Configuring Office 365 Modern Authentication for BlackBerry Dynamics Apps

Contents

System requirements..... 5

Steps to set up Office 365 modern authentication for BlackBerry Dynamics apps..... 6

Enable modern authentication for the Mail service in BEMS 7

Obtain an Azure app ID for BEMS with credential authentication..... 9
Obtain an Azure app ID for BEMS with certificate-based authentication..... 10
Associate a certificate with the Azure app ID for BEMS..... 11

Enable modern authentication for the Docs service in BEMS..... 14

Configuring Docs for Rights Management Services..... 14
Steps to deploy Azure IP Rights Management Services support for the Docs service..... 15
Enable modern authentication for the SharePoint storage service..... 20

Configure BlackBerry Work for iOS and Android app settings for Office 365 modern authentication..... 21

Obtain an Azure app ID for BlackBerry Work..... 21

Configure BlackBerry Work for Windows and macOS app settings for Office 365 modern authentication..... 23

Obtain an Azure app ID for BlackBerry Work for Windows and macOS..... 23

Configure BlackBerry Notes and BlackBerry Tasks app settings for Office 365 modern authentication..... 25

Obtain an Azure app ID for BlackBerry Tasks and BlackBerry Notes 25

Additional configuration options..... 27

Configure single sign-on for BlackBerry Dynamics apps in BlackBerry UEM..... 27

Troubleshooting..... 29

How data flows when BlackBerry Work uses Office 365 modern authentication..... 29
Enable ADFS debug logging..... 29
When ADFS is not accessible outside of the work network, attempts to use Office 365 modern authentication may fail in BlackBerry Work, Notes, and Tasks..... 30

Legal notice..... 32

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
- 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. Log on to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New application registration**.
5. In the **Name** field, enter a name for the app.
6. In the **Application type** drop-down list, select **Native**.
7. In the **Redirect URI** field, enter `https://localhost:8443`
8. Press **Enter**.
9. Click **Create**.
10. Select the app name that you created.
11. Click **Settings**.
12. Click **Required permissions**.
13. Click **Add**.
14. Click **Select an API**.
15. Select **Office 365 Exchange Online**.
16. Click **Select**.
17. Select the **Access mailboxes as the signed-in user via Exchange Web Service** checkbox for Microsoft Office 365.
18. Click **Select**.
19. Click **Done**.
20. Click **Grant Permissions**.
21. Click **Yes**.
22. Click **Add**.
23. Click **Select an API**.
24. Click **Microsoft Graph**.
25. Click **Select**.
26. In the **Delegated Permissions** section, select the **Sign in and read user profile** checkbox.
27. Click **Select**.
28. Click **Done**.
29. Click **Grant Permissions**.
30. Click **Yes**.
31. Copy the **Application ID**. The Application ID is displayed in the main **App Registrations** page for the specified app. This is used as the **Client application ID** when you configure BEMS to communicate with Microsoft Office 365.

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

1. Log in to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New application registration**.
5. In the **Name** field, enter a name for the app.
6. In the **Application type** drop-down list, select **Web app / API**.
7. In the **Sign-on URI** field, 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. Press **Enter**.
9. Click **Create**.
10. If not already selected, select the app name that you created.
11. Click **Settings**.
12. In the **Settings** column, click **Properties**.
13. In the **Properties** column, copy the **Appl ID URI**. This will be used to associate a certificate with the Azure app ID for BEMS.
14. Click **Required permissions**.
15. Click **Add**.
16. Click **Select an API**.
17. Select **Office 365 Exchange Online**.
18. Click **Select**.
19. Select the **Use Exchange Web Service with full access to all mailboxes** checkbox.
20. Click **Select**.
21. Click **Done**.
22. Click **Grant Permissions**.
23. Click **Yes**.
24. Click **Add**.
25. Click **Select an API**.
26. Click **Microsoft Graph**.
27. Click **Select**.
28. In the **Delegated Permissions** section, select the **Sign in and read user profile** checkbox.
29. Click **Select**.
30. Click **Done**.
31. Click **Grant Permissions**.
32. Click **Yes**.
33. Copy the **Application ID**. The Application ID is displayed in the main **App Registrations** page for the specified app. This is used as the **Client application ID**.
34. Do not close portal.azure.com.

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 **Settings > Keys**.
c) Click **Upload Public Key**.
d) Click and navigate to the location where you exported the certificate in step 2.
e) Click **Open**.
f) Click **Save**.

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.	• 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 the Azure IP authentication information for the Docs service
3	Obtain an Azure app ID for the Connect, Presence, and Docs service
4	Configure the Docs security settings

Obtain the Azure IP authentication information for the Docs service

The Docs service authenticates to AzureIP 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. Record the the following information:

- Symmetric key
- AppPrincipalID

5. Connect to AzureIP with an account that has tenant administrator permissions. Type `Connect-AadrmService`. Press **Enter**.
6. Obtain the BPOS Tenant ID. Type `(Get-AadrmConfiguration).BPOSId`. Press **Enter**. Record the BPOS Tenant ID.
7. If the super user feature is not enabled, enable it now. Type `Enable-AadrmSuperUserFeature`. Press **Enter**.
8. Make the service principal a super user for Azure IP. Type `Add-AadrmSuperUser -ServicePrincipalId <AppPrincipalId>`where <*AppPrincipalId*> is the AppPrincipalID from step 3. Press **Enter**.
9. Disconnect from AzureIP. Type `Disconnect-AadrmService`. Press **Enter**.

Obtain an Azure app ID for the Connect, Presence, and Docs service

When your environment is configured for Skype for Business Online, Microsoft SharePoint Online or Microsoft Azure-IP you must register the BEMS component services in Azure. You can register one or more of the services in Azure. In this task, the Connect, Presence, and Docs services and Microsoft Azure-IP are registered in Azure.

If you configure the Connect service, you can enable the conversation history to allow users to access conversations that are saved in the Conversation History folder of the user's Microsoft Exchange mailbox. Saving the conversation history is supported in the following environments:

- Users in a Skype for Business on-premises that have mailboxes on an on-premises Microsoft Exchange Server.
- Users in a Skype for Business Online environment that have mailboxes on an on-premises Microsoft Exchange Server.
- Users in a Skype for Business Online environment that have mailboxes on Microsoft Office 365.

Saving the conversation history is not supported in an on-premises Skype for Business environment where users have mailboxes on Microsoft Office 365.

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

1. Log on to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New application registration**.
5. In the **Name** field, enter a name for the app. For example, AzureAppIDforBEMS.
6. In the **Application type** drop-down list, select **Web app / API**.
7. In the **Sign-On URL** field, enter `https://localhost:8443`.
8. Press **Enter**.
9. Click **Create**.
10. Click **Settings**.
11. Click **Required permissions**.
12. Click **Add**.
13. Click **Select an API**.
14. Complete one or more of the following tasks:

Service	Permissions
If you configure Connect to use Skype for Business Online,	**a.** Search for and click **Skype for Business Online**. **b.** Click **Select**. **c.** Set the following permissions: • **Application Permissions**: Make sure that all options are selected. • **Delegated Permissions**: Make sure that all options are selected. **d.** Click **Select**. **e.** Click **Done**. **f.** If you enable saving the conversation history, complete the following steps: **1.** In the **Required permissions** column, click **Add**. **2.** Click **Select an API**. **3.** Select **Office 365 Exchange Online**. **4.** Click **Select**. **5.** Set the following permissions: • **Delegated Permissions Access mailboxes as the signed-in user via Exchange Web Services** **6.** Click **Select**. **7.** Click **Done**.
If you configure Presence to use Skype for Business Online	**a.** Search for and click **Skype for Business Online**. **b.** Click **Select**. **c.** Set the following permissions: • **Application Permissions**: Make sure that all options are selected. • **Delegated Permissions**: Make sure that all options are selected. **d.** Click **Select**. **e.** Click **Done**.
If you configure Docs to use Microsoft SharePoint Online,	**a.** Search for and click **Office 365 SharePoint Online**. **b.** Click **Select**. **c.** Set the following permissions: • **Application Permissions**: None. Clear the check boxes for all options. • **Delegated Permissions**: Select the **Read and write items and lists in all site collections** checkbox. **d.** Click **Select**. **e.** Click **Done**.
If you use Microsoft Azure-IP	**a.** Search for and click **Microsoft Graph**. **b.** Click **Select**. **c.** Set the following permissions: • **Application Permissions**: Read directory data • **Delegated Permissions**: Read directory data **d.** Click **Select**. **e.** Click **Done**.

15. Click **Grant Permissions**. Click **Yes**.

Important: This step requires tenant administrator privileges.

16. In the **Settings** column, click **Keys**.
17. In the **Key description** field, enter a key description up to a maximum of 16 characters including spaces.
18. I n the **Duration** field, select an expiration. Available expirations are: In 1 year, In 2 years, Never expires.
19. Click **Save**.
20. Copy the key **Value**.

    Important: The Value is available only when you create it. You cannot access it after you leave the page. This is used as the **BlackBerry BEMS Connect/Presence Service App Key** value in the Connect and Presence services and **Application Key** in the Docs service in the BEMS Dashboard.
21. Copy the **Application ID**. The Application ID is displayed in the main **App Registrations** page for the specified app. This is used as the **BlackBerry BEMS Connect/Presence Service App ID** in the Connect and Presence services, the **Application Key** and in the Docs > Storages service, and the **BEMS Service Azure Application ID** in the Docs > Settings in the BEMS Dashboard.

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 the Azure IP authentication information for the Docs service.
  - BPOS TenantID
  - Symmetric Key
  - AppPrincipalID
  - Azure Tenant Name
  - BEMS Service Azure Application ID
  - BEMS Service Azure Application Key

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 (Lighweight 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 required 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.

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. Click the Authentication Provider drop-down list and click **Modern**.
5. Complete the following fields. For more information on obtaining the Application ID and Application Key, see Obtain an Azure app ID for the Connect, Presence, and Docs service. For information on obtaining the Client ID, see Obtain an Azure app ID for BlackBerry Work.
   - Tenant name/ID
   - Application ID
   - Application Key
   - Client ID
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.

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 server. In the **Redirect URI** field, specify the URI that you entered in the 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 application registration**.
5. In the **Name** field, enter a name for the app. This is the name that users will see.
6. In the **Application type** drop-down list, select **Native**.
7. In the **Redirect URI** field, enter
   - **com.blackberry.work://connect/o365/redirect**
8. Click **Create**.

9. After the app has been created, in the toolbar under the name of the app, click **Settings**.
10. Under API Access, click **Required permissions**.
11. Click **Add**.
12. Click **Select an API**
13. Select **Office 365 Exchange Online**.
14. Click **Select**.
15. Select the following permission for Office 365 Exchange Online:
    - **Access mailboxes as the signed-in user via Exchange Web Services**
16. Click **Select**.
17. Click **Done**.
18. Click **Add**.
19. Click **Select an API**.
20. Click **Microsoft Graph**.
21. Select the following permissions for Microsoft Graph:
    - **Delegated Permissions**
      - **Sign in and read user profile**
      - **Send mail as a user**
22. Click **Select**.
23. Click **Done**.
24. Click **Select an API**.
25. Click **Windows Azure Active Directory**.
26. If it is not already selected, select **Sign in and read user profile** and then click **Save** if you changed the value.
27. Click **Select**.
28. Click **Done**.
29. Click **Add**.
30. Click **Select an API**.
31. If your environment is configured for Skype for Business Online, complete the following steps:
    a) Search for and select the app name that you created for Obtain an Azure app ID for the Connect, Presence, and Docs service (for example, AzureAppIDforBEMS).
    b) Click **Select**.
    c) Select all of the permissions under **Delegated Permissions**. Make sure that all of the options are selected.
    d) Click **Select**.
    e) Click **Done**.
32. 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.
33. Click **Yes**. You can now copy the Application ID for the app that you created. It is located under the name of the app, in the Application 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.

1. Log on to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New application registration**.
5. In the **Name** field, enter a name for the app. This is the name that users will see.
6. In the **Application type** drop-down list, select **Native**.
7. In the **Redirect URI** field, enter the following:
   - **chrome-extension://glilhfdenplejncjmngdaojopbobomfa/app/ms_oauth_finish.html**
8. Click **Create**.
9. After the app has been created, in the toolbar under the name of the app, click **Settings**.
10. Under API Access, click **Required permissions**.
11. Click **Add**.
12. Click **Select an API**.
13. Select **Office 365 Exchange Online**.
14. Click **Select**.
15. Select the following permission for Office 365 Exchange Online:
    - **Access mailboxes as the signed-in user via Exchange Web Services**

16. Click **Select**.
17. Click **Done**.
18. Click **Add**.
19. Click **Select an API**.
20. Click **Microsoft Graph**.
21. Click **Select**.
22. Select the following permissions for Microsoft Graph:
    - **Sign in and read user profile**
    - **Send mail as a user**
23. Click **Select**.
24. Click **Done**.
25. Click **Windows Azure Active Directory**.
26. If it is not already selected, select **Sign in and read user profile** and then click **Save** if you changed the value.
27. 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.
28. Click **Yes**.
    You can now copy the Application ID for the app that you created. 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 application registration**.
5. In the **Name** field, enter a name for BlackBerry Tasks. This is the name that users will see.
6. In the **Application type** drop-down list, select **Native**.
7. In the **Redirect URI** field, enter the following:
   - **com.blackberry.work://connect/o365/redirect**

8. Click **Create**.
9. After the app has been created, in the toolbar under the name of the app, click **Settings**.
10. Click **Required permissions**.
11. Click **Add**.
12. Click **Select an API**.
13. Select **Office 365 Exchange Online (Microsoft.Exchange)**.
14. Click **Select**.
15. Select the following permission for Office 365 Exchange Online (Microsoft.Exchange)
    - **Access mailboxes as the signed-in user via Exchange Web Service**
16. Click **Select**.
17. Click **Done**.
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 for BlackBerry Tasks. 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.

Enable ADFS debug logging

You can turn on ADFS debugging logging to help you troubleshoot issues.

Set Trace level and enable the ADFS tracing log

1. Run command prompt as an administrator.
2. Type the following command: **C:Windowssystem32>wevtutil sl "AD FS Tracing/Debug" /L:5**
3. Open **Event Viewer.**
4. Right-click on **Application and Services Logs.** and select **View** > **Show Analytics**.

5. Navigate to AD FS Tracing – Debug.
6. Right-click and select **Enable Log** to start Trace Debugging immediately.
7. Navigate to AD FS Tracing – Debug.
8. Right-click and select **Disable Log** to stop Trace Debugging. It is difficult to scroll and search in the events page by page in the Debug Log, so it is recommended that you save all Debug events to a *.evtx file first.
9. Open the saved log again and observe that it now includes ADFS Tracing events. These can be analyzed, according to the applicable timestamps, for troubleshooting purposes.

Enable Object access auditing to see access data in security logs

To observe detailed information about access activities on the ADFS servers, you must enable object access auditing in two locations on the ADFS servers:

1. To turn on auditing in the ADFS UI, do the following:
   a. On the primary ADFS server, right-click on **Service.**
   b. Select the **Success audits** and **Failure audits** checkboxes. These settings are valid for all ADFS servers in the farm.
2. To modify the Local Security Policy, do the following:
   a. Search Windows for **gpedit.msc**.
   b. Navigate to **Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy**.
   c. In the policy list, right-click on **Audit Object Access**
   d. Select the **Success** and **Failure** checkboxes. These settings have to be enabled in the Local Security Policy on each ADFS server (or in an equivalent GPO that is set in Active Directory).
   e. Click **OK**.
   f. Open the security event logs on the ADFS servers and search for the timestamps that correspond to any testing or troubleshooting that is being conducted.

When ADFS is not accessible outside of the work network, attempts to use Office 365 modern authentication may fail in BlackBerry Work, Notes, and Tasks

When ADFS is not accessible outside of the work network, attempts to use modern authentication may fail, especially for Android devices, and BlackBerry Work may display a blank white screen for a long time.

BlackBerry Work requires a valid path to the ADFS server. The required network path depends on whether ADFS is published externally and what routing rules are configured in the BlackBerry Dynamics Connectivity profile. Android devices also require additional configuration to allow connectivity to ADFS servers that are hosted internally and not published externally. These steps are not required if your ADFS servers are published externally.

For ADFS servers hosted internally, complete the following steps.

Update the connectivity profile to direct the connection to ADFS through the BlackBerry Proxy:

1. Depending on your environment, navigate to the Connectivity Profile location:
   - BlackBerry UEM 12.8 or later: Policies and Profiles > Networks and Connections > BlackBerry Dynamics
   - BlackBerry UEM 12.7 or earlier: Policies and Profiles > Connectivity
2. Select the profile that you need to update.
3. Under **Additional Servers**, add the FQDN of the ADFS host name.

Update the app configuration settings

1. In the BlackBerry UEM console, navigate to **Apps > BlackBerry Work**.
2. Select the app configuration that you need to update.
3. Select the **Advanced Settings** tab.
4. Check **Proxy Office 365 Modern Authentication requests** (Android only).
5. Save settings.

Update the WIASupportedUserAgent string

If ADFS is configured to allow Windows Integrated Authentication for internal connections, it may be necessary to modify the 'WIASupportedUserAgent' property on ADFS. Depending on your configuration, BlackBerry Work can be configured to use Forms Based authentication instead. For information on how to set this value, see Configure single sign-on for BlackBerry Dynamics apps in BlackBerry UEM.

Note: Generally, it is recommended that you use forms based authentication. Windows Integrated Authentication is not directly supported by BlackBerry Work. However, WIA can be used if Kerberos Constrained Delegation is also configured. For more information on implementing KCD with BlackBerry Work, see http://support.blackberry.com/kb/articleDetail?articleNumber=000046407.

Legal notice

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
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada