Configuring Office 365 Modern Authentication for BlackBerry Dynamics Apps

Contents

System requirements

To use Microsoft Office 365 modern authentication with your BlackBerry Dynamics apps, you require the following:

- Office 365 or Exchange Online
- Active Directory Federation Services running on an on-premises Windows server or a similar single sign-on or identity provider service
- If you are using Kerberos Constrained Delegation in your environment, Microsoft Azure Active Directory Connect must be used to synchronize on-premises directories with Azure AD by providing a common identity for accessing both cloud and on-premises resources
- User email addresses and UPNs must match as recommended by Microsoft
- BlackBerry UEM version 12.8 or later
- BlackBerry Enterprise Mobility Server version 2.10 or later
- The following are the minimum versions of the apps that you require:

  BlackBerry Notes for Android version 2.10 or later

  BlackBerry Notes for iOS version 2.10 or later

  BlackBerry Tasks for Android version 2.10 or later

  BlackBerry Tasks for iOSversion 2.10 or later

  BlackBerry Work for Android version 2.10 or later

  BlackBerry Work for iOS version 2.10 or later

  BlackBerry Work for macOS version 1.8 or later

  BlackBerry Work for Windows version 1.8 or later

  BlackBerry Connect for Android version 2.7.1 or later

  BlackBerry Connect for iOS version 2.7.1 or later

Steps to set up Office 365 modern authentication for BlackBerry Dynamics apps

Complete the following steps to set up your environment to use Office 365 modern authentication with BlackBerry Dynamics apps.

Step	Action
1	Set up your environment to support Office 365 modern authentication. Make sure that your environment meets the minimum system requirements.
2	In BEMS, enable modern authentication for the Mail service.
3	In BEMS, enable modern authentication for the Docs service: • Configuring Docs for Rights Management Services • If required in your environment, enable modern authentication for the the SharePoint storage service.
4	In BlackBerry UEM, configure the settings in the app configurations and create an Azure app ID for the BlackBerry Dynamics apps that you want to use with Office 365 modern authentication. Any of the following apps can be configured: • BlackBerry Work for iOS and Android • BlackBerry Work for macOS and Windows • BlackBerry Notes • BlackBerry Tasks
5	Optionally, configure additional options.

Enable modern authentication for the Mail service in BEMS

You must allow BEMS to authenticate with Microsoft Office 365 to access users' mailboxes and send notifications to users' devices when new email is received on the device.

Before you begin:

- Verify that you have the following information and completed the following task:
  - If you enable modern authentication using Credential, the Client Application ID. For instructions, see Obtain an Azure app ID for BEMS with credential authentication.
  - If you enable Modern Authentication using a Client Certificate:
    - The Client Application ID with certificate based authentication. For instructions, see Obtain an Azure app ID for BEMS with certificate-based.
    - Request and associate a certificate to the Azure app ID for BEMS

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Mail**.
2. Click **Microsoft Exchange**.
3. In the **Select Authentication type** section, select an authentication type based on your environment and complete the associated tasks to allow BEMS to communicate with Microsoft Office 365:

Authentication type	Description	Task
Credential	This option uses the BEMS username and password to authenticate to Microsoft Office 365.	**a.** In the **Username** field, enter the service account's User Principal Name (UPN) **b.** In the **Password** field, enter the password for the service account.
Client Certificate	This option uses a client certificate to allow the BEMS service account to authenticate to Microsoft Office 365.	**a.** For the **Upload PFX file**, click **Choose File** and select the client certificate file. For instructions on obtaining the .pfx file, see Associate a certificate with the Azure app ID for BEMS. **b.** In the **Enter PFX file Password** field, enter the password for the client certificate.

4. Select the **Enable Modern Authentication** checkbox.
5. In the **Authentication Authority** field, enter the Authentication Server URL that BEMS accesses and retrieve the OAuth token for authentication with Office 365 (for example, https://login.microsoftonline.com/<*tenantname*>). By default, the field is prepopulated with https://login.microsoftonline.com/common.
6. In the **Client Application ID** field, enter one of the following app IDs depending on the authentication type you selected:
   - Obtain an Azure app ID for BEMS with credential authentication
   - Obtain an Azure app ID for BEMS with certificate-based authentication
7. In the **Server Name** field, enter the FQDN of the server. By default, the field is prepopulated with https://outlook.office365.com.

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

8. Under the **Autodiscover and Exchange Options** section, complete one of the following actions. Most environments only require the default settings. Before modifying the settings, test the change in your environment.

Task	Steps
Override Autodiscover URL	If you select to override the autodiscover process, BEMS uses the override URL to obtain user information from Microsoft Office 365. **a.** Select the **Override Autodiscover URL** checkbox. **b.** In the **Autodiscover URL** field, type the autodiscover endpoint (for example, https://example.com/autodiscover/autodiscover.svc).
Autodiscover and Microsoft Exchange Server options	**a.** Select the **Swap ordering of <*domain.com*>/autodiscover and autodiscover. <*domain.com*>/autodiscover** check box to assist in resolving the autodiscover URL. Consider selecting this option if the order results in timeouts or other failures. **b.** Modify the **TCP Connect timeout for Autodiscover url(milliseconds)** field as required to prevent failures when autodiscovery takes too long. By default, the timeout is set to 120000. The recommended timeout is between 5000 milliseconds (5 seconds) and 120000 milliseconds (120 seconds). **c.** By default, the **Enable SCP record lookup** checkbox is selected. If you clear the checkbox, BEMS does not perform a Microsoft Active Directory lookup of Autodiscover URLs. This option is not available when Override Autodiscover URL is selected. **d.** Select the **Use SSL connection when doing SCP lookup** checkbox to allow BEMS to communicate with the Microsoft Active Directory using SSL. If you enable this feature, you must import the Microsoft Active Directory certificate to each computer that hosts an instance of BEMS. This option is not available when Override Autodiscover URL is selected. **e.** By default, the **Enforce SSL Certificate validation when communicating with Microsoft Exchange and LDAP server** check box is selected. **f.** By default, the **Allow HTTP redirection and DNS SRV record** checkbox is selected. If you clear the checkbox, you disable HTTP Redirection and DNS SRV record lookups for retrieving the Autodiscover URL when discovering users for BlackBerry Work Push Notifications. **g.** Select the **Force re-autodiscover of user on all Microsoft Exchange errors** checkbox to force BEMS to perform the autodiscover again for the user when Microsoft Office 365 returns an error message.

9. In the **End User Email Address** field, type an email address to test connectivity to Microsoft Office 365 using the service account. You can delete the email address after you complete the test.
10. Click **Save**.

After you finish: If you selected **Client Certificate** authentication, you can view the certificate information. Click **Mail**. The following certificate information is displayed:

- Subject

- Issuer
- Validation period
- Serial number

Obtain an Azure app ID for BEMS with credential authentication

1. Sign in to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for the app.
6. Select a supported account type.
7. In the **Redirect URI** section, in the drop-down list, select **Web** and enter `https://localhost:8443`
8. Click **Register**. The new registered app appears.
9. In the **Manage** section, click **API permissions**.
10. Click **Add a permission**.
11. In the **Select an API** section, click **Microsoft APIs** tab.
12. Click **Exchange**.
13. If you are creating the Microsoft Office 365 application to use Microsoft Intune, set the following permissions:
    - Delegated permissions: Access mailboxes as the signed-in user via Exchange Web Services (**EWS > EWS.AccessAsUser.All**)
14. Select the **Add permissions**.
15. Click **Add a permission**.
16. Click **Microsoft Graph**. If the Microsoft Graph API permission is not listed, add Microsoft Graph.
17. Set the following permissions for Microsoft Graph.
    - Delegated permissions: Sign in and read user profile (**User > User.Read**).
18. Click one of the following:
    - If the Microsoft Graph API permission existed in the API permissions list, click **Update permissions**.
    - If you needed to add the Microsoft Graph API permission, click **Create**.
19. Click **Add a permissions**.
20. Click **Grant admin consent**. Click **Yes**.

    Important: This step requires tenant administrator privileges.
21. To allow autodiscovery to function as expected, set the authentication permissions.
    a) In the **Manage** section, click **Authentication**.
    b) Under the **Implicit grant** section, select the **ID Tokens** checkbox.
    c) In the **Default client type**, select **Yes**.
    d) Click **Save**.
22. Click **Overview**. Copy the **Application (client) ID**. The Application (client) ID is displayed in the main **Overview** page for the specified app. This is used as the **Client application ID** when you enable modern authentication and configure BEMS to communicate with Microsoft Office 365.

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

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

   This app is a daemon, not a web app, and does not have a sign-on URL.
8. Click **Register**. The new registered app appears.
9. In the **Manage** section, click **Expose an API**. The scope restricts access to data and functionality protected by the API.
   a) Click **Add a scope**.
   b) Click **Save and continue**.
   c) Complete the following fields and options:
      - Scope name: Provide a unique name for the scope.
      - Who can consent: Click **Admins and user**.
      - Admin consent display name: Enter a descriptive name.
      - Admin consent description: Enter a description for the scope.
      - State: Click **Enable**.
10. Copy the **Application ID URI**. This is used to associate a certificate with the Azure app ID for BEMS. The Application ID URI appears in the format of api://{*appID*}.
11. In the **Manage** section, click **API permissions**.
12. Click **Add a permission**.
13. In the **Select an API** section, click **Microsoft APIs** tab.
14. Click **Exchange**.
15. If you are creating the Microsoft Office 365 application to use Microsoft Intune, set the following permissions:
    - Application permissions: Use Exchange Web Service with full access to all mailboxes (**full_access_as_app**)
16. Click **Add permissions**.
17. Click **Microsoft Graph**. If the Microsoft Graph API permission is not listed, add it.
18. Set the following permission for Microsoft Graph.
    - Delegated permissions: Sign in and read user profile (**User > User.Read**)
19. Click **Add permissions**.
20. Click **Grant admin consent**.
21. Click **Yes**.
22. To allow autodiscovery to function as expected, set the authentication permissions.
    a) In the **Manage** section, click **Authentication**.
    b) Under the **Implicit grant** section, select the **ID Tokens** checkbox.
    c) In the **Default client type**, select **No**.
    d) Click **Save**.

23. Click **Overview** to view the app that you created in step 5. Copy the **Application (client) ID**. The Application (client) ID is displayed in the main **Overview** page for the specified app. This is used as the **Client application ID** in the BEMS dashboard when you enable modern authentication and configure BEMS to communicate with Microsoft Office 365.

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

Associate a certificate with the Azure app ID for BEMS

You can request and export a new client certificate from your CA server or use a self-signed certificate.

1. Complete one of the following tasks:

Certificate	Task
If you are using an existing CA server	**a.** Request the certificate. The certificate that you request must include the app name in the subject of the certificate. Where <*app name*> is the name you assigned the app in step 5 of Obtain an Azure app ID for BEMS with certificate-based authentication. **b.** Export the public key of the certificate as a .cer or .pem file. The public key is used for the Azure app ID that is created. **c.** Export the private key of the certificate as a .pfx file. The private key is imported to the BEMS dashboard.

If you are using a self-signed certificate	**a.** Create a self-signed certificate using the New-SelfSignedCertificate command. For more information, visit docs.microsoft.com and read New-SelfSignedCertificate. **1.** On the computer running Microsoft Windows, open the Windows PowerShell. **2.** Enter the following command: `$cert=New-SelfSignedCertificate -Subject "CN=<app name>" -CertStoreLocation "Cert:\CurrentUser\My" -KeyExportPolicy Exportable -KeySpec Signature`. Where <*app name*> is the name you assigned the app in step 5 of . The certificate that you request must include the Azure app name in the subject field. **3.** Press **Enter**. **b.** Export the public key from the Microsoft Management Console (MMC). Make sure to save the public certificate as a .cer or .pem file. The public key is used for the Azure app ID that is created. **1.** On the computer running Windows, open the Certificate Manager for the logged in user. **2.** Expand **Personal**. **3.** Click **Certificates**. **4.** Right-click the <*user*>@<*domain*> and click **All Tasks > Export**. **5.** In the **Certificate Export Wizard**, click **No, do not export private key**. **6.** Click **Next**. **7.** Select **Base-64 encoded X.509 (.cer)**. Click **Next**. **8.** Provide a name for the certificate and save it to your desktop. **9.** Click **Next**. **10.** Click **Finish**. **11.** Click **OK**. **c.** Export the private key from the Microsoft Management Console (MMC). Make sure to include the private key and save it as a .pfx file. For instructions, visit docs.microsoft.com and read Export a Certificate with the Private Key. The private key is imported to the BEMS dashboard. **1.** On the computer running Windows, open the Certificate Manager for the logged in user. **2.** Expand **Personal**. **3.** Click **Certificates**. **4.** Right-click the <*user*>@<*domain*> and click **All Tasks > Export**. **5.** In the **Certificate Export Wizard**, click **Yes, export private key.**. **6.** Click **Next**. **7.** Select **Personal Information Exchange – PKCS #12 (.pfx)**. Click **Next**. **8.** Select the security method. **9.** Provide a name for the certificate and save it to your desktop. **10.** Click **Next**. **11.** Click **Finish**. **12.** Click **OK**.

2. Upload the public certificate that you exported in step 1 to associate the certificate credentials with the Azure app ID for BEMS.

a) In portal.azure.com, open the <*app name*> you assigned the app in step 5 of Obtain an Azure app ID for BEMS with certificate-based authentication.
b) Click **Certificates & secrets**.
c) In the **Certificates** section, click **Upload certificate**.
d) In the **Select a file** search field, navigate to the location where you exported the certificate in step 2.
e) Click **Add**.

Enable modern authentication for the Docs service in BEMS

Depending on your environment, configure the following:

- Configuring Docs for Rights Management Services
- If required in your environment, enable modern authentication for the the SharePoint storage service.

Configuring Docs for Rights Management Services

Active Directory Rights Management Services (AD RMS) and Azure-IP RMS from Microsoft allows documents to be protected against access by unauthorized people by storing permissions to the documents in the document file itself. Access restrictions can be enforced wherever the document resides or is copied or forwarded to. For documents to be protected with AD RMS or Azure-IP RMS, the app that the document is associated with must be RMS aware. For more information about AD RMS and Azure-IP RMS, visit Comparing Azure Information Protection and AD RMS.

Note: For this release, BEMS doesn't support both the AD RMS and Azure-IP RMS in the same environment.

Support for RMS protected documents is provided through two methods:

- In Docs and BlackBerry Work, support for RMS protected documents is provided through the Microsoft Office Web Apps server with viewing and editing enabled through the BlackBerry Access browser. Note that while BlackBerry Access browser is a BlackBerry Dynamics app with all the secure features it provides, it has only partial support for RMS features.
- In BlackBerry Work, support for RMS protected documents is provided directly in BlackBerry Work and through BlackBerry Work.

The following table compares the features of RMS protected documents in BlackBerry Work and through BlackBerry Access. These features require a client that is RMS aware.

	RMS protected documents directly in BlackBerry Work	RMS protected documents through BlackBerry Access
Features	• View protected documents directly in BlackBerry Work. This feature requires BEMS 2.10 or later. • Protect unprotected documents in BlackBerry Work. This feature requires BEMS 2.12 or later. • Change permissions for documents in BlackBerry Work. This feature requires BEMS 2.12 or later. • Upload a new file and save it as protected. This feature requires BEMS 2.12 or later and BlackBerry Work app 2.18 or later.	• View and edit protected documents in Docs and BlackBerry Work through the BlackBerry Access browser.

	RMS protected documents directly in BlackBerry Work	RMS protected documents through BlackBerry Access
Security	• Users can save what is on screen as a web clip and this screenshot file can be shared with other BlackBerry Dynamics apps. Mitigation is to disable web clips in the BlackBerry Access policy.	• Share the Microsoft Office Web Apps URL that is used to render the document viewing or editing with other BlackBerry Dynamics apps. The URL expires in thirty minutes but during this time, other BlackBerry Dynamics apps might be able to access it without any authentication. For example, if it is shared with BlackBerry Work, the URL can be emailed to others. If it is shared with a BlackBerry Dynamics app that allows printing, then the page that is rendered might be printed. Mitigation would be to enable user agent in the BlackBerry Access policy and then use it to create filtering rules in the Microsoft Office Web Apps server so that only BlackBerry Access is able to access the URL. The Microsoft IIS URL Rewrite extension can be used to create the rules. • Users can save what is on screen as a web clip and this screenshot file can be shared with other BlackBerry Dynamics apps. Mitigation is to disable web clips in BlackBerry Access policy. • When editing a document, by default, copy and paste of content would be possible by default polices only within the BlackBerry Dynamics secure container environment. Ensure that the protection provided is adequate given these limitations and satisfies your RMS protection requirements before enabling this support.

Steps to deploy Azure IP Rights Management Services support for the Docs service

When you configure Azure IP RMS support for the Docs service, you complete the following steps:

Step	Action
1	On the computer that hosts BEMS, install the Rights Management Services Client 2.1. To download the client, visit www.microsoft.com/downloads and search for ID=38396.
2	Obtain an Azure app ID for the

Step	Action
3	If necessary, migrate any labels that you need in the environment. **Note:** BEMS-Docs service only supports migrated unified labels. For instructions to migrate labels, visit https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-migrate-labels.
4	Convert protections templates to labels. For more information about converting templates to labels, visit https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-templates and read "*To convert templates to labels*".
5	Configure the Docs security settings

Obtain the Azure IP authentication information for the Docs service

The Docs service authenticates to Azure-IP using a fixed symmetric key and is associated with a super user service principal and a BPOS tenant ID that are generated using Windows PowerShell. The values are used to configure the BEMS dashboard. Authenticating to Azure-IP allows the Docs service to decrypt protected documents and determine the rights a user has on a document.

Before you begin: On the computer that you use to complete this task, make sure that the following software is installed:

- Windows PowerShell 3.0 or later.
- Windows PowerShellGet (previously known as OneGet). For more information about downloading PowerShellGet, visit https://www.microsoft.com/en-us/download/details.aspx?id=51451.
- Microsoft NuGet. For more information about NuGet, visit https://docs.microsoft.com/en-us/nuget/.
  To install NuGet, in Windows PowerShell type `Install-PackageProvider -Name NuGet -MinimumVersion <version number> -Force`. Where <version number> is a minimum of 2.8.5.201.
- AADRM (Azure AD Rights Management). For more information about AADRM, visit https://docs.microsoft.com/en-us/azure/information-protection/install-powershell
  To install AADRM, in Windows PowerShell, type `Install-Module -Name AADRM`.
- Azure Active Directory (MSOnline). For more information about MSOnline, visit https://docs.microsoft.com/en-us/powershell/module/msonline/?view=azureadps-1.0.
  To install MSOnline, in Windows PowerShell, type `Install-Module MSOnline`.

For more information about the following commands, visit https://docs.microsoft.com/en-us/azure/information-protection/rms-client/client-admin-guide-powershell.

1. Open the Windows PowerShell (run as administrator) and complete the following instructions.
2. Connect to the Azure AD with an account that has tenant administrator permissions. Type `Connect-MsolService`. Press **Enter**.
3. Create a new service principal. Type `New-MsolServicePrincipal`. Add a display name for the service principal (for example, BEMSDocsAzureIPServicePrincipal). Press **Enter**.
4. Connect to AzureIP with an account that has tenant administrator permissions. Type `Connect-AadrmService`. Press **Enter**.
5. Disconnect from AzureIP. Type `Disconnect-AadrmService`. Press **Enter**.

Obtain an Azure app ID for the

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

1. Sign in to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for the app. For example, AzureAppIDforBEMS.
6. Select a supported account type.
7. In the **Redirect URI** drop-down list, select **Web** and enter `https://localhost:8443`.
8. Click **Register**.
9. Record the **Application (client) ID**.
10. In the **Manage** section, click **API permissions**.
11. Click **Add a permission**.
12. In the **Select an API** section, click **APIs my organization uses**.
13. If your environment is configured for Azure-IP, search for and click **Microsoft Information Protection Sync Service**. Set the following permission:
    - In delegated permissions, select the **Read all unified policies a user has access to** checkbox (**UnifiedPolicy > UnifiedPolicy.User.Read**).
14. Click **Add permissions**.
15. Click **Add a permission**.
16. Complete one or more of the following tasks:

Service	Permissions
If you configure Docs to use Microsoft SharePoint Online or Microsoft OneDrive for Business	**a.** Click **SharePoint**. **b.** Set the following permissions: • In application permissions, clear all of the permissions. 1. Click **Application permissions**. 2. Click **expand all**. Make sure that all options are cleared. • In delegated permissions, select the **Read and write items and lists in all site collections** checkbox (**AllSite > AllSites.Manage**) **c.** Click **Add permissions**.
If you use Microsoft Azure-IP	**a.** Click **Microsoft Graph**. If Microsoft Graph is not listed, add Microsoft Graph. **b.** Set the following permissions: • In application permissions, select the **Read directory data** checkbox (**Directory > Directory.Read.All**). • In delegated permissions, select the **Read directory data** checkbox (**Directory > Directory.Read.All**). **c.** Click **Update permissions**.

17. Click **Grant admin consent**. Click **Yes**.

    Important: This step requires tenant administrator privileges.

18. To allow autodiscovery to function as expected, set the authentication permissions. Complete the following steps:
    a) In the **Manage** section, click **Authentication**.
    b) Under the **Implicit grant** section, select the **ID Tokens** checkbox.
    c) In the **Default client type**, select **No**.
    d) Click **Save**.
19. Define the scope and trust for this API. In the **Manage** section, click **Expose an API**. Complete the following tasks.

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

20. In the **Manage** section, click **Certificates & secrets** and add a client secret. Complete the following steps:
    a) Click **New client secret**.
    b) In the **Description** field, enter a key description up to a maximum of 16 characters including spaces.
    c) Set an expiration date (for example, In 1 year, In 2 years, Never expires).
    d) Click **Add**.
    e) Copy the key **Value**.

    Important: The Value is available only when you create it. You cannot access it after you leave the page.

Configure the Docs security settings

Docs security settings control acceptable Microsoft SharePoint Online domains, the URL of the approved Microsoft Office Web Apps (OWAS), the appropriate LDAP domains to use, whether you want to use Kerberos constrained delegation for user authentication, and Azure-IP authentication. Delegation allows a service to impersonate a user account to access resources throughout the network. Constrained delegation limits this trust to a select group of services explicitly specified by a domain administrator.

Before you begin: Verify that one or more of the following are configured in your environment:

- Kerberos constrained delegation for the BlackBerry Docs service is configured in your environment. For instructions, see Configuring Kerberos constrained delegation for the Docs service.

- Resource-based Kerberos constrained delegation for the BlackBerry Docs service is configured in your environment. For instructions, see Configuring resource based Kerberos constrained delegation for the Docs service.
- Your environment is configured to use Azure-IP, have the following information. For instructions, see Obtain an Azure app ID for the .
  - Azure Tenant Name
  - BEMS Service Azure Application ID
  - BEMS Service Azure Application Key
- Optionally, you can configure BEMS to allow users to authenticate to Microsoft SharePoint Online with an email address that is different from the email address that was used to install and activate BlackBerry Work. For instructions, see Enable the use of an alternate email address to authenticate to BEMS-Docs.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Settings**.
3. Select the **Enable Kerberos Constrained Delegation** checkbox to allow Docs to use Kerberos constrained delegation.
4. Separated by a comma, enter each of the Microsoft SharePoint Online domains you plan to make available. For more information, see Configuring support for Microsoft SharePoint Online and Microsoft OneDrive for Business.
5. Enter the URL for your approved **Office Web App Server**.
6. Provide your Microsoft Active Directory user domains (separated by commas), then enter the corresponding **LDAP Port**. LDAP (Lightweight Directory Access Protocol) is used to look up users and their membership in user groups.
7. Select the **Use SSL for LDAP** checkbox for secure communication with your Microsoft Active Directory servers.
8. Add the **Workspaces Public Key**. Adding the public key allows BEMS and the BlackBerry Workspaces server to communicate with each other. For more information about locating the public key, contact BlackBerry Technical Support Services.
9. Select the **Enable Azure Information Protections** check box to allow Docs to authenticate to Azure-IP. Complete the **Azure registration** fields to authenticate Docs to Azure-IP to allow the Docs to decrypt protected documents and confirm the rights any given user has on a document.
10. Click **Save**.
11. Restart the Good Technology Common Services for the changes to take effect.

Enable modern authentication for the SharePoint storage service

You can also enable modern authentication for the SharePoint storage service when you have Microsoft SharePoint configured in your environment.

Before you begin: If you enable modern authentication, configured the Azure registration in the **Docs > Settings** screen. For more information, see Configure the Docs security settings.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Storages**.
3. Click the storage name **SharePoint Online**.
4. If this is a new installation, the following settings are selected by default:
   - **Authentication Provider** drop-down list: **Modern**
   - **Use Azure registration from Settings** check box is selected. SharePoint uses the Azure registration settings that are specified in the **Docs > Settings** screen. For more information, see Configure the Docs security settings.

5. If you upgraded from BEMS 2.10 or earlier and modern authentication was configured, no additional actions are required. Optionally, select the **Use Azure registration from Settings** check box for SharePoint to use the Azure registration settings that are specified in the **Docs > Settings** screen. For more information, see Configure the Docs security settings.
6. To make the storage available on user devices, select the select the **Enable Storage** checkbox.

   Note: It may take up to an hour or a restart of the apps for storage changes to take effect on users' devices. It may take up to five minutes for the changes to take effect on the server. Enabling and disabling storage providers on this page affects what storage resources are visible at any given time for users, but it has no such impact on the server. If this option is not selected, users can't access the fileshare and receive the following error message on the device: **Data sources could not be retrieved. Unable to connect to the server**.

After you finish: Add repositories in the storage added. For instructions, see Managing Repositories

Configure BlackBerry Work for iOS and Android app settings for Office 365 modern authentication

You must add your Exchange ActiveSync server information and, optionally, configure other settings.

1. On the menu bar, click **Apps**.
2. Click the BlackBerry Work app.
3. On the **BlackBerry Dynamics** tab, in the App configuration table, click +.
4. Type a name for the app configuration.
5. On the **Advanced** settings tab, under **Office 365** configure the following settings:
   a) Select the **Use Office 365 Modern Authentication** option to use modern authentication instead of basic authentication. Modern authentication enables BlackBerry Work to use sign-in features such as multi-factor authentication, SAML-based third-party identity providers, and smart card and certificate-based authentication.
   b) In the **Azure App ID** field, specify the Microsoft Azure app ID for BlackBerry Work. For information on how to obtain an Azure ID, see Obtain an Azure app ID for BlackBerry Work
   c) In the **Office 365 Sign On URL** field, specify the web address that BlackBerry Work should use when signing in to Office 365. If you do not specify a value, BlackBerry Work will use https://login.microsoftonline.com during setup. In most configurations, this field should be left blank.
   d) In the **Office 365 Tenant ID** field, specify the tenant ID of the Office 365 server that you want BlackBerry Work to connect to during setup. If you do not specify a value, a value of "common" is used. In most configurations, this field should be left blank.
   e) In the **Office 365 Resource** field, specify the URL of the Microsoft Exchange Online server. In the **Redirect URI** field, specify the URI that you entered in the Microsoft Azure portal. In most configurations, this field should be left blank.
   f) Optionally, select the **Proxy Office 365 Modern Authentication requests (Android only)** setting to force all Office 365 modern authentication requests to go through the BlackBerry Proxy instead of connecting directly to the Internet. This setting should be enabled if your Active Directory Federation Services (ADFS) server is not published externally to the internet. If your ADFS server is published externally, this setting is optional.
6. Optionally, configure any other settings. See app configuration settings for a description of all of the settings that you can configure.
7. Click **Save**.

Obtain an Azure app ID for BlackBerry Work

If you are configuring Office 365 settings in the app configuration for BlackBerry Work, you may need to obtain and copy the Azure app ID for BlackBerry Work.

1. Log on to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for the app. This is the name that users will see.
6. Select a supported account type.
7. In the **Redirect URI** drop-down list, select **Public client (mobile & desktop)** and enter `com.blackberry.work://connect/o365/redirect`

8. Click **Register**.
9. In the **Manage** section, click **API permissions**.
10. Click **Add a permission**.
11. In the **Select an API** section, click the **Microsoft APIs** tab.
12. Select **Exchange**.
13. If your environment is using Microsoft Office 365, set the following permissions:
    - Delegated permissions: Access mailboxes as the signed-in user via Exchange Web Services (**EWS > EWS.AccessAsUser.All**)
14. Click **Add permissions**.
15. Click **Add a permission**.
16. Click **Microsoft Graph**. If Microsoft Graph is not listed, add Microsoft Graph.
17. Set the following permissions for Microsoft Graph:
    - Delegated permissions
      - Sign in and read user profile (**User > User.Read**)
      - Send mail as a user (**Mail > Mail.Send**)
18. Click one of the following:
    - If Microsoft Graph existed in the API permissions list, click **Update permissions**.
    - If you needed to add Microsoft Graph, click **Create**.
19. Click **Add a permission**.
20. If your environment uses Skype for Business Online, complete the following steps:
    a) Click **Skype for Business**.
    b) Set the following **Delegated Permissions**: Make sure that all of the options are selected.
    c) Click **Select**.
    d) Click **Done**.
21. Click **Add permissions**.
22. Click **Grant Permissions** to apply the permissions for the app. These settings will not be applied to the app until you have granted the updated permissions.
23. Click **Yes**.
24. Allow BlackBerry Work implicit grant to request the token directly from the authorization end point.
    a) In the **Manage** section, click **Authentication**.
    b) Under the **Implicit grant** section, select the **ID Tokens** checkbox.
    c) In the **Default client type**, select **Yes**.
    d) Click **Save**.
25. Click **Yes**. You can now copy the Application ID for the app that you created. In the **Manage** section, click **Overview**. It is located under the name of the app, in the Application (client) ID field.

Configure BlackBerry Work for Windows and macOS app settings for Office 365 modern authentication

1. On the menu bar, click **Apps**.
2. Click the BlackBerry Access app.
3. On the BlackBerry Dynamics tab, in the App configuration table, click +.
4. Type a name for the app configuration.
5. On the **BlackBerry Work (Mac and Win)** settings tab, configure the following settings:
   a) Select the **Use Office 365 Modern Authentication** option.
   b) In the **Office 365 Resource** field, specify the URL of the Microsoft Exchange Online server. In the Redirect URI field, specify the URI that you entered in the Microsoft Azure portal. In most configurations, this field should be left blank.
   c) In the **Office 365 Tenant ID** field, specify the tenant ID of Office 365 server that you want BlackBerry Work to connect to during setup. If you do not specify a value, a value of "common" is used. In most configurations, this field should be left blank.
   d) In the **Azure App ID** field, specify the Microsoft Azure app ID for BlackBerry Work. For information on how obtain an Azure ID, see Obtain an Azure app ID for BlackBerry Work for Windows and macOS. In most configurations, this field should be left blank.
6. Optionally, configure any other settings. See app configuration settings for a description of all of the settings that you can configure.
7. Click **Save**.

Obtain an Azure app ID for BlackBerry Work for Windows and macOS

If you are configuring Office 365 settings in the app configuration for BlackBerry Work, you may need to obtain and copy the Azure app ID for BlackBerry Work for Windows and macOS.

Note: If you have already created an Azure app ID for BlackBerry Work for iOS and BlackBerry Work for Android, make sure that you do not use the same Azure app ID for for BlackBerry Work for Windows and macOS. BlackBerry Work for Windows and macOS need their own Azure app ID.

1. Log on to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for the app. This is the name that users will see.
6. Select a supported account type.
7. In the **Redirect URI** drop-down list, select **Public client (mobile & desktop)**. and enter `chrome-extension://glilhfdenplejncjmngdaojopbobomfa/login.html`
8. Click **Register**.
9. In the **Manage** section, click **API permissions**.
10. Click **Add a permission**.
11. In the **Select an API** section, click the **Microsoft APIs** tab.
12. Select **Exchange**.
13. If your environment is using Office 365 Exchange Online, set the following permissions:

- Delegated permissions: Access mailboxes as the signed-in user via Exchange Web Services (**EAS > EWS.AccessAsUser.All**).

14. Click **Add permissions**.
15. Click **Microsoft Graph**. If Microsoft Graph is not listed, add Microsoft Graph.
16. Set the following permissions for Microsoft Graph:
    - Delegated permissions
      - Sign in and read user profile (**User > User.Read**)
      - Send mail as a user (**Mail > Mail.Send**)
17. Click one of the following:
    - If Microsoft Graph existed in the API permissions list, click **Update permissions**.
    - If you needed to add Microsoft Graph, click **Create**.
18. Click **Grant Permissions** to apply the permissions for the app. These settings will not be applied to the app until you have granted the updated permissions.
19. Click **Yes**.
    You can now copy the Application ID for the app that you created. In the **Manage** section, click **Overview**. It is located under the name of the app, in the Application ID field.

Configure BlackBerry Notes and BlackBerry Tasks app settings for Office 365 modern authentication

1. On the menu bar, click **Apps**.
2. Click the BlackBerry Notes or BlackBerry Tasks app.
3. On the **BlackBerry Dynamics** tab, in the **App configuration** table, click +.
4. Type a name for the app configuration.
5. In the **Microsoft Office 365 Modern Auth Settings** section, configure options for Microsoft Office 365. If selected, specify the following:
   a) Select the **Use Office 365 Modern Authentication** option to use modern authentication instead of basic authentication. Modern authentication enables BlackBerry Notes and BlackBerry Tasks to use sign-in features such as multi-factor authentication, SAML-based third-party identity providers, and smart card and certificate-based authentication.
   b) In the **Office 365 Sign On URL** field, specify the web address that BlackBerry Notes or BlackBerry Tasks should use when signing in to Office 365. If you do not specify a value, BlackBerry Notes or BlackBerry Tasks will use https://login.microsoftonline.com during setup. In most configurations, this field should be left blank.
   c) In the **Office 365 Tenant ID** field, specify the tenant ID of the Microsoft Office 365 server that you want BlackBerry Notes or BlackBerry Tasks to connect to during setup. If you do not specify a value, a value of "common" is used. In most configurations, this field should be left blank.
   d) In the **Azure App ID** field, specify the Microsoft Azure app ID for BlackBerry Notes or BlackBerry Tasks. It is the same Azure App ID as the one you used for BlackBerry Work. For information on how obtain an Azure app ID, see Obtain an Azure app ID for BlackBerry Tasks and BlackBerry Notes .
   e) In the **Office 365 Resource** field, specify the URL of the Microsoft Exchange Online server. In most configurations, this field should be left blank.
   f) In the **Redirect URI** field, specify the URI that you entered in the Microsoft Azure portal. In most configurations, this field should be left blank.
   g) Select the **Proxy Office 365 Modern Authentication requests (Android only)** setting to force all Office 365 modern authentication requests to go through the BlackBerry Proxy instead of connecting directly to the Internet. This setting should be enabled if your Active Directory Federation Services (ADFS) server is not published externally to the internet. If your ADFS server is published externally, this setting is optional.
6. Click **Save**.

Obtain an Azure app ID for BlackBerry Tasks and BlackBerry Notes

If you are configuring Office 365 settings in the app configuration for BlackBerry Tasks and BlackBerry Notes, you may need to obtain and copy the Azure app IDs for BlackBerry Tasks and BlackBerry Notes.

1. Log on to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for BlackBerry Tasks. This is the name that users will see.
6. Select a supported account type.
7. In the **Redirect URI** drop-down list, select **Public client (mobile & desktop)**and enter `com.blackberry.work://connect/o365/redirect`
8. Click **Register**.

9. In the **Manage** section, click **API permissions**.
10. Click **Add a permission**.
11. In the **Select an API** section, click the **Microsoft APIs** tab.
12. If your environment is using Office 365 Exchange Online, set the following permissions:
    - Delegated permissions: Access mailboxes as the signed-in user via Exchange Web Services (**EWS > EWS.AccessAsUser.All**)
13. Click **Add permissions**.
14. Click **Grant Permissions** to apply the permissions for the app. These settings will not be applied to the app until you have granted the updated permissions.
15. Click **Yes**.
    You can now copy the Application ID for the app that you created for BlackBerry Tasks. In the **Manage** section, click **Overview**. It is located under the name of the app, in the Application (client) ID field. Repeat the steps for BlackBerry Notes.

Additional configuration options

Active Directory Federation Services supports multiple types of authentication, including forms-based authentication and Windows Integrated Authentication.

To support Windows Integrated Authentication for BlackBerry Dynamics apps, you must configure Constrained Delegation and you may need to configure ADFS to allow BlackBerry Dynamics clients to use Windows Integrated Authentication.

For instructions on how to configure your environment, refer to the following:

- Configuring intranet forms-based authentication for devices that do not support WIA
- Configure single sign-on for BlackBerry Dynamics apps in BlackBerry UEM
- Configure Kerberos Constrained Delegation for BlackBerry Dynamics apps

Configure single sign-on for BlackBerry Dynamics apps in BlackBerry UEM

You can enable single sign-on for BlackBerry Dynamics apps in an environment that's already set up for Microsoft Office 365 with Microsoft Active Directory Federation Services and single sign-on.

Before you begin:

Before you begin, make sure that you have configured the following:

- Configure single sign-on in Office 365 with Active Directory Federation Services version 2.0 or 3.0, relying on Windows Authentication and Kerberos.
- Configure BlackBerry UEM for Kerberos constrained delegation.

1. Verify the SPN for Active Directory Federation Services. For Active Directory Federation Services to use Kerberos, the Active Directory Federation Services service must have registered an SPN. This SPN should already be registered by the prerequisite Active Directory Federation Services configuration in Office 365.
   a) Open a command prompt on a computer with Active Directory RSAT tools installed.
   b) Enter the command: `setspn -q HOST/`*fqdn.of.adfs.server*, where *fqdn.of.adfs.server* is the FQDN of your Active Directory Federation Services server.

   This command exposes the name service account that serves Active Directory Federation Services. For a safer form of delegation (HOST allows any protocol, only HTTP is needed) you might want to register the HTTP SPN of the Active Directory Federation Services service account with the following command: `setspn -S HTTP/fqdn.of.adfs.server`*ADFS_service_account*, where *ADFS_service_account* is the name of the Active Directory Federation Services service account shown in the previous command.
2. Enable the User Agent in Active Directory Federation Services. By default, Active Directory Federation Services allows only known user agents to use Windows Authentication. All other user agents are considered external and are served with Forms Based Authentication (FBA) or certificate authentication.
   a) To enable single sign-on in BlackBerry Dynamics apps, you need to add the BlackBerry Dynamics app user agent string to Active Directory Federation Services to allow Windows Authentication for the BlackBerry Dynamics app and Kerberos constrained delegation. For all platforms, theBlackBerry Dynamics app user agent string begins with `Mozilla/5.0.`.
   b) To verify the Active Directory Federation Services user agents, enter the following command: `Get-ADFSProperties | Select -ExpandProperty WIASupportedUserAgents`

c) Edit and run the following script to add the new user agent to Active Directory Federation Services. **$NewUserAgent** must be edited to the value that you will add.

```
$NewUserAgent = "Mozilla/5.0"
$CurrentUserAgents = Get-ADFSProperties | Select -ExpandProperty
 WIASupportedUserAgents
$UserAgentAddArray = $CurrentUserAgents + $NewUserAgent
Set-ADFSProperties -WIASupportedUserAgents $UserAgentAddArray
```

d) To verify that the Active Directory Federation Services user agent has been added, run the **Get-ADFSProperties** command again: `Get-ADFSProperties | Select -ExpandProperty WIASupportedUserAgents`

e) Restart the Active Directory Federation Services service.

3. Set delegation on the Kerberos account.

a) Log in to BlackBerry UEM.

b) Click **Settings** > **BlackBerry Dynamics** > **Properties**.

c) Scroll to find the value of the **gc.krb5.principal.name** property. Set this object name in Microsoft Active Directory.

d) On your Microsoft Active Directory server, click the **Delegation** tab.

e) Click **ADD** and enter the Active Directory Federation Services service account name that you discovered in step 1.

f) Add the HTTP SPN.

g) Click **OK**.

Troubleshooting

If you are experiencing issues, refer to the following topics for possible solutions.

How data flows when BlackBerry Work uses Office 365 modern authentication

Modern authentication simplifies authentication for developers by providing identity as a service (IaaS), with support for industry-standard protocols such as OAuth 2.0. Any app that wants to outsource authentication to Azure Active Directory must first be registered in Azure AD, which registers and uniquely identifies the app in the directory, with an app ID. Azure AD is responsible for verifying the identity of users and apps that exist in an organization's directory, and then issuing security tokens for these users and apps after successful authentication. When using the Azure Active Directory Authentication Libraries (ADAL), much of the flow is handled for the developer. When troubleshooting an issue, it is helpful to understand the flow of data so you can focus on the point where the data flow breaks.

1. Using a browser pop-up, the BlackBerry Work app makes a request to the authorization endpoint in Azure AD. This request includes the app ID, the redirect URI of the BlackBerry Work app (as shown in the Azure Portal), and the app ID URI for the web API. If the user hasn't already signed in, they are prompted to sign in again.
2. Azure AD authenticates the BlackBerry Work user and the user will be required to consent if they haven't already done so. After granting consent and upon successful authentication, Azure AD issues an authorization code response back to the redirect URI used by BlackBerry Work.
3. When Azure AD issues an authorization code response back to the redirect URI, the BlackBerry Work app stops browser interaction and extracts the authorization code from the response. Using this authorization code, the BlackBerry Work app sends a request to the Azure AD token endpoint that includes the authorization code, details about the BlackBerry Work app (app ID and redirect URI), and the desired resource (app ID URI for the web API).
4. The authorization code and information about the BlackBerry Work app and web API are validated by Azure AD. After successful validation, Azure AD returns two tokens: a JWT access token and a JWT refresh token. In addition, Azure AD returns basic information about the user, such as their display name and tenant ID.
5. Over HTTPS, the BlackBerry Work app uses the returned JWT access token to add the JWT string with a "Bearer" designation in the Authorization header of the request to the web API. The web API then validates the JWT token and, if validation is successful, returns the desired resource.
6. When the access token expires, the BlackBerry Work app will receive an error that indicates that the user needs to authenticate again. If the BlackBerry Work app has a valid refresh token, it can be used to acquire a new access token without prompting the user to sign in again. If the refresh token expires, the BlackBerry Work app will need to interactively authenticate the user once again.

Authentication fails when email address and UPN do not match

BlackBerry Work, BlackBerry Notes, BlackBerry Tasks, and BlackBerry Connect require that user email addresses and UPN values match. If these values do not match, modern authentication will fail because the token being returned from Azure does not match the email address of the BlackBerry Dynamics app. Microsoft recommends that email address and UPN match.

For more information, visit https://support.blackberry.com/community/s/article/50721 to read article 000050721.

Expected behavior when an Microsoft Active Directory password is changed

When a user changes their Active Directory password, it may take some time for the user's access token to expire before BlackBerry Work, BlackBerry Notes, BlackBerry Tasks, or BlackBerry Connect prompts the user to re-authenticate. The length of time before the token expires is configured in Microsoft Azure. BlackBerry has no control over access token expiry time. The default lifespan of an access token is one hour. If the previously used credentials are no longer valid when a user's access token expires, the user must authenticate again. If a user logs in with a password (for example, they are using Forms Based authentication), the authentication form is displayed and the user must enter their credentials again. If a user logs in without a password (for example, they are using Kerberos Constrained Delegation or Certificate Based Authentication), the user is automatically re-authenticated and does not have to enter their credentials again.

For more information, visit https://support.blackberry.com/community/s/article/55799 to read article 000055799.

Steps to migrate existing on-premises users to Microsoft Outlook Online using modern authentication

Step	Action
1	Configure modern authentication and and validate that it is working correctly.
2	Migrate user mailboxes from your on-premises Microsoft Exchange server to Microsoft Exchange Online. After the migration completes, users will receive a prompt to log in to their mailboxes. Wait while the BlackBerry Dynamics apps trigger autodiscover and connect to the new mailbox location. The amount of time this takes depends on how many users have been migrated and how often BlackBerry Work is opened. Refer to the Last Contact Time and container activity report to estimate whether users have received the new mailbox configuration from autodiscover. Do not proceed to the next step until all users have authenticated.
3	Assign the app configuration with the correct modern authentication settings to users. For BlackBerry Work for iOS and Android, see Configure BlackBerry Work for iOS and Android app settings for Office 365 modern authentication. For BlackBerry Work for Windows and macOS, see Configure BlackBerry Work for Windows and macOS app settings for Office 365 modern authentication. For BlackBerry Notes and Tasks, see Configure BlackBerry Notes and BlackBerry Tasks app settings for Office 365 modern authentication.

Configure and validate modern authentication

Complete the following tasks to configure modern authentication and validate that is working correctly.

Item	Description
☐	Because basic authentication must work during the migration process, make sure that basic authentication is working for users with mailboxes on Outlook Online. It can be disabled later.
☐	Make sure that your environment meets all of the prerequisites to enable modern authentication.
☐	Perform the following tasks using test accounts: • Validate modern authentication functionality using Microsoft Exchange Online test accounts. It is recommended that you create test accounts on your on-premises Microsoft Exchange server and mimic the migration with these accounts to Microsoft Exchange Online. • Make sure that each required BlackBerry Dynamics app can authenticate using Microsoft Exchange Online test accounts. • Make sure that BEMS Push Notifications are functioning for Microsoft Exchange Online test accounts.
☐	Validate that autodiscover is configured properly for Hybrid Exchange environments according to Microsoft's recommendations. For more information, see Office 365 Exchange Hybrid Deployments Busting the Autodiscover Myth.

Legal notice

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

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

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

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

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

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

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

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

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada