must come only from the following Windows Server versions. No other server versions are supported.
  - Internet Information Server with Windows Server 2008 R2
  - Internet Information Server with Windows Server 2012 R2
- Valid KDC service certificates must be located either in the BlackBerry Dynamics Certificate Store or the Device Certificate Store.

Client certificates

- The minimum keylength for the certificates must be 2,048 bytes.
- The Extended Key Usage property of the certificate must be Microsoft Smart Card logon (1.3.6.1.4.1.311.20.2.2).
- Client certificates must include the User Principal Name (for example, user@domain.com) in the Subject Alternative Name of object ID szOID_NT_PRINCIPAL_NAME 1.3.6.1.4.1.311.20.2.3
- If the user is issued more than one client certificate, the domain of the User Principal Name must match the domain of the resource that is being accessed to ensure that the correct certificate is used.
- Certificates must be valid. Validate them against the servers listed above.

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. 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.

Integrating BlackBerry UEM with Cisco ISE

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

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

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

Cisco ISE administrators can view, sort, and filter data about devices in the Cisco ISE management console. Administrators can also perform the following device management tasks: lock a device, delete the work data from a device, or delete all data from a device.

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

Step	Action
1	Verify that your organization's environment meets the requirements to integrate BlackBerry UEM with Cisco ISE.
2	Create a BlackBerry UEM administrator account that Cisco ISE can use to obtain data about devices.
3	Add the BlackBerry Web Services certificate to the Cisco ISE certificate store.
4	Connect BlackBerry UEM to Cisco ISE and set up an authorization profile and access policies.

Requirements: Integrating BlackBerry UEM with Cisco ISE

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

Item	Requirement
Listening port	Cisco ISE uses the default BlackBerry Web Services listening port, 18084, to obtain data about devices from UEM. If port 18084 was not available when UEM was installed, the setup application selected another available port for this purpose. To verify the correct port value, in the BlackBerry UEM Core log file (CORE), search for `(^/ciscoise/.*)` and record the port number that is listed just before this text.
Firewall	If a firewall exists between UEM and Cisco ISE, configure the firewall to allow HTTPS sessions between both systems.

Create an administrator account that Cisco ISE can use

Cisco Identity Services Engine (ISE) requires a dedicated BlackBerry UEM administrator account that it can use to retrieve data about devices. You can use an existing administrator account or you can create a new administrator account. It must be a local administrator account (not a directory user). The administrator account requires a role with the following permissions:

- View users and activated devices
- Manage devices
- Lock device and set message
- Delete only work data
- Delete all device data

The default Security Administrator and Enterprise Administrator roles have these permissions. To create a new administrator account with a custom role, complete the following steps using an administrator account with the Security Administrator role.

Before you begin: If you want to create a custom role for the administrator account, in the BlackBerry

UEM management console, click **Settings > Administrators > Roles >** . Select the necessary permissions. Click **Save**.

1. In the BlackBerry UEM management console, on the menu bar, click **Users**.
2. Click **Add user**.
3. Click the **Local** tab.
4. Specify a first name, last name, display name, username, and email address.
5. In the **Console password** field, type a password for the administrator account.
6. Select the **Do not set device activation password** option.
7. Click **Save**.
8. On the menu bar, click **Settings**.
9. Click **Administrators > Users**.
10. Click .
11. Search for and click the user account that you created.
12. In the **Role** drop-down list, click the custom role that you created, the default Security Administrator role, or the default Enterprise Administrator role.
13. Click **Save**.

After you finish: Add the BlackBerry Web Services certificate to the Cisco ISE certificate store

Add the BlackBerry Web Services certificate to the Cisco ISE certificate store

To enable Cisco Identity Services Engine (ISE) to connect with BlackBerry UEM, you must export the BlackBerry Web Services certificate and import it into the Cisco ISE certificate store. If your organization's BlackBerry UEM domain has multiple instances of BlackBerry UEM, you only have to export the certificate from one instance.

If you do not have a Cisco ISE administrator account, send these instructions to a Cisco ISE administrator.

Note: Steps 3 and after are based on Cisco ISE version 1.4. For the latest Cisco ISE documentation, visit Cisco ISE Configuration Guides to read the *Cisco Identity Services Engine Administrator Guide*.

Before you begin: Create an administrator account that Cisco ISE can use.

1. In a browser, navigate to **https://*<server_name>*:*<BlackBerry_Web_Services_port>*/enterprise/admin/util/ws?wsdl** where *<server_name>* is the FQDN of the computer that hosts the BlackBerry UEM Core component. The default *<BlackBerry_Web_Services_port>* value is 18084.
2. Export the BlackBerry Web Services certificate and save it to your desktop. For instructions, see the documentation for the browser you are using.

   Example: In Google Chrome, click the lock icon next to the URL. On the **Connection** tab, click **Certificate information**. On the **Details** tab, click **Copy to File** and follow the instructions on the screen.
3. Log in to the Cisco ISE management console.
4. On the menu bar, click **Administration > System > Certificates**.
5. In the left pane, click **Trusted Certificates**.
6. Click **Import**. Browse to and select the BlackBerry Web Services certificate.
7. Select the **Trust for client authentication and Syslog** check box.
8. Select the **Trust for authentication of Cisco Services** check box.
9. Click **Submit**.

After you finish: Connect BlackBerry UEM to Cisco ISE.

Connect BlackBerry UEM to Cisco ISE

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

Note: The following steps are based on Cisco ISE version 1.4. For the latest Cisco ISE documentation, visit Cisco ISE Configuration Guides to read the *Cisco Identity Services Engine Administrator Guide*.

Before you begin: Add the BlackBerry Web Services certificate to the Cisco ISE certificate store.

1. Log in to the Cisco ISE management console.
2. On the menu bar, click **Administration > Network Resources > External MDM**.
3. Click **Add**.
4. In the **Name** field, type a friendly name for the connection.
5. In the **Hostname or IP address** field, type the FQDN or IP address of the BlackBerry UEM domain.
6. In the **Port** field, type `18084`.

If port 18084 was not available when BlackBerry UEM was installed, the setup application selected another available port for this purpose. To verify the correct port value, in the BlackBerry UEM Core log file (CORE), search for `(^/ciscoise/.*)` and record the port number that is listed just before this text.

7. In the **User Name** field, type the username for the BlackBerry UEM administrator account.
8. In the **Password** field, type the password for the BlackBerry UEM administrator account.
9. In the **Polling Interval** field, specify how often, in minutes, you want Cisco ISE to poll BlackBerry UEM for device data. It is a best practice to use the default value of 240 minutes.

   Note: If you set this value to 60 minutes or less, you might notice a significant performance impact on your organization's environment. If you set this value to 0, Cisco ISE does not poll BlackBerry UEM.
10. Click the **Enable** check box.
11. Click **Test Connection** to verify that Cisco ISE can connect to BlackBerry UEM.
12. Click **Submit**.

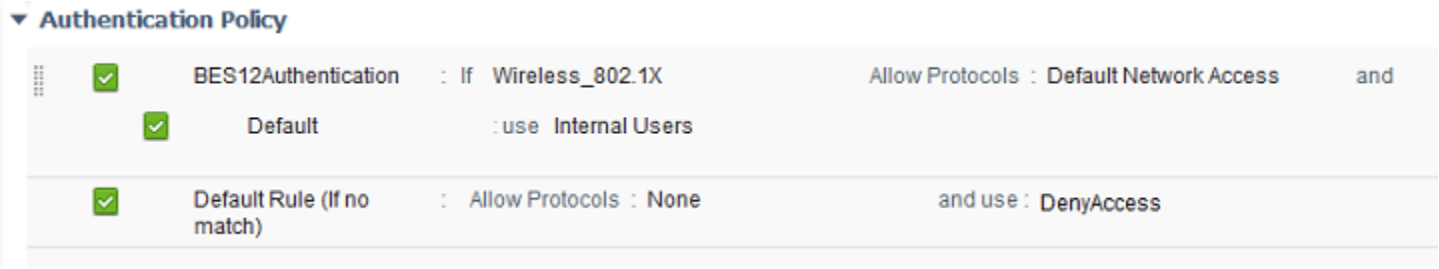
After the connection is established, you can view the dictionary attributes for BlackBerry UEM in **Policy > Policy Elements > Dictionaries > System > MDM > Dictionary Attributes**. Log entries for Cisco ISE polling are written to the BlackBerry UEM Core (CORE) log file.

After you finish: Perform the following configuration tasks in the Cisco ISE management console. For the latest instructions, visit Cisco ISE Configuration Guides to read the *Cisco Identity Services Engine Administrator Guide* (see Set Up MDM Servers With Cisco ISE).

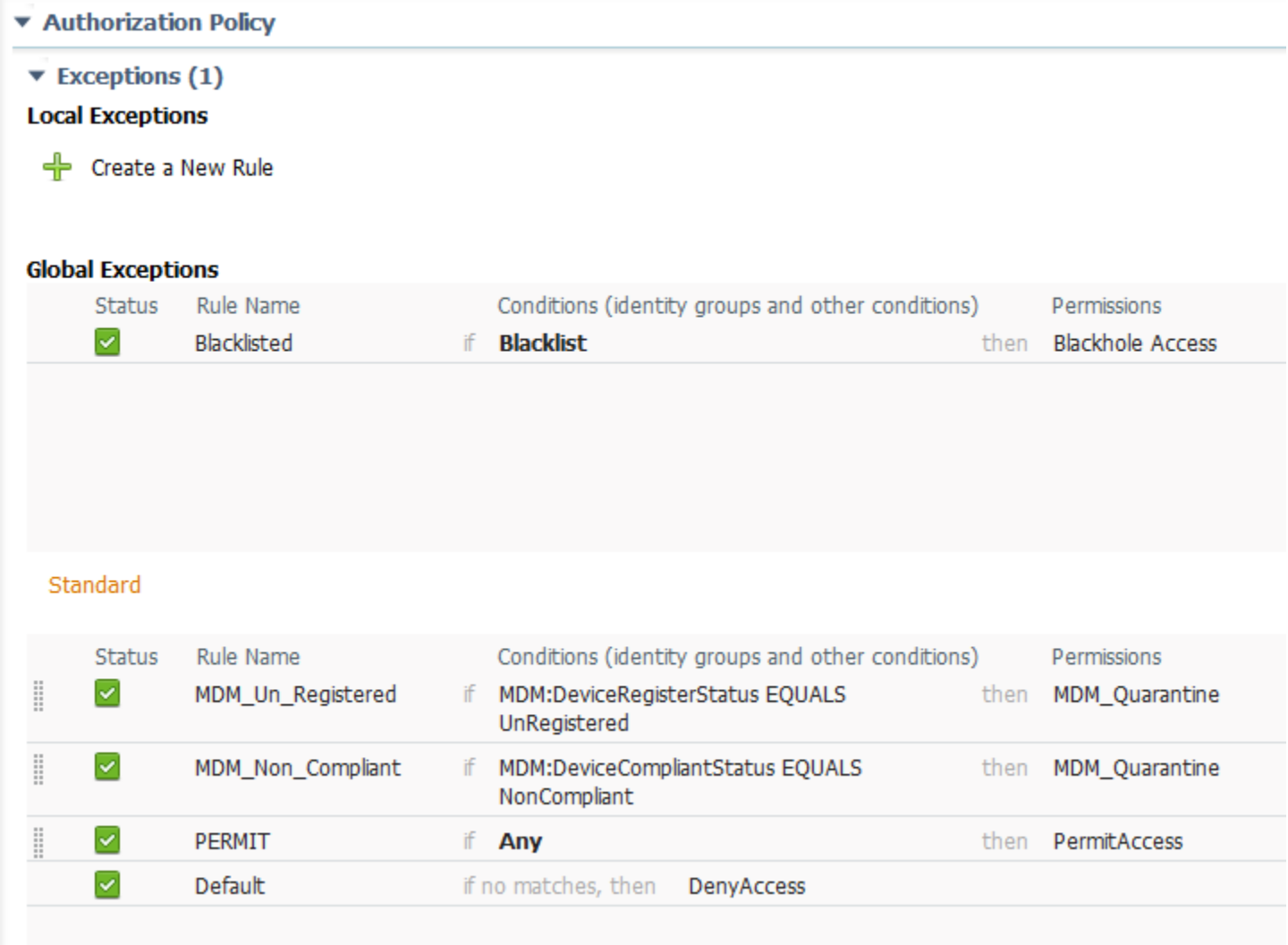
- Configure ACLs on the wireless LAN controller.
- Configure an authorization profile that will redirect devices that are not activated on BlackBerry UEM. For more information, see Redirecting devices that are not activated on BlackBerry UEM.
- Configure authorization policy rules that determine how Cisco ISE handles devices that are not activated on BlackBerry UEM or compliant with BlackBerry UEM. In **Policy > Policy Sets**, create a policy. For an example policy, see Example: Authorization policy rules for BlackBerry UEM.

Example: Authorization policy rules for BlackBerry UEM

Authentication policy



Authorization policy



Managing network access and device controls using Cisco ISE

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

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

Redirecting devices that are not activated on BlackBerry UEM

If Cisco Identity Services Engine (ISE) identifies a device that is trying to access the work network (Wi-Fi or VPN), and the device is not activated on UEM, Cisco ISE opens an enrollment page in the device browser that redirects the user to the BlackBerry UEM Self-Service console.

The user requires a UEM user account to log in to BlackBerry UEM Self-Service and activate the device. Instruct users to contact the UEM administrator if Cisco ISE directs them to the enrollment page.

Note: If a user's device was previously activated with UEM then deactivated, the user is not redirected to BlackBerry UEM Self-Service when the user tries to access the work network from the device. To resolve this issue, when you remove a device from UEM, delete the data for that device from Cisco ISE.

Legal notice

©2023 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Patents, as applicable, identified at: www.blackberry.com/patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

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

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

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

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

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

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

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

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

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

Published in Canada