BlackBerry BRIDGE

Administration Guide

3.19

Contents

What is BlackBerry BRIDGE?..... 5

Architecture: BlackBerry BRIDGE in an on-premises BlackBerry UEM environment..... 6

Architecture: BlackBerry BRIDGE in a BlackBerry UEM Cloud environment..... 8

Data flow: Sending documents between BlackBerry Work and Microsoft Intune managed apps using the BlackBerry BRIDGE app..... 9

Data flow: Sending documents between Microsoft Intune-managed apps and BlackBerry Dynamics apps using the BlackBerry BRIDGE app..... 10

Steps to manage BlackBerry BRIDGE in an on-premises BlackBerry UEM environment..... 12

Steps to manage BlackBerry BRIDGE in a BlackBerry UEM Cloud environment..... 13

System requirements..... 14

Connecting BlackBerry UEM to Microsoft Entra ID..... 15

Create a Microsoft Entra ID account..... 15

Configure BlackBerry UEM to synchronize with Entra Active Directory..... 16

Synchronize Microsoft Active Directory with Microsoft Entra ID..... 16

Create an enterprise endpoint in Entra..... 16

Configuring BlackBerry UEM to synchronize with Microsoft Intune..... 18

Configure BlackBerry UEM to synchronize with Microsoft Intune in BlackBerry UEM..... 18

Managing the BlackBerry BRIDGE app..... 19

Adding the Intune managed mobile apps to the app list..... 19

View public BlackBerry Dynamics app entitlements..... 19

Grant tenant-wide admin consent to the BlackBerry BRIDGE app..... 19

Update the app list..... 20

Creating directory-linked groups..... 21

Create a directory-linked group..... 21

Managing apps protected by Microsoft Intune..... 23
Create a Microsoft Intune app protection profile..... 23
Turn off interoperability between BlackBerry Dynamics apps and app managed by Intune..... 25
Assign the Intune app protection profile to a directory-linked group 25

Options for installing and activating BlackBerry BRIDGE..... 27
Install BlackBerry BRIDGE using the BlackBerry UEM Client on iOS devices..... 27
Install BlackBerry BRIDGE using the BlackBerry UEM Client on Android devices..... 28
Install BlackBerry BRIDGE from the App Store on iOS devices..... 29
Install BlackBerry BRIDGE from Google Play on Android devices..... 29

Using BlackBerry BRIDGE with Microsoft Authenticator on Android devices....31

Wipe apps managed by Microsoft Intune..... 32

Troubleshooting BlackBerry BRIDGE..... 33
Change the log level to Warn for Microsoft Intune customers..... 33
Upload log files to BlackBerry Support..... 33
Unable to save a copy of a file in the Intune-managed app..... 33

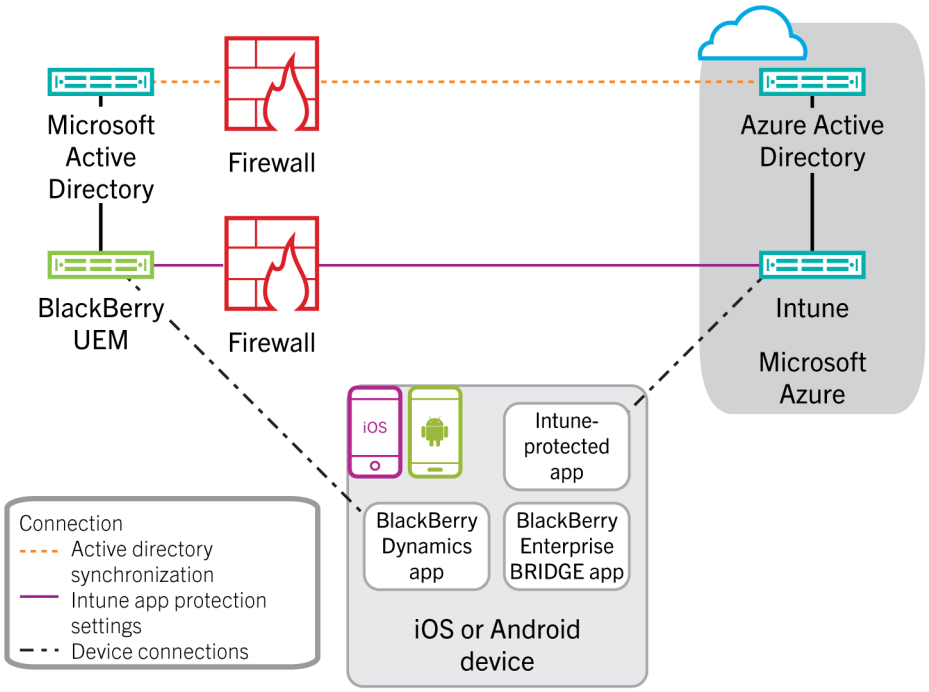
Legal notice..... 34

What is BlackBerry BRIDGE?

BlackBerry BRIDGE is a Microsoft Intune app that is enabled for BlackBerry Dynamics. It allows you to securely view, edit, and save documents using Intune managed Microsoft apps, such as Microsoft Office, Microsoft Word, Microsoft PowerPoint, Microsoft Excel, Microsoft Teams, Microsoft OneNote, and Microsoft Viva Engage in BlackBerry Dynamics on iOS and Android devices. The following are the features of BlackBerry BRIDGE.

Feature	Description
Secure sharing and storing of data	Share your documents as email attachments (requires BlackBerry Work). Maintain data encryption during the document-sharing process between BlackBerry Dynamics apps and Intune managed mobile apps.
Document access, create, and editing	Access documents while you are on the go from native Microsoft mobile apps. View, create, edit, and save documents.
User experience	Seamlessly transfer files to native Microsoft mobile apps from within BlackBerry Work and from native Microsoft mobile apps to BlackBerry Dynamics apps.
Document fidelity	Documents are rendered with Microsoft native fidelity on all devices.
PDF slide show presentation tool	On iOS devices, use BlackBerry BRIDGE to present PDF slide shows.

Architecture: BlackBerry BRIDGE in an on-premises BlackBerry UEM environment

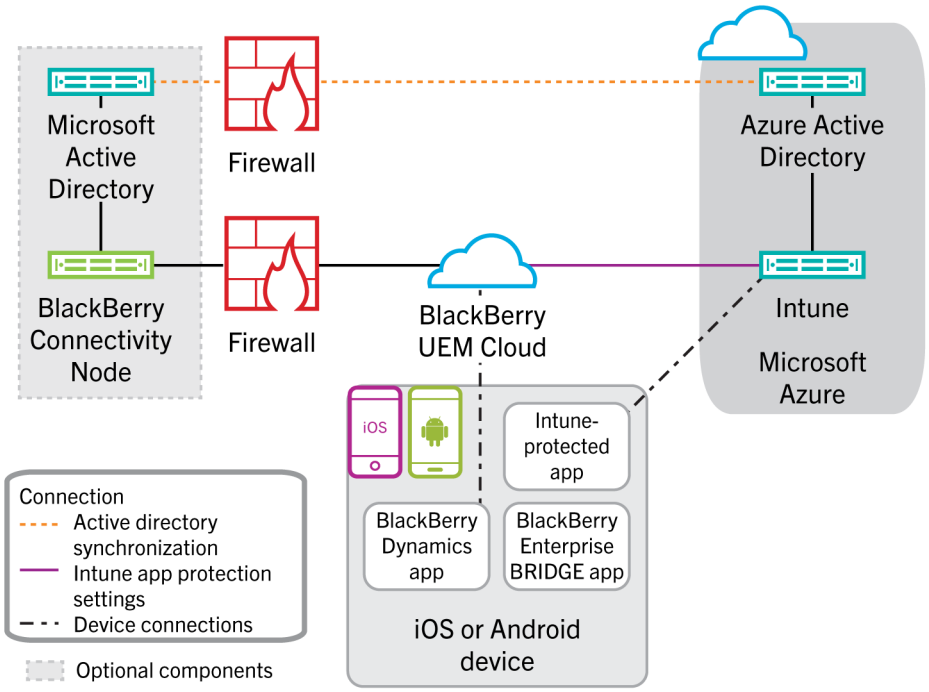


Note: Each directory-linked group can link to only one company directory. For example, if BlackBerry UEM has two Microsoft Active Directory connections (A and B), and you create a directory-linked group that is linked to connection A, you can link only to directory groups from connection A. You must create new directory linked groups for any other directory connections.

Component	Description
BlackBerry UEM Core	The BlackBerry UEM Core is the central component of the BlackBerry UEM architecture. It consists of several subcomponents that are responsible for: • Logging, monitoring, reporting, and management functions • Authentication and authorization services for the BlackBerry UEM Core local directory and company directories • Scheduling and sending commands, IT policies, and profiles to devices
Microsoft Intune	Microsoft Intune is a cloud-based EMM service that provides both MDM and MAM features. Intune MAM provides security features for apps such as Microsoft 365 that protect data within apps.
Microsoft Entra ID	Microsoft Entra ID is the Microsoft cloud computing service for deploying and managing apps and services.

Component	Description
Microsoft Graph API	The Microsoft Graph API connects the BlackBerry UEM MAM and Intune app protection profile to Intune and synchronizes the Microsoft Intune app protection profile settings to Intune. This is one-way synchronization from BlackBerry UEM to Intune.
Devices	The BlackBerry BRIDGE app is supported on Android and iOS devices.

Architecture: BlackBerry BRIDGE in a BlackBerry UEM Cloud environment



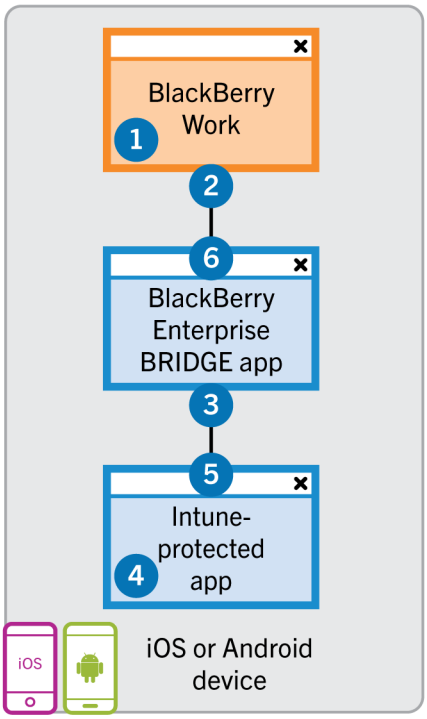
Note: Each directory-linked group can link to only one company directory. For example, if BlackBerry UEM has two Microsoft Active Directory connections (A and B), and you create a directory-linked group that is linked to connection A, you can link only to directory groups from connection A. You must create new directory linked groups for any other directory connections.

Component	Description
BlackBerry UEM Cloud	BlackBerry UEM Cloud is a service that allows you to manage devices used in your organization's environment.
BlackBerry Connectivity Node (BlackBerry Cloud Connector component)	The BlackBerry Connectivity Node is a collection of BlackBerry UEM Cloud components that you install inside your organization's firewall. It has five components, including the BlackBerry Cloud Connector, that add functionality to BlackBerry UEM Cloud. The BlackBerry Connectivity Node is required if your environment needs to connect to on on-premises Active Directory. It is not required if you use Microsoft Entra ID Active Directory. The BlackBerry Cloud Connector connects the BlackBerry UEM Cloud to your on-premises Active Directory behind the firewall to allow basic attribute synchronization, search functionality, and user authentication services. For information about the other BlackBerry Connectivity Node components, see the BlackBerry UEM Cloud Administration content. The BlackBerry Connectivity Node uses port 3101 to communicate with BlackBerry UEM Cloud.

Component	Description
Microsoft Active Directory	BlackBerry UEM Cloud supports connectivity with your organization's Microsoft Active Directory or LDAP company directory behind the firewall using the BlackBerry Connectivity Node.
Microsoft Intune	Microsoft Intune is a cloud-based EMM service that provides both MDM and MAM features. Intune MAM provides security features for apps such as Microsoft 365 that protect data within apps.
Microsoft Entra ID Active Directory	Microsoft Entra ID Active Directory is a cloud-based directory management service.
Microsoft Entra ID	Microsoft Entra ID is the Microsoft cloud computing service for deploying and managing apps and services.
Microsoft Graph API	The Microsoft Graph API connects the BlackBerry UEM MAM and Intune app protection profile to Intune and synchronizes the Microsoft Intune app protection profile settings to Intune. This is one-way synchronization from BlackBerry UEM to Intune.
Devices	The BlackBerry BRIDGE app is supported on Android and iOS devices.

Data flow: Sending documents between BlackBerry Work and Microsoft Intune managed apps using the BlackBerry BRIDGE app

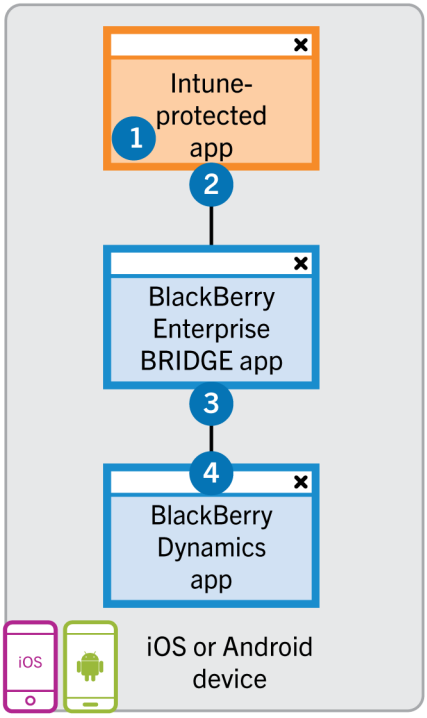
This data flow shows how to share documents that are received as email attachments in BlackBerry Work or saved to the Local Docs folder or an Enterprise remote Docs location to Intune managed apps on Android and iOS devices when the BRIDGE app is installed. In this example, a user opens a Microsoft Word document that has been received as an email attachment and that requires feedback.



1. The user downloads and previews a file received as an email attachment in BlackBerry Work.
2. If the Microsoft Intune app protection policy profile allows it, the device sends a copy of the file using the AppKinetics Transfer File service through secured channels to the BRIDGE app.
3. The BRIDGE app securely sends a copy of the file over an Intune protected channel to the Intune managed app (for example, Microsoft Word). The BRIDGE app deletes the copy of the file within the BRIDGE app after the file transfer is complete.
4. The user preforms the following actions:
   a. Saves a copy of the file in an Intune protected area of the Intune managed app.
   b. Modifies the file as required and saves the updated file.
5. The device sends a copy of the file back to the BRIDGE app over the Intune protected channel.
6. The BRIDGE app sends the copy of the file to BlackBerry Work using the AppKinetics Transfer File service through secured channels to attach to the original or a new email or to save to the Local Docs folder or an Enterprise remote Docs location. The BRIDGE app deletes the copy of the file within the BRIDGE app after the file transfer is complete.

Data flow: Sending documents between Microsoft Intune-managed apps and BlackBerry Dynamics apps using the BlackBerry BRIDGE app

This data flow shows how to share documents that are created in supported Intune-managed apps and BlackBerry Dynamics apps on Android and iOS devices when the BRIDGE app is installed. In this example, a user creates a new file in Microsoft Word and sends the file to the manager for review.



1. The user performs the following actions:
   - Creates a file in Microsoft Word.
   - Saves a copy of the file in an Intune protected area of the Intune-managed app.
2. The device sends a copy of the file to the BRIDGE app over the Intune protected channel.
3. The user selects to Send Email.
4. If the Microsoft Intune app protection policy profile allows it, the BRIDGE app sends a copy of the file to BlackBerry Work using the AppKinetics Transfer File service through secured channels to attach to an email (or to save to the Local Docs folder or an Enterprise remote Docs location). The BRIDGE app deletes the copy of the file within the BRIDGE app after the file transfer is complete.

Steps to manage BlackBerry BRIDGE in an on-premises BlackBerry UEM environment

When you configure your environment for BlackBerry BRIDGE, you perform the following actions.

Note: Some of these tasks might have been completed when you installed and configured BlackBerry UEM.

Step	Action
1	Review system requirements.
2	Install BlackBerry UEM or upgrade to the latest version of BlackBerry UEM. For instructions, see the BlackBerry UEM Installation and Upgrade content.
3	Connect BlackBerry UEM to Microsoft Entra ID.
4	Configure BlackBerry UEM to synchronize with Microsoft Intune.
5	Configure BlackBerry Work and make it available to users. For instructions, see the BlackBerry Work administration content for details.
6	Make the BlackBerry BRIDGE app available to users. Optionally, users can download and install the app from the App Store or Google Play.
7	Make the Microsoft PowerPoint, Microsoft Word, Microsoft Excel, Microsoft Excel, Microsoft Teams, Microsoft OneNote, and Microsoft Viva Engage apps available to users. Users can download and install the apps from the App Store or Google Play.
8	Create one or more directory-linked groups and assign the apps to the directory-linked group.
9	Assign a Microsoft Intune app protection profile to a directory-linked group.
10	Instruct users to install and activate the BlackBerry BRIDGE app on their devices.

Steps to manage BlackBerry BRIDGE in a BlackBerry UEM Cloud environment

When you configure your environment for BlackBerry BRIDGE, you perform the following actions.

Note: Some of these tasks might have been completed when you installed and configured BlackBerry UEM.

Step	Action
1	Review system requirements.
2	Make sure that a BlackBerry UEM Cloud tenant is available in your environment.
3	If you use an on premise Active Directory, install the most recent version of the BlackBerry Connectivity Node (BlackBerry Cloud Connector component). For instructions, see Configuring BlackBerry UEM. The BlackBerry Connectivity Node is not required if you use Microsoft Entra ID Active Directory for your directory.
4	Connect BlackBerry UEM Cloud to Microsoft Entra ID.
5	Configure BlackBerry UEM Cloud to synchronize with Microsoft Intune.
6	Configure BlackBerry Work and make it available to users. For instructions, see the BlackBerry Work administration content for details.
7	Make the BlackBerry BRIDGE app available to users. Optionally, users can download and install the app from the App Store or Google Play.
8	Make the Microsoft PowerPoint, Microsoft Word, Microsoft Excel, Microsoft Teams, Microsoft OneNote, and Microsoft Viva Engage apps available to users. Users can download and install the apps from the App Store or Google Play.
9	Create one or more directory-linked groups and assign the apps to the directory-linked group.
10	Assign a Microsoft Intune app protection profile to a directory-linked group.
11	Instruct users to install and activate the BlackBerry BRIDGE app on their devices.

System requirements

To use BlackBerry BRIDGE, your organization must meet the following requirements:

Item	Description

Server requirements	• For an on-premises BlackBerry UEM environment,
	  • An on-premises BlackBerry UEM
	  • BlackBerry UEM must be connected to a Microsoft Active Directory instance. For more information, see the BlackBerry UEM Configuration content for details.
	  • Microsoft Intune tenant in Microsoft Entra ID
	• For a BlackBerry UEM Cloud environment,
	  • A BlackBerry UEM Cloud tenant
	  • Microsoft Intune tenant in Microsoft Entra ID

Services	Microsoft Entra ID account with appropriate permissions and required licenses. For more information about account permissions, visit https://support.blackberry.com/community to read article 50341.
Device OS	For device OS compatibility, see the Mobile/Desktop OS and Enterprise Applications Compatibility Matrix

Apps	• The following apps and required licenses:
	  • Microsoft Office
	  • Microsoft Word
	  • Microsoft PowerPoint
	  • Microsoft Excel
	  • Microsoft Teams
	  • Microsoft OneNote
	  • Microsoft Viva Engage
	• One or more BlackBerry Dynamics apps for example, BlackBerry Work version 2.18 or later and entitlement.
	  Note: Some elements of the features that are are included with this release require an updated BlackBerry Work app. An updated BlackBerry Work app will be released in the near future.
	• For Android devices, make sure that the Microsoft Intune Company Portal app is installed on devices but not activated. For more information, see https://docs.microsoft.com/en-us/mem/intune/fundamentals/end-user-mam-apps-android#access-apps.

Connecting BlackBerry UEM to Microsoft Entra ID

Microsoft Entra ID is the Microsoft cloud computing service for deploying and managing apps and services. You must connect BlackBerry UEM to Entra if you want to use BlackBerry UEM to deploy iOS and Android apps managed by Microsoft Intune.

In a BlackBerry UEM Cloud environment, if your organization uses Microsoft Active Directory instead of Entra Active Directory, to connect with Entra you must install the most recent version of the BlackBerry Connectivity Node to allow BlackBerry UEM Cloud to access your company directory. For instructions, see the BlackBerry UEM Configuration content.

Note: You must use the Microsoft Entra ID account with appropriate permissions to complete these tasks. For more information about account permissions, visit https://support.blackberry.com/community to read article 50341.

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

Step	Action
1	Create a Microsoft Entra ID account.
2	If you use BlackBerry UEM Cloud and your organization uses Entra Active Directory, configure BlackBerry UEM Cloud to synchronize with Entra Active Directory.
3	If your organization uses an on-premises Microsoft Active Directory and you want to use BlackBerry UEM to deploy apps managed by Microsoft Intune apps, Synchronize Microsoft Active Directory with Microsoft Entra ID.
4	Create an enterprise endpoint in Entra to allow the on-premises BlackBerry UEM or BlackBerry UEM Cloud to connect to Microsoft Intune.
5	Configure BlackBerry UEM to synchronize with Microsoft Intune.

Create a Microsoft Entra ID account

To deploy apps protected by Microsoft Intune to iOS and Android devices in BlackBerry UEM, you must have a Microsoft Entra ID account and authenticate BlackBerry UEM with Entra.

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

1. Go to https://azure.microsoft.com and click **Free account**. Follow the instructions to create the account.
   You are required to provide credit card information to create the account.
2. Sign in to the Entra management portal at https://entra.microsoft.com and log in with the username and password you created when you created your account.

After you finish: Synchronize Microsoft Active Directory with Microsoft Entra ID.

Configure BlackBerry UEM to synchronize with Entra Active Directory

Complete this task only if your environment is using BlackBerry UEM Cloud.

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

1. Log in to the Entra portal and go to the app that your organization uses to allow connections to Entra Active Directory.

   For more information, see Quickstart: Register an application in Microsoft Entra ID.
2. Add your BlackBerry UEM Cloud tenant URL to the list of **Redirect URLs** for the app and click **Save**.
3. In the management console, click **Settings > External integration > Company directory**.
4. Click + beside **Microsoft Azure Active Directory connection**.
5. Enter a **Directory connection name** and the **Domain** for your Entra Active Directory.
6. Click **Continue**.
7. Enter the Microsoft user ID and password associated with the app.
8. Click **Accept**.
9. Click **Save**.

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

Synchronize Microsoft Active Directory with Microsoft Entra ID

To send apps protected by Microsoft Intune to iOS and Android devices, users must exist in the Microsoft Entra ID directory. Synchronize users and groups between your on-premises Active Directory and Entra Active Directory using Microsoft Entra ID Connect. For more information, visit https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect.

Before you begin: Create a Microsoft Entra ID account

1. Download Entra ID Connect from http://www.microsoft.com/en-us/download/details.aspx?id=47594.
2. Install the Entra ID Connect software.
3. Configure Entra ID Connect to connect your on-premises Active Directory with the Entra Active Directory.

After you finish: Create an enterprise endpoint in Entra

Create an enterprise endpoint in Entra

To give BlackBerry UEM access to Microsoft Entra ID you must create an enterprise endpoint within Entra. The enterprise endpoint allows BlackBerry UEM to authenticate with Microsoft Entra ID. For more information, see the Microsoft resource Quickstart: Register an application in Microsoft Entra ID.

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

Note: When you create the application to use Microsoft Intune (step 11), you must use the Entra account with Global administrator permissions.

Before you begin:

- Synchronize Microsoft Active Directory with Microsoft Entra ID
- If you use modern authentication, make sure that you have the Reply URL. For instructions on obtaining the Reply URL for modern authentication, see Configure BlackBerry UEM to synchronize with Microsoft Intune in BlackBerry UEM.

1. Log in to the Entra portal.
2. In the left column, click **Applications > App registrations**.
3. Click **Endpoints**.
4. Copy the **OAuth 2.0 token endpoint (v1)** value and paste it to a text file.

   This is the **OAuth 2.0 token endpoint** required in BlackBerry UEM.
5. Close the **Endpoints** list and click **New registration**.
6. In the **Name** field, enter a name for the app.
7. Select a supported account type.
8. In the **Redirect URI** section, in the drop-down list, select **Web** and enter a valid URL. The URL format is https://<*FQDN_of_the_BlackBerry_UEM_server*>:<*port*>/admin/intuneauth
   - If you use client credentials authentication or don't have a registered domain, you can use: `http://localhost/`
   - If you use modern authentication, enter the Reply URL from the BlackBerry UEM. For instructions, see Configure BlackBerry UEM to synchronize with Microsoft Intune in BlackBerry UEM.
9. Click **Register**. The new registered app appears.
10. Copy the **Application ID** of your app and paste it to a text file.

    This is the **Client ID** required in BlackBerry UEM.
11. If you are creating the application to use Microsoft Intune. click **API permissions** in the **Manage** section. Perform the following steps.
    a) Click **Add a permission**.
    b) Select **Microsoft Graph**.
    c) Select **Delegated permissions**.
    d) Scroll down in the permissions list and under **Delegated Permissions**, set the following permissions for Microsoft Intune:
       - **DeviceManagementApps.ReadWrite.All** (Read and write Microsoft Intune apps)
       - **User.ReadBasic.All** (Read all users' basic profiles)
       - **Group.Read.All** (Read all groups)
    e) Click **Add permissions**.
    f) Under **Grant consent**, click **Grant admin consent**.

       Note: You must be a global administrator to grant permissions.
    g) When you are prompted, click **Yes** to grant permissions for all accounts in the current directory.
12. Select **Certificates and secrets** in the **Manage** section. Perform the following actions:
    a) Under **Client secrets**, click **New client secret**.
    b) Type a description for the client secret
    c) Select a duration for the client secret.
    d) Click **Add**.
    e) Copy the value of the new client secret.

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

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

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

Configuring BlackBerry UEM to synchronize with Microsoft Intune

Microsoft Intune is a cloud-based EMM service that provides both MDM and MAM features. Intune MAM provides security features for apps, including Office 365 apps, that protect data within apps. For example, Intune can require that data within apps be encrypted and prevent copying and pasting, printing, and using the Save as command.

After you connect BlackBerry UEM to Microsoft Intune, you can use the UEM management console to create and modify Microsoft Intune app protection profiles.

Before you configure BlackBerry UEM to synchronize with Microsoft Intune, you must connect BlackBerry UEM to Microsoft Azure.

Configure BlackBerry UEM to synchronize with Microsoft Intune in BlackBerry UEM

Before you begin: Connect BlackBerry UEM to Microsoft Entra ID and create an enterprise endpoint in Entra. For more information, see Create an enterprise endpoint in Entra.

Note: The Client Credentials authentication method has been removed in BlackBerry UEM 12.14 and later. For existing servers that have been upgraded to UEM 12.14, the administrator must take action to migrate the configuration to Modern Authentication. New integrations created in BlackBerry UEM 12.14 or later will not have the Client Credentials option available. For more information, visit support.blackberry.com/community to read article 80612.

1. Log in to the BlackBerry UEM management console.
2. Click **Settings > External Integration > Microsoft Intune**.
3. Enter the the following information that you copied from the Entra portal when you created the enterprise app in Entra:
   - **Azure Tenant ID**: The ID of the Azure Active Directory where you registered the app
   - **Client ID**: The application ID generated by the Entra app registration
   - **Client key**: The client secret generated by the Entra app registration
4. Confirm the **Reply URL**. The **Reply URL** field is automatically populated with the web address of the BlackBerry UEM management console. This URL is required when you create the enterprise endpoint in Microsoft Entra ID. For more information, see connecting BlackBerry UEM to Microsoft Azure.

   Note: The Reply URL is automatically derived from the %AdminPortalURL% default variable. By default, this variable will be set to the first UEM Core server installed in the environment. This variable can be modified by going to Settings > General Settings > Default Variables. For more information, see the BlackBerry UEM Managing device configurations content.
5. Click **Next**.

After you finish: Create a Microsoft Intune app protection profile

Managing the BlackBerry BRIDGE app

To permit users to use BlackBerry BRIDGE, you must complete the following actions:

Step	Action
1	Add the public BlackBerry BRIDGE app from the BlackBerry Marketplace for Enterprise Software to the app list in the BlackBerry UEM console.
2	Assign the app to user accounts or directory-linked groups.
3	Purchase the entitlement (com.blackberry.intune.bridge) and assign it to each user that you assign the BlackBerry BRIDGE app to.
4	Grant tenant-wide admin consent to the BlackBerry BRIDGE app.

Adding the Intune managed mobile apps to the app list

You can add the Microsoft Intune managed mobile apps, Microsoft Word, Microsoft PowerPoint, and Microsoft Excel to the app list from the App Store or Google Play. After the apps are added to the app list, you can assign them to users. Optionally, users can download the apps from the App Store or Google Play. For more information about adding iOS apps or Android apps to the app list, see the BlackBerry UEM administration content.

View public BlackBerry Dynamics app entitlements

1. Log in to https://account.blackberry.com.
2. Expand **Entitlements**.

Grant tenant-wide admin consent to the BlackBerry BRIDGE app

BlackBerry BRIDGE uses a new client app identifier and requires admin consent on the app within your Microsoft Entra tenant to access resources within the Entra portal. If you do not grant admin consent, users might receive an "admin approval is required" message and will be unable to use the app. Verify that users are running BlackBerry BRIDGE version 3.17.2 or later.

1. Use one of the following methods in the Microsoft resource Grant tenant-wide admin consent to an application to grant consent:
   - Grant tenant-wide admin consent in Enterprise apps pane
   - Grant admin consent in App registrations pane
2. Create the URL using the new client identifier to grant the app tenant-wide admin consent. Verify that you use the client ID: 970e35b7-b4de-4e5e-bc1b-db8fed6529c1

Update the app list

You can update the app list to make sure that you have the latest information about iOS and Android apps in the apps list. Updating the app information does not mean that the app is updated on a user's device. Users receive update notifications for their work apps in the same way that they receive update notifications for their personal apps.

1. On the menu bar, click **Apps**.
2. Click .

Creating directory-linked groups

You can create groups in BlackBerry UEM that are linked to one or more groups in your company directory. These BlackBerry UEM groups are called "directory-linked groups." Only directory user accounts can be members of a directory-linked group.

Important: You must create directory-linked groups because Microsoft Intune app protection profiles can be assigned only to directory-linked groups. The directory-linked group must be a security group in Microsoft Active Directory. If the group is a distribution group, users won't have the appropriate permissions and cannot log in after the BRIDGE app is installed on their device. For more information on Microsoft Intune app protection profiles, see Managing apps protected by Microsoft Intune

At a scheduled interval, BlackBerry UEM automatically synchronizes the membership of a directory-linked group with its associated company directory group or groups. Users that were added or removed from the company directory group are added or removed from the directory-linked group.

Note: When users are moved into a company directory group that is linked to a directory-linked group, they are assigned the policies, profiles, and apps that are assigned to the group. When users are removed from a company directory group that is linked to a directory-linked group, the policies, profiles, and app are removed from the user.

Each directory-linked group can link to only a single company directory. For example, if BlackBerry UEM has two Microsoft Active Directory connections (A and B), and you create a directory-linked group that is linked to connection A, you can link only to directory groups from connection A. You must create new directory linked groups for any other directory connections.

To enable this feature, see the following:

- In an on-premises BlackBerry UEM environment, see Enable directory-linked groups in the Configuration content.
- In a BlackBerry UEM Cloud environment, see Enable directory-linked groups in the Configuration content

Synchronizing directory-linked groups does not add or delete users in BlackBerry UEM. To allow BlackBerry UEM to create user accounts when new company directory users are created, you must enable and configure onboarding. For more information,

- In an on-premises BlackBerry UEM environment, see Enabling onboarding in the Configuration content.
- In a BlackBerry UEM Cloud environment, see Enabling onboarding in the Configuration content.

Create a directory-linked group

Before you begin:

- Enable directory-linked groups. For instructions, see
  - In an on-premises BlackBerry UEM environment, see Enabling onboarding in the Configuration content.
  - In a BlackBerry UEM Cloud environment, see Enabling onboarding in the Configuration content.
- Make sure that the directory-linked group is a security group and not a distribution group in Microsoft Active Directory.

1. On the menu bar, click **Groups**.
2. Click .
3. Type the group name.
4. In the **Linked directory groups** section, perform the following actions:
   a) Click +.

b) Type the name or partial name of the company directory group you want to link to.
c) If you have more than one company directory connection, select the connection that you want to search. After you have made this selection, the directory-linked group is permanently associated with the selected connection.
d) Click .
e) Select the company directory group in the search results list.
f) Click **Add**. The company directory group displays in the list and the company directory connection the group is linked to displays beside the section title.
g) If necessary, select the **Link nested groups** check box. You can leave the check box unselected to link to all nested groups, or you can select the check box to allow the directory settings to control the number of nested groups.
h) Repeat these steps to link additional groups.

5. To assign a user role to the directory-linked group, perform the following actions:
   a) In the **User role** section, click .
   b) In the drop-down list, click the name of the user role that you want to assign to the group.
   c) Click **Add**.
6. To assign an IT policy or profile to the directory-linked group, perform the following actions:
   a) In the **IT policy and profiles** section, click .
   b) Click **IT policy** or a profile type.
   c) In the drop-down list, click the name of the IT policy or profile that you want to assign to the group.
   d) Click **Assign**.
7. To assign an app to the directory-linked group, in the **Assigned apps** section, click .
8. Search for the app.
9. In the search results, select the app.
10. Click **Next**.
11. In the **Disposition** drop-down list for the app, perform one of the following actions:
    - To install the app automatically on devices, and to prevent users from removing the app, select **Required**. This option is not available for BlackBerry apps.
    - To permit users to install and remove the app, select **Optional**.
12. For iOS devices, to assign per-app VPN settings to an app or app group, in the **Per app VPN** drop-down list for the app or app group, select the settings to associate with the app or app group.
13. Click **Assign**.
14. Click **Add**.

Managing apps protected by Microsoft Intune

For iOS and Android devices, if you want to use Microsoft Intune app protection policies to protect data in Office 365 apps, you can do so while using BlackBerry UEM to manage the devices. You can connect BlackBerry UEM to Intune, allowing you to set Microsoft Intune app protection policies from within the BlackBerry UEM management console. A new app protection policy for iOS devices allows you to display only the Microsoft Intune managed apps that support the document type that users share to Intune managed apps. In this release, this feature must be enabled in the Microsoft Entra ID portal. In an upcoming release of BlackBerry UEM, administrators will be able to enable this feature in the BlackBerry UEM console or in the Microsoft Entra ID portal.

To deploy apps protected by Intune, you must first configure the connection between BlackBerry UEM and Intune. For more information, see Connecting BlackBerry UEM to Microsoft Entra ID.

Intune uses app protection policies to protect apps. To protect apps from the BlackBerry UEM management console, you create an Intune app protection profile. When you create or update an app protection profile in BlackBerry UEM, the settings are sent to Intune and update the settings in the corresponding app protection policy.

Warning:

- If you update the Intune app protection policy in the Entra portal, the changes are not synchronized with BlackBerry UEM. After you create a Microsoft Intune app protection profile in BlackBerry UEM, you can enable the feature for iOS devices in the corresponding policy in the Entra portal. Modifying or deleting any other settings in the Entra portal can prevent other users from activating BlackBerry BRIDGE.
- Creating an Intune policy in Entra and assign it to a directory-linked group that includes users that are managed by BlackBerry UEM is not supported.

Create a Microsoft Intune app protection profile

When you create or update a Microsoft Intune app protection profile in BlackBerry UEM, the profile settings are sent to Intune to update the corresponding app protection policy. Microsoft Intune app protection profiles can be assigned only to directory-linked groups. You can enable a new policy for iOS devices to display only the Microsoft Intune-managed apps that support the document type that users share to Microsoft Intune apps. In this release, this feature must be enabled in the Microsoft Entra ID portal. In an upcoming release of BlackBerry UEM, administrators will be able to enable this feature in the BlackBerry UEM console or in the Microsoft Entra ID portal.

Note: The Microsoft Intune app protection profile settings are sent to Intune and update the settings in the corresponding app protection policy. In the Entra portal, you can then enable the 'Send org data to other apps' policy to display only the Microsoft Intune-managed apps that support the document type that iOS users share to Intune managed apps. Modifying or deleting any other settings in Entra can prevent other users from activating BlackBerry BRIDGE.

For more information about Microsoft Intune app protection profile settings, see Create a Microsoft Intune app protection profile. If you configure the Microsoft Intune app protection profile to Prevent Save as and allow users to save files to a Local storage, users receive the error message "Action Not Allowed. Your organization only allows you to open work or school data in this app" when they try to send a file from the device to a not secure local storage. Files must be opened from a corporate location (for example, a secured local storage, Microsoft OneDrive for Business or Microsoft SharePoint).

Before you begin:

- Make sure that you configure BlackBerry UEM to synchronize with Microsoft Intune. The Microsoft Intune app protection profile does not appear on the Policies and Profiles page if the connection isn't configured.
- For Android devices, make sure the Microsoft Company Portal app is installed on devices but not activated. For more information, see https://docs.microsoft.com/intune/app-protection-enabled-apps-android.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Protection > Microsoft Intune app protection profile**.
3. Click +.
4. Type a name and description for the profile.
5. Select the **Enable interoperability between Intune and Dynamics apps** checkbox.

   When you enable this feature, the following policy settings are set to Policy Managed apps only and cannot be changed for security reasons such as enforcing data to remain within the intune protected secure environment:

   - Allow app to transfer data to other apps
   - Allow app to receive data from other apps
6. Optionally, in the custom JSON field, edit the JSON values if you want to customize messages and warning seen by your users in the BRIDGE app.
7. Select the **Prevent Save as** checkbox and select one or more of the following options to prevent users from sharing saved files to the following locations:

   - Local storage: Allows users to save a copy of the file in the Intune-managed app.
   - OneDrive for Business
   - SharePoint

   Note: If you want users to share files from Microsoft Teams, you must clear the **Prevent Save as** checkbox.
8. Add the required App packages for devices in your organization.
   a) Beside the App package IDs, click +.
   b) Select the appropriate App package IDs.
      - For Microsoft Office
        - On iOS devices, select com.microsoft.officemobile
        - On Android devices, select com.microsoft.office.officehubrow
      - For Microsoft Excel, select com.microsoft.office.excel
      - For Microsoft PowerPoint, select com.microsoft.office.powerpoint
      - For Microsoft Word, select com.microsoft.office.word
      - For Skype for Business, select com.microsoft.skype.teams
      - For Microsoft OneNote, select com.microsoft.onenote
      - For Microsoft Viva Engage
        - On iOS devices, select wefwef
        - On Android devices, select com.yammer.v1
9. Select the following apps:
   - For Microsoft Office
     - On iOS devices, select com.microsoft.officemobile
     - On Android devices, select com.microsoft.office.officehubrow
   - For Microsoft Excel, select com.microsoft.office.excel
   - For Microsoft PowerPoint, select com.microsoft.office.powerpoint
   - For Microsoft Word, select com.microsoft.office.word
   - For Skype for Business, select com.microsoft.skype.teams
   - For Microsoft OneNote, select com.microsoft.onenote
   - For Microsoft Viva Engage
     - On iOS devices, select wefwef
     - On Android devices, select com.yammer.v1

10. Click **Save**.
11. Click **Add**.
12. Optionally for iOS devices, configure the corresponding app protection policy in the Entra portal to display only the Intune-managed apps that support the document type that is shared to Intune-managed apps.

    Note: If you modify the corresponding app protection policy in the Entra portal, subsequent updates must be completed in the portal. Do not modify other settings in the policy, or it might prevent other iOS users from activating BlackBerry BRIDGE.

    a. Sign in to the Microsoft Endpoint Manager admin center portal at https://endpoint.microsoft.com/.
    b. In the left column, click **Apps**.
    c. In the **Policy** section, click **App protection policies**.
    d. Search for and open the policy that was created in BlackBerry UEM and synchronized to Entra.
    e. Under **Manage**, click **Properties**.
    f. In the **Data protection** section, click **Edit**.
    g. In the **Send org data to other apps** drop-down list, select **Policy managed apps with Open-In/Share filtering**.
    h. Click **Review + save**.
    i. Click **Save**.

After you finish: Assign the Intune app protection profile to a directory-linked group.

Turn off interoperability between BlackBerry Dynamics apps and app managed by Intune

You can turn off interoperability between the BlackBerry BRIDGE app and Intune managed apps in your BlackBerry UEM and BlackBerry UEM Cloud management console. Turning off interoperability causes the BlackBerry BRIDGE app to stop working, but does not affect the functionality of other Intune managed apps. For example, users can view the content of a Microsoft Word file, but the files are not opened in the Intune protected area of Microsoft Word. The BlackBerry BRIDGE app is not uninstalled from the device.

Before you begin: Create a Microsoft Intune app protection profile.

1. In the management console, on the menu bar, click **Policies and Profiles**.
2. Click **Protection > Microsoft Intune app protection** profile.
3. Click the Microsoft Intune app protection profile that you want to turn off the interoperability feature for.
4. Click ✎.
5. Clear the **Enable interoperability between Intune and Dynamics apps** check box.
6. Click **Save**.

Assign the Intune app protection profile to a directory-linked group

Before you begin: Create a Microsoft Intune app protection profile.

Warning: If users are members of multiple directory-linked groups and each group is assigned a different Microsoft Intune app protection profile, the BlackBerry BRIDGE app might not activate successfully or function as expected.

1. On the menu bar, click **Groups**.
2. Search for the directory-linked group.
3. In the search results, click the name of the directory-linked group.
4. On the **Settings** tab, in the **Assigned profile** section, click +.
5. Click **Microsoft Intune app protection profile**.

6. In the drop-down list, click the name of the Intune app protection profile that you want to assign to the group.
7. Click **Assign**.

Options for installing and activating BlackBerry BRIDGE

Before users can begin using BlackBerry BRIDGE, it must be activated. The steps that users take to install the app depends on how you have configured your environment. If you have not yet configured your activation settings, see the managing BlackBerry Dynamic apps administration guide for steps on how to configure your environment to support BlackBerry Dynamics apps.

The following options are available for activating BlackBerry BRIDGE on iOS and Android devices:

- Install and activate BlackBerry BRIDGE using the BlackBerry UEM Client: This option provides users with a consistent, streamlined activation experience. Users need only their email address and an activation password and do not require an access key. Users must install the UEM Client to activate their devices with MDM. For this option to be available to users, you must allow the UEM Client to manage the activation of BlackBerry Dynamics apps. For more information, see BlackBerry Dynamics profile settings.
- Install and activate BlackBerry BRIDGE from the App Store or Google Play: Users choose this option if they are downloading and installing on their device, if they have not installed the UEM Client, or if you have not allowed the BlackBerry UEM Client to manage the activation of BlackBerry Dynamics apps.

Install BlackBerry BRIDGE using the BlackBerry UEM Client on iOS devices

You can send the following instructions to iOS and Android device users that are installing BlackBerry BRIDGE using the BlackBerry UEM Client.

Before you begin:

- Make sure that a BlackBerry Dynamics app, for example,BlackBerry Work, is installed and activated on your device.
- Make sure that the supported Microsoft Intune-managed apps are installed and activated on your device.

1. If the app was not automatically pushed to your device by your administrator, open your Work Apps app and install the BlackBerry BRIDGE app. If you do not see the BlackBerry BRIDGE app in your Work Apps app, contact your administrator to make the app available to you.
2. On your device, tap **BB Bridge**.
3. Tap **Login**.
4. On the **Microsoft Sign in** page, enter your email address.
5. Tap **Next**.
6. If your organization has a login page, enter your username.
7. Tap **Next**.
8. Enter your password.
9. Tap **Sign in**.
10. Tap **OK** to acknowledge that your organization protects the data in the app and to restart the app.
11. Tap **BB Bridge**.
12. If prompted, set a PIN or use Touch ID to access your organization's data using the BlackBerry BRIDGE app.
13. Read the license agreement and if you agree, tap **I agree**.
14. To activate the BlackBerry BRIDGE app, enter your password for the BlackBerry Dynamics app that is displayed in the activation request. For example, BlackBerry Work or BlackBerry UEM Client.
15. Tap **OK**.

16. If this is the first time that you have logged in to the BlackBerry BRIDGE app, the Tutorials screen opens and displays a list of tutorials. You can view the tutorials or tap **Close** to close the Tutorials screen.
17. In the reminder dialog box, tap **OK**. You can view the tutorial later from the Settings screen.

Install BlackBerry BRIDGE using the BlackBerry UEM Client on Android devices

You can send the following instructions to Android device users that are installing BlackBerry BRIDGE using the BlackBerry UEM Client.

Before you begin:

- Make sure the Microsoft Intune Company Portal app is installed on your device. You do not need to activate the app. For more information, see https://docs.microsoft.com/intune/app-protection-enabled-apps-android.
- Make sure that the supported Microsoft Intune managed apps are installed and activated on your device.
- Make sure that a BlackBerry Dynamics app, for example,BlackBerry Work, is installed and activated on your device.

1. If the app was not automatically pushed to your device by your administrator, open your Work Apps app and install the BlackBerry BRIDGE app. If you do not see the BlackBerry BRIDGE app in your Work Apps app, contact your administrator to make the app available to you.
2. On your device, tap **BRIDGE**.
3. Tap **Login**
4. If the Intune Company Portal app is not installed on your device, you are prompted with the **To use your work or school account with this app, you must install the Intune Company Portal app. Tap "Play Store" to continue** message. Tap **Play Store** to install the Microsoft Intune Company Portal app.
5. Tap **Login**
6. On the **Microsoft Sign in** page, enter your email address.
7. Tap **Next**.
8. On your organization's login page, enter your username.
9. Tap **Next**.
10. Enter your password.
11. Tap **Sign in**.
12. Click **OK**, to acknowledge that your IT department is helping to protect your work or school data using the BRIDGE app.
13. To activate the BlackBerry BRIDGE app, enter your password for the BlackBerry Dynamics app that is displayed in the activation request. For example, BlackBerry Work or BlackBerry UEM Client.
14. Click **OK**, to acknowledge that your organization protects the data in the app and to restart the app.
15. If BlackBerry Work opens, place it in the background.
16. If you are prompted, set a PIN or use your fingerprint to access your organization's data using the BlackBerry BRIDGE app.
17. Confirm the PIN.
18. Read the license agreement and if you agree, tap **Accept**.
19. If this is the first time that you have logged in to the BRIDGE app, the tutorials open. Complete one of the following tasks:
    - Tap **Skip** to close the tutorials without viewing them. Tap **OK**. You can view the tutorial later from the Settings screen.

- View the Tutorials. Tap **Next** to advance to the next page. Click **Done**. A reminder prompt is not displayed, but the tutorial is available in the Settings screen to view again.

Install BlackBerry BRIDGE from the App Store on iOS devices

You can send the following instructions to iOS device users that are installing the BlackBerry BRIDGE app on devices that don't have the BlackBerry UEM Client installed, or if you didn't allow the UEM Client to manage the activation of the BlackBerry BRIDGE app.

Before you begin:

- Make sure that a BlackBerry Dynamics app, for example,BlackBerry Work, is installed and activated on your device. For instructions, see the BlackBerry Work user guide for your device.
- Make sure that the supported Microsoft Intune managed apps are installed and activated on your device.

1. Download the BlackBerry BRIDGE app from the App Store.
2. Tap **BB Bridge**.
3. Tap **Login**.
4. On the **Microsoft Sign in** page, enter your email address field.
5. Tap **Next**.
6. If your organization has a login page, enter your username.
7. Tap **Next**.
8. Enter your password.
9. Tap **Sign in**.
10. Tap **OK** to acknowledge that your organization protects the data in the app and to restart the app.
11. Tap **BB Bridge**.
12. If prompted, set a PIN to access your organizations data using the BlackBerry BRIDGE app.
13. Read the license agreement and if you agree, tap **I agree**.
14. To activate the BlackBerry BRIDGE app, enter your password for the BlackBerry Dynamics app or use Touch ID.
15. Tap **OK**.
16. If this is the first time you have logged in to the BlackBerry BRIDGE app, the Tutorials screen opens and displays a list of tutorials. You can view the tutorials or tap **Close** to close the Tutorials screen
17. Click **OK**. You can view the tutorial later from the Settings screen.

Install BlackBerry BRIDGE from Google Play on Android devices

You can send the following instructions to device users that are installing the BlackBerry BRIDGE app on their devices.

Before you begin:

- Make sure that a BlackBerry Dynamics app, for example, BlackBerry Work, is installed and activated on your device.
- Make sure the Microsoft Intune Company Portal app is installed on your device. You do not need to activate the app. For more information, see https://docs.microsoft.com/intune/app-protection-enabled-apps-android.
- Make sure that the supported Microsoft Intune managed apps are installed and activated on your device.

1. Download the BlackBerry BRIDGE app from Google Play.
2. Tap **BB BRIDGE**.

3. If the Intune Company Portal app is not installed on your device, you are prompted with the following message: **To use your work or school account with this app, you must install Intune Company Portal app. Tap "Play Store" to continue**. Tap **Play Store** to install the Microsoft Intune Company Portal app.
4. Tap **Login**.
5. On the **Microsoft Sign in** page, enter your email address.
6. Tap **Next**.
7. If your organization has a login page, enter your username.
8. Tap **Next**.
9. Enter your password.
10. Tap **Sign in**.
11. Click **OK** to acknowledge that your IT department is helping to protect your work or school data using the BRIDGE app.
12. To activate the BlackBerry BRIDGE app, enter your password for the BlackBerry Dynamics app or use your fingerprint.
13. Click **OK** to acknowledge that your organization protects the data in the app and to restart the app.
14. If BlackBerry Work opens, place it in the background.
15. If you are prompted, set a PIN or use your fingerprint to access your organization's data using the BlackBerry BRIDGE app.
16. Confirm the PIN.
17. Read the license agreement and if you agree, tap **Accept**.
18. If this is the first time you have logged in to the BlackBerry BRIDGE app, the tutorials open. Complete one of the following tasks:
    - Tap **Skip** to close the tutorial without viewing them. Tap **OK**. You can view the tutorial later from the Settings screen.
    - View the Tutorials. Tap **Next** to advance to the next page. Tap **Done**. A reminder prompt is not displayed, but the tutorial is available in the Settings screen to view again.

Using BlackBerry BRIDGE with Microsoft Authenticator on Android devices

Users can provision BlackBerry BRIDGE using Microsoft Authenticator on their Android devices. When users add their work or school account to the Microsoft Authenticator app, they must enable the "Enable phone sign-in" option for the BlackBerry BRIDGE user account. For more information, see the Microsoft resource Sign in using Microsoft Authenticator. If users don't enable the phone sign-in option, they are redirected to the Microsoft Authenticator app to activate BlackBerry BRIDGE when they open the BlackBerry BRIDGE and again when they tap Login.

Wipe apps managed by Microsoft Intune

You can use the Wipe apps command to delete the data from apps that are managed by Intune on iOS and Android devices. The apps are not uninstalled when this command is sent.

1. On the menu bar, click **Users**.
2. Search for and click the user that you want to wipe the data from.
3. Click the **<*device model*> (Intune)** tab.
4. Click **Wipe apps**.

Troubleshooting BlackBerry BRIDGE

This section helps you troubleshoot BlackBerry BRIDGE issues.

Change the log level to Warn for Microsoft Intune customers

Complete this task in an on-premises BlackBerry UEM environment. If you use Microsoft Intune, you should change the log level to Warn.

1. On the BlackBerry UEM server that you want to change the log level for, locate the log4J.xml file. The default location of the file is `C:\Program Files\BlackBerry\BES\Core\tomcat-core\webapps\ROOT\WEB-INF\classes`
2. In the file, above the <root> value, add the following information: `<logger name="org.apache.http.wire"> <level value="warn"/> </logger>`
3. Restart the BlackBerry UEM Core service.

Upload log files to BlackBerry Support

If BlackBerry Support requests log files, you can instruct users to upload log files to help troubleshoot issues that the users are having with the BlackBerry BRIDGE app. Depending on the size of the logs, instruction users to allow a short period before they close the Settings screen or place the app in the background to allow the logs to be uploaded to BlackBerry.

1. Open the BlackBerry BRIDGE app.
2. Tap .
3. Tap **Send Logs to BlackBerry**.

Unable to save a copy of a file in the Intune-managed app

Possible cause

Microsoft Intune app protection profile is configured to prevent saving files in a local storage.

Possible solution

Verify users can save files to the local storage.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Protection > Microsoft Intune app protection profile**.
3. Click the profile that you want to change.
4. Click .
5. In the **Data relocation** section, select the **Prevent Save as** check box.
6. Select the **Local storage** check box.
7. Click **Save**.

Legal notice

© 2025 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, EMBLEM Design, ATHOC, 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