



Configuring Office 365 and Hybrid Office 365 environments Modern Authentication for BlackBerry Dynamics Apps

March 2021

Contents

- System requirements..... 5**

- Steps to set up modern authentication for BlackBerry Dynamics apps.....6**

- Configure BlackBerry Work for iOS and Android app settings for Office 365 modern authentication..... 7**
 - Configure BlackBerry Work for iOS and Android app settings for BEMS-Docs..... 8
 - Obtain an Azure app ID for BlackBerry Work.....8
 - Allow users to use the UPN to authenticate to Microsoft Exchange Online..... 9

- Enable modern authentication for the Mail service in BEMS..... 11**
 - Obtain an Azure app ID for BEMS with credential or passive authentication.....14
 - Obtain an Azure app ID for BEMS with certificate-based authentication..... 15
 - Associate a certificate with the Azure app ID for BEMS..... 16
 - Import the trusted mutual TLS certificates into the BEMS keystore..... 19

- Enable modern authentication for the Connect and Presence services in BEMS..... 20**
 - Configure Skype for Business Online for the Connect service.....20
 - Obtain an Azure app ID for the Connect client..... 20
 - Allow users to use the UPN to authenticate to Skype for Business Online.....21
 - Configure Skype for Business Online for the Presence service..... 22

- Obtain an Azure app ID for the BEMS-Connect, BEMS-Presence, and BEMS-Docs component service..... 24**

- Enable modern authentication for the Docs service in BEMS..... 28**
 - Configuring Docs for Rights Management Services..... 28
 - Steps to deploy Azure IP Rights Management Services support for the Docs service.....29
 - Enable modern authentication for Microsoft SharePoint Online.....31
 - Enable the use of an alternate email address to authenticate to BEMS-Docs..... 32

- Configure BlackBerry Work for Windows and macOS app settings for Office 365 modern authentication..... 33**
 - Obtain an Azure app ID for BlackBerry Work for Windows and macOS..... 33

Configure BlackBerry Notes and BlackBerry Tasks app settings for Office 365 modern authentication.....	35
Obtain an Azure app ID for BlackBerry Tasks and BlackBerry Notes	35
Configuring Good Enterprise Services in BlackBerry UEM or Good Control.....	37
Verify that Good Enterprise Services are available in BlackBerry UEM.....	37
Add the BEMS instance to the Good Enterprise Services and BlackBerry Work entitlement app.....	37
Additional configuration options.....	40
Configure single sign-on for BlackBerry Access in BlackBerry UEM.....	40
Configure alternate login and Office 365 resource URLs.....	41
Troubleshooting.....	42
How data flows when BlackBerry Work uses Office 365 modern authentication.....	42
Authentication fails when email address and UPN do not match.....	42
Expected behavior when an Microsoft Active Directory password is changed.....	43
Steps to migrate existing on-premises users to Microsoft Outlook Online using modern authentication....	43
Configure and validate modern authentication.....	45
Enable the mailbox migration flow.....	45
Legal notice.....	47

System requirements

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

- Office 365, Microsoft Exchange Online, or hybrid Microsoft Office 365 and on-premises Microsoft Exchange Server*
- BlackBerry UEM version 12.8 or later
- BlackBerry Enterprise Mobility Server version 2.10 or later

Note: * Hybrid Microsoft Office 365 and on-premises Microsoft Exchange Server environments are supported in BEMS 3.2 or later.

- The following are the apps that you require. To allow users in your environment to use the latest features and enhancements, it is recommended that users upgrade the BlackBerry Dynamics apps on their devices to the latest software versions.
 - BlackBerry Notes for Android
 - BlackBerry Notes for iOS
 - BlackBerry Tasks for Android
 - BlackBerry Tasks for iOS
 - BlackBerry Work for Android
 - BlackBerry Work for iOS
 - BlackBerry Work for macOS
 - BlackBerry Work for Windows
 - BlackBerry Connect for Android
 - BlackBerry Connect for iOS
- Authentication server or identity provider requirements
 - Users must be able to authenticate using their email address or UPN. Other identifiers are not supported.
 - To support Windows Integrated Authentication or Kerberos Constrained Delegation, you must synchronize your on-premises Active Directory to Microsoft Azure Active Directory Connect, and the Username value in Azure AD must be the email address or UPN.
- Modern authentication works as expected before you enable BlackBerry Dynamics apps. Verify the functionality by successfully opening a browser, navigating to outlook.office365.com, and entering the credentials of a user with a mailbox on Microsoft Exchange Online.

Steps to set up modern authentication for BlackBerry Dynamics apps

Complete the following steps to set up your environment to use Office 365 or hybrid Microsoft Office 365 and on-premises Microsoft Exchange Server modern authentication with BlackBerry Dynamics apps.

Step	Action
1	Make sure that your environment meets the minimum system requirements.
2	<p>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 or hybrid Microsoft Office 365 and on-premises Microsoft Exchange Server modern authentication. Any of the following apps can be configured:</p> <ul style="list-style-type: none">• BlackBerry Work for iOS and Android• BlackBerry Work for macOS and Windows• BlackBerry Notes• BlackBerry Tasks
3	In BEMS, enable modern authentication for the Mail service.
4	In BEMS, enable modern authentication for the Connect and Presence services.
5	<p>In BEMS, enable modern authentication for the Docs service:</p> <ul style="list-style-type: none">• Enable modern authentication for the the Microsoft SharePoint Online• Steps to deploy Azure IP Rights Management Services support for the Docs service
6	In BlackBerry UEM, configure Good Enterprise Services and assign the BlackBerry Work entitlement to users.
7	Optionally, configure additional options.

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 Configuration** settings tab, under **Office 365 Settings** configure the following settings:
 - a) Optionally, 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. This option overrides autodiscover and provisions BlackBerry Work to use outlook.office365.com for mail settings. If this is not required in your environment, do not enable this option and manually configure your ActiveSync endpoint in the BlackBerry Work app configuration settings on the Basic Configuration tab. For more information, see the [BlackBerry Work app configuration settings](#).
 - 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) Select the **Use Office 365 Modern Authentication for Presence** option to use modern authentication with the presence service. The **Enable presence service** option on the Apps Settings tab must also be selected.
 - g) 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 organization's authentication server is not published externally to the internet. If your authentication server is published externally, this setting is optional.
6. Optionally, enable the **Migration Flow Enabled** option. Enabling this option allows users' email to continue to synchronize and minimizes downtime during the migration. If this option is not enabled, users can't send or receive email during the migration. For more information about enabling the migration flow, see [Enable the mailbox migration flow](#).
7. Optionally, configure any other settings. See [app configuration settings](#) for a description of all of the settings that you can configure.
8. Click **Save**.

Configure BlackBerry Work for iOS and Android app settings for BEMS-Docs

Complete these steps if your environment is configured for Microsoft SharePoint Online for the BEMS-Docs service and users' mail server is Microsoft Exchange on-premises.

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 Configuration** tab, under **Office 365 Settings** configure the following settings:
 - a) Select the **Use Office 365 Settings** option.
 - 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 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.
6. 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. If you need to obtain multiple Azure app IDs (for example, Docs, BEMS, and BlackBerry Connect), it is recommended that you create a separate app ID for each app.

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. Complete one or more of the following tasks:

Environment	Permissions
If your environment is configured to use Microsoft Office 365	<ol style="list-style-type: none"> a. Click Microsoft Graph. If Microsoft Graph is not listed, add Microsoft Graph. b. Set the following permissions: <ul style="list-style-type: none"> • In delegated permissions, select the following permissions: <ul style="list-style-type: none"> • Sign in and read user profile checkbox (User > User.Read) • Send mail as a user checkbox (Mail > Mail.Send) c. Click one of the following: <ul style="list-style-type: none"> • If Microsoft Graph existed in the API permissions, click Update permissions. • If you needed to add Microsoft Graph, click Create. d. Click Add permissions.
If your environment is configured to use Microsoft Exchange Online for email	<ol style="list-style-type: none"> a. Click the Microsoft Graph. b. Set the following permissions: <ul style="list-style-type: none"> • In delegated permissions, select Access mailboxes as the signed-in user via Exchange Web Services checkbox (EWS > EWS.AccessAsUser.All). c. Click Add permissions.
If your environment is configured for Microsoft Exchange Online and uses Skype for Business Online for meetings	<ol style="list-style-type: none"> a. Click Skype for Business. b. Select all delegated permissions. <ol style="list-style-type: none"> 1. Click Delegated permissions. 2. Click expand all. Make sure that all options are selected. c. Click Add permissions.
If your environment is configured to use Microsoft SharePoint Online or Azure-IP to enable modern authentication for the BlackBerry Work client	<ol style="list-style-type: none"> a. Click the APIs my organization uses tab. b. Search for and click the BEMS app that you created in Obtain an Azure app ID for the BEMS-Connect, BEMS-Presence, and BEMS-Docs component service. For example, AzureAppIDforBEMS. c. Select all delegated permissions. <ol style="list-style-type: none"> 1. Click Delegated permissions. 2. Click expand all. Make sure that all options are selected. d. Click Add permissions.

13. Click **Grant admin consent for <Organization name>** to apply the permissions for the app. These settings will not be applied to the app until you have granted the updated permissions.

14. Click **Yes**.

15. 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.

Allow users to use the UPN to authenticate to Microsoft Exchange Online

If users in your environment are configured with UPNs that are different from their email address, complete the following steps for the BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks client. No additional

configuration is required to allow users to use UPN to authenticate when they use BlackBerry Connect. However, if your users' BlackBerry Connect UPNs don't match their email addresses, you must disable the username validation checking. For instructions, see [Allow users to use the UPN to authenticate to Skype for Business Online](#).

By default, BlackBerry UEM creates implicit UPNs for BlackBerry Dynamics apps (for example, *samAccountName@Internal_domain_name*) and uses the implicit UPN to authenticate to Microsoft Exchange Online. Consider the following scenario for userA using BlackBerry Work in your environment:

- BlackBerry UEM creates an implicit UPN: userA@example.internaldomain.com
- The Active Directory has the following information for userA and environment:
 - Domain sign in is example.internal.com
 - SamAccountName is userA
 - UserA email address format is *firstname.lastname@example.com*
 - UserA's UPN (explicit UPN) is userA@example.com

In this scenario, the external email domain and the internal domain are different. As a result, the explicit UPN in the Active Directory and the implicit UPN created by BlackBerry UEM don't match and authentication fails. For more information, visit support.blackberry.com/community to read article 58448.

Before you begin: Make sure that the client is running version 2.19 or later.

1. In the BlackBerry UEM console, on the menu bar, click **Apps**.
2. Search for and click the app that you want to enable UPN for authentication.
3. In the **App configuration** section, click an app configuration.
4. Complete one or more of the following steps:
 - a) For BlackBerry Work, on the **Advanced Configuration** tab, in the **Exchange User Name** section, select the **UPN** checkbox.
 - b) For BlackBerry Notes and BlackBerry Tasks, on the **Exchange Settings** tab, in the **Exchange User Name** section, select the **UPN** checkbox.
5. Click **Save**.

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

Note: For information on configuring modern authentication for the Mail service using BEMS Cloud, see the [BlackBerry UEM Cloud content](#).

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

- If you have a hybrid Microsoft Office 365 and on-premises Microsoft Exchange Server environment, and you enable Modern Authentication, make sure that the on-premises Microsoft Exchange Server is configured to use hybrid modern authentication. For more information, visit <https://docs.microsoft.com/en-us/microsoft-365/enterprise/configure-exchange-server-for-hybrid-modern-authentication?view=o365-worldwide>. If the Microsoft Exchange Server is not configured appropriately, users won't receive email notifications.
 - Verify that you have the following information and completed the following task:
 - If you enable modern authentication, obtain 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:
 - Obtain 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](#)
 - If your environment uses Modern Authentication with Credential Authentication and the federation metadata endpoint is protected by mutual TLS authentication, make sure that you imported the mutual TLS certificate in to the BEMS keystore. For instructions, see [Import the mutual TLS certificates into the BEMS keystore](#). This feature requires that you enable modern authentication using Credential or Client Certificate.
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 a defined BEMS username and password to authenticate to Microsoft Office 365 using Basic Authentication.	<p>a. In the Username field, enter the service account's User Principal Name (UPN)</p> <p>b. In the Password field, enter the password for the service account.</p> <p>Important:</p> <p>When using modern authentication, BEMS leverages the WS-Trust protocol. For BEMS to authenticate with AzureAD, the MetadataExchangeUri value must be set within Azure in your organization's Federation settings. If the MetadataExchangeUri value is not set, BEMS cannot authenticate using the modern authentication settings. For more information, visit https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoldomainauthentication?view=azureadps-1.0.</p> <p>Some third-party identity providers (IDPs) may not require this value to be set during the initial configuration. If the MetadataExchangeUri for your organization is not currently set, consult with your IDP vendor or with Microsoft before you make any changes to your Federation settings.</p>
Client Certificate	This option uses a client certificate to allow the BEMS service account to authenticate to Microsoft Office 365 using Basic Authentication.	<p>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 to the Azure app ID for BEMS.</p> <p>b. In the Enter PFX file Password field, enter the password for the client certificate.</p>
Passive Authentication	This option uses an identity provider (IDP) to authenticate the user and provide BEMS with OAuth tokens to authenticate to Microsoft Office 365. In a hybrid environment, authenticates to on-premises Microsoft Exchange Server*.	Proceed to step 5.

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

4. Select the **Enable Modern Authentication** checkbox.
5. If your environment uses Client certificate authentication, 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>> or <https://login.microsoftonline.com/<tenantid>>). By default, the field is prepopulated with <https://login.microsoftonline.com/common>.
6. In the **Client Application ID** field, enter one of the following Azure app IDs:
 - Credential and passive authentication: [see Obtain an Azure app ID for BEMS with credential authentication](#)
 - Certificate-based authentication: [Obtain an Azure app ID for BEMS with certificate-based authentication](#)
7. In the **Server Name** field, enter the FQDN of the Microsoft Office 365 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. If you use Credential or Client certificate authentication and the metadata endpoint is protected by mutual TLS authentication, select the **Use Mutual TLS Authentication** check box to allow BEMS to respond to mutual TLS authentication requests. This step requires that the mutual TLS certificate is imported into BEMS. For instructions, see [Import the mutual TLS certificates into the BEMS keystore](#).

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

9. If you use Passive Authentication, complete the following steps:
 - a) In the **Redirect URI** field, enter the URL that the IDP redirects the administrator to when the client app ID is authorized and the authentication tokens are provided. If you remotely log in to the computer that hosts the BEMS and perform the configuration from the computer's browser, enter <https://localhost:8443/PassiveAuth>), otherwise enter <https://<FQDN of the computer that hosts the BEMS instance>:8443/PassiveAuth>.

Note: The URI must be the same as the BEMS URI and whitelisted in the portal for Azure application ID.

 - b) Click **login**.
 - c) Enter the credentials for the service account.
 - d) Click **OK** to acknowledge that the authentication tokens were obtained
 - e) Important: BEMS doesn't automatically refresh the OAuth tokens. Repeat steps b to d to refresh the OAuth tokens. The tokens expiration time depends on your tenant policy (by default, the token expiration is 90 days). When the OAuth tokens expire, email notifications on the users' devices stop. The OAuth token expiration is displayed after you login to the IDP.

10. 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	<p>If you select to override the autodiscover process, BEMS uses the override URL to obtain user information from Microsoft Office 365.</p> <ol style="list-style-type: none"> 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).

Task	Steps
Autodiscover and Microsoft Exchange Server options	<ol style="list-style-type: none"> 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.

11. 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.

12. 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 or passive authentication

If you need to obtain multiple Azure app IDs (for example, Docs, BlackBerry Work, and BlackBerry Connect), it is recommended that you create a separate app ID for each app.

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

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

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

If you need to obtain multiple Azure app IDs (for example, Docs, BlackBerry Work, and BlackBerry Connect), it is recommended that you create a separate app ID for each app.

1. Sign in to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for the app.
6. Select a supported account type.
7. Optionally, in the **Redirect URI** section, in the drop-down list, select **Public/client (mobile & desktop)** and enter `http://<name of the app given in step 5>`.
This app is a daemon, not a web app, and does not have a sign-on URL.
8. Click **Register**. The new registered app appears.
9. In the **Manage** section, click **API permissions**.
10. Click **Add a permission**.
11. In the **Select an API** section, click **APIs my organization uses**.
12. Click **Office 365 Exchange Online**.
13. Set the following permissions for Office 365 Exchange Online:
 - Application permissions: Use Exchange Web Service with full access to all mailboxes (**full_access_as_app**)
14. Click **Add permissions**.
15. Click **Microsoft Graph**. If the Microsoft Graph API permission is not listed, add it.
16. Set the following permission for Microsoft Graph.
 - Delegated permissions: Sign in and read user profile (**User > User.Read**)
17. Click **Add permissions**.
18. Click **Grant admin consent**.
19. Click **Yes**.
20. Click **Overview** to view the app that you created in step 5. Copy the **Application (client) ID**. The Application (client) ID is displayed in the main **Overview** page for the specified app. This is used as the **Client application ID** in the BEMS dashboard when you enable modern authentication and configure BEMS to communicate with Microsoft Office 365.

After you finish: [Associate a certificate with the Azure app ID for BEMS](#)

Associate a certificate with the Azure app ID for BEMS

You can request and export a new client certificate from your CA server or use a self-signed certificate. The private key must be in .pfx format to upload to the BEMS dashboard. For more information, see [Enable modern authentication for the Mail service in BEMS](#). The public key can be exported as a .cer or .pem file to upload to Microsoft Azure.

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 [Obtain an Azure app ID for BEMS with certificate-based authentication](#). 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 (.pem or .cer file) 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**.

Import the trusted mutual TLS certificates into the BEMS keystore

In environments where the metadata endpoint is protected by mutual TLS authentication, you must import the mutual TLS certificate into the BEMS keystore. Adding this certificate allows BEMS respond to mutual TLS verification requests as required. Use DBManager to import the certificates. By default, DBManager is located in the installation folder at *<drive>:\GoodEnterpriseMobilityServer\GoodEnterpriseMobilityServer\DBManager*.

Before you begin: Save a copy of the .pfx certificate that you exported from the Certificate Authority to a convenient location on the computer that hosts BEMS.

1. On the computer that hosts the on-premises BEMS, verify that the PATH System variable includes the path to the JAVA directory.
 - a) In a command prompt, type `set | findstr "Path"`.
 - b) Press **Enter**.
2. Import the mutual TLS certificate.
 - a) On the computer that hosts BEMS, in a command prompt run as administrator, navigate to DBManager.
 - b) Type, `tools\dbmanager\target>java -classpath "*" com.good.tools.db.client.Client -dbHost "localhost" -dbName "BEMS_DB_name" -dbType sqlserver -action addprivatekey -keyPassword "password" -p12File "<certificate_file-path>/<file name>.pfx" -alias "mutualTLS" -tenantId "default" -integratedAuth true`
3. In the Windows Service Manager, restart the Good Technology Common Services service.
4. Repeat step 4 on each computer that hosts the BEMS-Mail component.

Enable modern authentication for the Connect and Presence services in BEMS

Depending on your environment, configure one or both of the following services:

- [Enable modern authentication for the Connect service](#)
- [Enable modern authentication for the Presence service](#)

Configure Skype for Business Online for the Connect service

Before you begin:

Have the following information:

- Skype for Business Online tenant name
- [Connect service app ID and app Key](#)
- [BlackBerry Connect app ID](#)

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Connect**.
2. Click **Service Account**, enter the BEMS service account credentials, and click **Save**.
3. Click **Skype for Business**.
4. Configure the Skype for Business Online settings:
 - a) Select the **Skype for Business Online** checkbox.
 - b) In the **Tenant name/ID** field, enter the tenant name for your Skype for Business Online. If you need to connect to more than one tenant, enter `common`.
 - c) In the **BlackBerry BEMS Connect/Presence Service App ID** field, enter the BlackBerry BEMS Connect service app ID. For instructions on obtaining the app ID, see [Obtain an Azure app ID for the BEMS-Connect, BEMS-Presence, and BEMS-Docs component service](#).
 - d) In the **BlackBerry BEMS Connect/Presence Service App Key** field, enter the BlackBerry BEMS Connect service app key. For instructions on obtaining the App Key, see [Obtain an Azure app ID for the BEMS-Connect, BEMS-Presence, and BEMS-Docs component service](#).
 - e) In the **BlackBerry Connect Client App ID** field, enter the BlackBerry Connect client app ID. For instructions, see [Obtain an Azure app ID for the Connect client](#).
5. Click **Test** to verify that the Azure information is accurate.
6. Sign in to a user account.
7. Click **Save**.

After you finish:

Depending on your environment configuration, you can configure BEMS to allow users to provision the BlackBerry Connect app using an email address that is different from the email address used to login to Skype for Business Online. For more information about setting the `ucwa.appresource.uservalidation.skip` parameter and understanding the settings in the common settings configuration file, see "[Appendix: Understanding the Skype for Business Online Common Settings configuration file](#)" in the [Connect Configuration content](#).

Obtain an Azure app ID for the Connect client

Before you begin: To grant permissions, you must use an account with tenant administrator privileges. If you need to obtain multiple Azure app IDs (for example, BlackBerry Work, BEMS, and Docs), it is recommended that you create a separate app ID for each app.

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 application.
6. Select a supported account type.
7. In the **Redirect URI** drop-down list, select **Public client (mobile & desktop)** and enter `urn:ietf:wg:oauth:2.0:oob`
8. Click **Register**.
9. Add an additional Redirect URI.
 - a. In the App that you registered, on the **Overview** page, click the link for the URI beside **Redirect URIs**.
 - b. In the **Mobile and desktop applications** section, click **Add URI**.
 - c. In the blank field, enter `com.blackberry.connect://ADAL/`
 - d. In the **Advanced Settings** section, set the **Treat application as a public client** to **Yes**.
 - e. Click **Save**.
10. Click **API permissions**.
11. Click **Add a permission**.
12. In the **Select an API** section, click **APIs my organization uses**.
13. Search for and select the application name that you created for [Obtain an Azure app ID for the BEMS-Connect, BEMS-Presence, and BEMS-Docs service](#).
14. Click **Add permissions**.
15. Complete only one of the following tasks:

Important: These tasks requires tenant administrator privileges.

 - In the **API permissions** screen, click **Grant admin consent for <organizational directory name>**. Click **Yes**.
 - Click **Azure Active Directory > Users > User settings**. Click **Manage how end users launch and view their applications**. Set the **Users can consent to apps accessing company data on their behalf** to **No**. Click **Save**.

Complete this option to present each BlackBerry Connect user with a prompt to approve that their user account is used to access the Connect service when they log in.
16. Copy the **Application (client) ID**. The Application (client) ID is displayed in the main **Overview**. This is used for the following:
 - **Client ID** in the Azure portal, **Expose an API > Add a client application** screen
 - **BlackBerry Connect Client App ID** in the BEMS dashboard for BlackBerry Connect
 - **BlackBerry Presence Client App ID** in the BEMS dashboard for BlackBerry Presence

Allow users to use the UPN to authenticate to Skype for Business Online

You can configure BEMS to allow users to authenticate to Skype for Business Online using their UPN address when it is different from the email address that was used to install and activate the BlackBerry Connect app.

Complete this task only if your environment uses modern authentication. You can configure BEMS to disable validating the email address when users authenticate to Skype for Business Online or the environment uses Azure-IP.

1. If your users are configured with UPNs that are different from their email address, enable the "Use explicit UPN" property to allow BlackBerry Connect to authenticate to Microsoft Office 365. For more information, see [the BlackBerry UEM on-premises configuration](#) content.
 - a) In BlackBerry UEM, on the menu bar, click **Settings > BlackBerry Dynamics > Global Properties**.
 - b) Under the **Kerberos Constrained Delegation** heading, select the **Use explicit UPN** checkbox.
 - c) Click **Save**.
2. Sign in to the computer that is running the BEMS-Connect service.
3. In a browser, open the Apache Karaf Web Console Configuration web site. Type `https://localhost:8443/system/console/configMgr` and login as administrator with the appropriate Microsoft Active Directory credentials.
4. On the menu, click **OSGi > Configuration**.
5. Click **Blackberry Connect UCWA common settings**.
6. In the `ucwa.appresource.uservalidation.skip` field, type `true`.
7. Click **Save**.
8. Close the browser.

Configure Skype for Business Online for the Presence service

Environments configured to use Skype for Business Online that are using non-trusted application mode use Unified Communications Web API (UCWA) software for the Presence service to communicate with the instant messaging server.

Before you begin:

- Have the following information. If you configured the Connect service, reuse the tenant name and app ID and app Key. For instructions, see [Obtain an Azure app ID for the BEMS-Connect, BEMS-Presence, and BEMS-Docs component service](#).
 - Tenant name
 - Service app ID and app Key
 - [BlackBerry Work app ID](#)
1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Presence**.
 2. If necessary, click **Service Account** and type the login credentials for the BEMS service account.
 3. Click **Skype for Business**.
 4. Configure the Skype for Business Online settings:
 - a) Select the **Skype for Business Online** checkbox.
 - b) In the **Tenant name/ID** field, enter the tenant name for your Skype for Business Online. If you need to connect to more than one tenant, enter `common`.
 - c) In the **BlackBerry BEMS Connect/Presence Service App ID** field, enter the BlackBerry BEMS Connect service app ID. For instructions on obtaining the app ID, see [Obtain an Azure app ID for the BEMS-Connect, BEMS-Presence, and BEMS-Docs component service](#).
 - d) In the **BlackBerry BEMS Connect/Presence Service App Key** field, enter the BlackBerry BEMS Connect service app key. For instructions on obtaining the app key, see [Obtain an Azure app ID for the BEMS-Connect, BEMS-Presence, and BEMS-Docs component service](#).
 - e) In the **BlackBerry Presence Client App ID** field, enter the enter the BlackBerry Work app ID. For instructions, see [Obtain an Azure app ID for BlackBerry Work](#).
 5. Click **Test** to verify that the Azure information is valid.
 6. Sign in to a user account.

7. Click **Save**.
8. If you configured the Presence service for Skype for Business Online, you do not need to start the Good Technology Presence service. Skype for Business Online don't require the Presence service to view users' presence status. If you try to start the service, the following error message is displayed. **Windows could not start the Good Technology Presence service on Local Computer. Error 5: Access denied.**

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

When your environment is configured for Skype for Business Online, Microsoft SharePoint Online, Microsoft OneDrive for Business, 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 environment 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 permissions.

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

Service	Permissions
<p>If you configure BEMS-Connect to use Skype for Business Online</p>	<ul style="list-style-type: none"> a. Click the Microsoft APIs tab. b. Click Skype for Business. c. Set the following permissions: <ul style="list-style-type: none"> • In application permissions, select all of the permissions. <ul style="list-style-type: none"> 1. Click Application permissions. 2. Click expand all. Make sure that all options are selected. • In delegated permissions, select all of the permissions <ul style="list-style-type: none"> 1. Click Delegated permissions. 2. Click expand all. Make sure that all options are selected. d. Click Add permissions. e. If you enable saving the conversation history, complete the following steps: <ul style="list-style-type: none"> 1. On the API permissions page, click Add a permission. 2. In the Select an API section, click Microsoft APIs tab. 3. Click Microsoft Graph. 4. In delegated permissions, select the Access mailboxes as the signed-in user via Exchange Web Services checkbox (EWS > EWS.AccessAsUser.All) 5. Click Add permissions.
<p>If you configure BEMS-Presence to use Skype for Business Online</p>	<ul style="list-style-type: none"> a. Search for and click Skype for Business. b. Set the following permissions: <ul style="list-style-type: none"> • In application permissions, select all of the permissions. <ul style="list-style-type: none"> 1. Click Application permissions. 2. Click expand all. Make sure that all options are selected. • In delegated permissions, select all of the permissions. <ul style="list-style-type: none"> 1. Click Delegated permissions. 2. Click expand all. Make sure that all options are selected. c. Click Add permissions.
<p>If you configure BEMS-Docs to use Microsoft SharePoint Online or Microsoft OneDrive for Business</p>	<ul style="list-style-type: none"> a. Search for and click SharePoint. b. Set the following permissions: <ul style="list-style-type: none"> • In application permissions, clear all of the permissions. <ul style="list-style-type: none"> 1. Click Application permissions. 2. Click expand all. Make sure that all options are cleared. • In delegated permissions, select the Read and write items and item lists in all site collections checkbox. None. Clear the check boxes for all options. • Delegated permissions Select the Read and write items and lists in all site collections checkbox. (AllSite > AllSites.Manage) c. Click Add permissions.

Service	Permissions
If you use Microsoft Azure-IP	<p>a. Click Microsoft Graph. If Microsoft Graph is not listed, add Microsoft Graph.</p> <p>b. Set the following permissions:</p> <ul style="list-style-type: none"> • 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). <p>c. Click Update permissions.</p> <p>d. Add a permission.</p> <p>e. In the Select an API section, click Azure Rights Management Services. Set the following permissions:</p> <ul style="list-style-type: none"> • In application permissions, select all of the permissions. <ol style="list-style-type: none"> 1. Click Application permissions. 2. Make sure that all Content options are selected. • In delegated permissions, select the user_impersonation checkbox. <p>f. Click Add permissions.</p> <p>g. Click Add a permission.</p> <p>h. In the Select an API section, click APIs my organization uses.</p> <p>i. Search for and click Microsoft Information Protection Sync Service. Set the following permission:</p> <ul style="list-style-type: none"> • In delegated permissions, select the Read all unified policies a user has access to checkbox (UnifiedPolicy > UnifiedPolicy.User.Read). <p>j. Click Add permissions.</p>

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

Important: This step requires tenant administrator privileges.

14. To allow autodiscovery to function as expected, set the authentication permissions. Complete the following steps:

- a) In the **Manage** section, click **Authentication**.
- b) Under the **Implicit grant** section, select the **ID Tokens** checkbox.
- c) In the **Default client type**, select **No**.
- d) Click **Save**.

15. Define the scope and trust for this API. In the **Manage** section, click **Expose an API**. Complete the following tasks.

Task	Steps
Add a scope	<p>The scope restricts access to data and functionality protected by the API.</p> <ol style="list-style-type: none"> Click Add a scope. Click Save and continue. Complete the following fields and settings: <ul style="list-style-type: none"> 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. Click Add Scope.
Add a client application	<p>Authorizing a client application indicates that the API trusts the application and users shouldn't be prompted for consent.</p> <ol style="list-style-type: none"> Click Add a client application. In the Client ID field, enter the client ID that you recorded in step 9 above. Select the Authorized scopes checkbox to specify the token type that is returned by the service. Click Add application.

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

- Click **New client secret**.
- In the **Description** field, enter a key description up to a maximum of 16 characters including spaces.
- Set an expiration date (for example, In 1 year, In 2 years, Never expires).
- Click **Add**.
- 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 BEMS-Connect and BEMS-Presence services and **BEMS Service Application Key** in the BEMS-Docs service in the BEMS Dashboard.

Enable modern authentication for the Docs service in BEMS

Depending on your environment, configure the following:

- [Enable modern authentication for Microsoft SharePoint Online](#)
- [Steps to deploy Azure IP Rights Management Services support for the Docs 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 and Office Online 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	<ul style="list-style-type: none">• View protected documents directly in BlackBerry Work.• Protect unprotected documents in BlackBerry Work.• Change permissions for documents in BlackBerry Work.• Upload a new file and save it as protected. This feature requires BlackBerry Work app 2.18 or later.	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Share the Microsoft Office Web Apps or Office Online Server 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 or Office OnlineServer 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 BEMS-Connect, BEMS-Presence, and BEMS-Docs component service.

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 " <i>To convert templates to labels</i> ".
5	Configure the Docs security settings

Configure the Docs security settings

Docs security settings control acceptable Microsoft SharePoint Online domains, the URL of the approved Microsoft Office Web Apps (OWAS) and Office Online Server, 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 BEMS-Connect, BEMS-Presence, and BEMS-Docs component service](#).
 - 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 or Office Online 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. For instructions about obtaining the Azure registration fields, see [Obtain an Azure app ID for the BEMS-Connect, BEMS-Presence, and BEMS-Docs component service](#).
10. Click **Save**.
11. Restart the Good Technology Common Services service for the changes to take effect.

Enable modern authentication for Microsoft SharePoint Online

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

Before you begin: If you enable modern authentication, configure 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**. For information about authentication providers and the storage provider that each can be used for, see ['Authentication providers' in the BlackBerry Docs Service Configuration content](#).
 - **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 **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 more information, see [Managing Repositories](#).

Enable the use of an alternate email address to authenticate to BEMS-Docs

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. Complete this task only if your environment is configured to use one of the following:

- If your environment is configured to use Windows authentication, you can configure BEMS to use the UserPrincipalName (UPN), email address or any other Active Directory attribute to authenticate to Microsoft SharePoint Online. By default, the UserPrincipalName attribute is used.
- If your environment uses modern authentication, you can configure BEMS to disable validating the email address when users authenticate to Microsoft SharePoint Online or the environment uses Azure-IP.

1. Sign in to the computer that is running the BEMS-Docs service.
2. In a browser, open the BEMS Karaf Console Configuration web site. Type `https://localhost:8443/system/console/configMgr` and login as administrator with the appropriate Microsoft Active Directory credentials.
3. On the menu, click **Main > Gogo**.
4. In the command, type one of the following commands:

Task	Attribute	Description
Authenticate to Microsoft SharePoint Online using mail	<code>docs:config</code> <code>SAMLUsernameAttribute</code> <code>mail</code>	Allows users to use their email address to authenticate to Microsoft SharePoint Online instead of the user's userPrincipalName. To use the users' UPN again to authenticate, type <code>docs:config</code> <code>SAMLUsernameAttribute</code> <code>UserPrincipalName</code>
Disable user validation when authenticating to one of the following: <ul style="list-style-type: none">• Microsoft SharePoint Online configured for modern authentication• Azure-IP	<code>docs:config</code> <code>adal.uservalidation.skip</code> <code>1</code>	Disables validation of the user's email address.

5. Close the browser.

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 to 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 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://glilhfdenplejncjmgdaojobbobomfa/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 (**EWS > 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 to 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 authentication server (for example, Active Directory Federation Services (ADFS) server) is not published externally to the internet. If your authentication 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.

Configuring Good Enterprise Services in BlackBerry UEM or Good Control

When you configure Good Enterprise Services in your environment, you perform the following actions:


1. [Verify the Good Enterprise Services app is available in BlackBerry UEM.](#)
2. [Add BEMS to the Good Enterprise Services entitlement app.](#)
3. Add the Good Enterprise Services entitlement app to users. You can use one or more of the following options. For instructions, [see the BlackBerry UEM Administration content.](#)
 - Apply the app directly by completing one of the following tasks:
 - [Assign the entitlement app to a user group](#)
 - [Assign the entitlement app to a user account](#)
 - [Assign the entitlement app to an app group.](#) Then complete one of the following tasks:
 - [Assign the app group to a user group](#)
 - [Assign the app group to a user account](#)

Verify that Good Enterprise Services are available in BlackBerry UEM


1. Log in to the BlackBerry UEM console.
2. On the menu bar, click **Apps**.
3. Search for **Good Enterprise Services**.





Add the BEMS instance to the Good Enterprise Services and BlackBerry Work entitlement app

You must add the BEMS instance to the Good Enterprise Services entitlement app to allow users to use the services. You must also add the BEMS instance to allow users to receive email notifications. If the BEMS instance is not added to the BlackBerry Work entitlement app, users receive email messages, but do not receive the notifications when the email messages are received. For more information about configuring your environment to support BlackBerry Dynamics apps, making the apps available to users, and configuring the app settings, see the [BlackBerry Work, Tasks, and Notes administration content.](#)

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > BlackBerry Dynamics connectivity**.
3. Click  to create a new connectivity profile or click the Default connectivity profile to edit it.
4. Complete one of the following tasks:

Task	Steps
Route all traffic	Select the Route all traffic checkbox to specify whether all BlackBerry Dynamics app data is routed through the BlackBerry Proxy. For more information about the BlackBerry Dynamics connectivity profile settings, see the Managing BlackBerry Dynamics apps content.

Task	Steps
Add the BEMS instance to the Additional servers	<ol style="list-style-type: none"> a. In the Additional servers section, click . b. In the Server field, specify the FQDN of the BlackBerry Enterprise Mobility Server. c. In the Port field, specify the port for the BlackBerry Enterprise Mobility Server. By default, the port number is 8443. d. In the Primary BlackBerry Proxy cluster drop-down list, select the name of the BlackBerry Proxy cluster that you want to set as the primary cluster. e. If necessary, in the Secondary BlackBerry Proxy cluster drop-down list, select the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.

5. Click **Save**.
6. Add the BEMS instance to the Good Enterprise Services entitlement app.
 - a) In the **App servers** section, click .
 - b) Click **Add**.
 - c) Search for and select **Good Enterprise Services**.
 - d) Click **Save**.
 - e) In the **App servers** for **Good Enterprise Services**, click .
 - f) In the **Server** field, specify the FQDN of the BlackBerry Enterprise Mobility Server.
 - g) In the **Port** field, specify the port of the BlackBerry Proxy cluster that is used to access the BlackBerry Enterprise Mobility Server.
 - h) In the **Priority** drop-down list, select the priority of the BlackBerry Proxy cluster that must be used to reach the domain.
 - i) If necessary, in the **Secondary BlackBerry Proxy cluster** drop-down list, select the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
 - j) Click **Save**.
7. Add the BEMS instance to the BlackBerry Work entitlement app.
 - a) In the **App servers** section, click .
 - b) Click **Add**.
 - c) Search for and select **BlackBerry Work**.
 - d) Click **Save**.
 - e) In the **App servers** for **BlackBerry Work**, click .
 - f) In the **Server** field, specify the FQDN of the BlackBerry Enterprise Mobility Server.
 - g) In the **Port** field, specify the port of the BlackBerry Proxy cluster that is used to access the BlackBerry Enterprise Mobility Server.
 - h) In the **Priority** drop-down list, select the priority of the BlackBerry Proxy cluster that must be used to reach the domain.
 - i) If necessary, in the **Secondary BlackBerry Proxy cluster** drop-down list, select the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
 - j) Click **Save**.
8. To save the updates to the existing profile, click **Save**.
9. To save the settings and add the new profile, click **Add**.

After you finish: Assign the entitlements to users. You can use one or more of the following options. For instructions, [see the BlackBerry UEM Administration content](#).

- Apply the app directly by completing one of the following tasks:
 - [Assign the entitlement app to a user group](#)
 - [Assign the entitlement app to a user account](#)
- [Assign the entitlement app to an app group](#). Then complete one of the following tasks:
 - [Assign the app group to a user group](#)
 - [Assign the app group to a user account](#)

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 prompts, BlackBerry Work must be BlackBerry Work 3.2 or later. Alternatively, you can configure Kerberos Constrained Delegation to suppress the password prompt. In some cases, the authentication server might need to be configured to allow BlackBerry Dynamics clients to use Windows Integration instead of Forms Based Integration. For more information about configuring the authentication server to use Windows Integration, contact your authentication service provider vendor.

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 Access in BlackBerry UEM](#)
- [Configure Kerberos Constrained Delegation for BlackBerry Dynamics apps](#)

Configure single sign-on for BlackBerry Access in BlackBerry UEM

You can enable single sign-on for BlackBerry Access 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:

- 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.
- Verify that the "Identify BlackBerry Access in User Agent" app setting is selected in BlackBerry UEM.

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.serverADFS_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 Access you need to add the BlackBerry Access user agent string to Active Directory Federation Services to allow Windows Authentication for BlackBerry Access and Kerberos constrained delegation. For all platforms, the BlackBerry Access 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-ADFSPProperties | Select -ExpandProperty  
    WIASupportedUserAgents  
$UserAgentAddArray = $CurrentUserAgents + $NewUserAgent  
Set-ADFSPProperties -WIASupportedUserAgents $UserAgentAddArray
```

- d) To verify that the Active Directory Federation Services user agent has been added, run the **Get-ADFSPProperties** command again: `Get-ADFSPProperties | Select -ExpandProperty WIASupportedUserAgents`
- e) Restart the Active Directory Federation Services service.
3. Set delegation on the Kerberos account.
- Log in to BlackBerry UEM.
 - Click **Settings > BlackBerry Dynamics > Properties**.
 - Scroll to find the value of the **gc.krb5.principal.name** property. Set this object name in Microsoft Active Directory.
 - On your Microsoft Active Directory server, click the **Delegation** tab.
 - Click **ADD** and enter the Active Directory Federation Services service account name that you discovered in step 1.
 - Add the HTTP SPN.
 - Click **OK**.

Configure alternate login and Office 365 resource URLs

If your organization uses alternate login and Office 365 resource URLs, you must configure the alternate URLs in the app configuration for each required app. For example, the U.S. Government uses alternate login and Office 365 resource URLs. The default URLs are as follows:

- Login URL: login.microsoftonline.com
- Office 365 resource URL: outlook.office365.com

The U.S. Government uses the following URLs:

- Login URL: login.microsoftonline.us
- Office 365 resource URL: outlook.office365.us

For more information about configuring alternate login and Office 365 resource URLs, visit <https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-national-cloud>.

Note: In addition to configuring the alternate login and Office 365 resource URLs, you must also ensure that your routing and connectivity profiles are configured appropriately and can access the alternate URLs.

Perform these steps on the app configuration of each required app.

- In the **Office 365 Sign On URL** field, type the login URL for your organization.
- In the **Office 365 Resource** field, type the Office 365 resource URL for your organization.
- In the **Exchange ActiveSync Settings** area, in the **ActiveSync Server** field, type the Office 365 resource URL for your organization.
- Save the app configuration.

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

By default, users authenticate using their email address when they use modern authentication. In most environments, the user's email address and username in Azure AD are the same and authentication is successful. In hybrid environments, the username attribute in Azure is synchronized from the UPN value from Active Directory. This requires the users' email address and UPN values to match for authentication to be successful.

In some environments, users' email addresses and UPN values do not match. In this scenario, authentication will fail because the authentication token returned to the client from Azure is identified as being for the wrong user and is rejected.

The following client versions provide support for administrators to allow users to authenticate using the UPN instead of their email addresses:

- BlackBerry Work for iOS version 2.19 or later
- BlackBerry Work for Android version 2.19 or later
- BlackBerry Notes for Android version 2.19 or later
- BlackBerry Notes for iOS version 2.19 or later
- BlackBerry Tasks for Android version 2.19 or later
- BlackBerry Tasks for iOS version 2.19 or later
- BlackBerry Connect for Android version 2.8.2 or later
- BlackBerry Connect for iOS version 2.8.2 or later

For instructions about how to enable users to use UPN to authenticate, see [Allow users to use the UPN to authenticate to Microsoft Exchange Online](#).

For instructions about how to configure BEMS to use an alternate email address to authenticate to BEMS-Docs, see [Enable the use of an alternate email address to authenticate to BEMS-Docs](#).

If users are running earlier versions of the client in your environment, the 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 the 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 validate that it is working correctly.

Step	Action
2	<p>Create, edit, or copy an existing BlackBerry Dynamics Connectivity profile for the migrating users. Include the following information:</p> <ul style="list-style-type: none"> If the authentication server and Microsoft Exchange Online must be accessed through the internal network, add the appropriate hosts to the Additional servers section. <p>Common Microsoft Exchange Online (Microsoft Office 365) hosts include the following:</p> <ul style="list-style-type: none"> aadcdn.msauth.net Microsoft's Content Distribution servers (for example, aad.cdn.msauth.net) login.microsoftonline.com <p>Common Microsoft Exchange Online hosts:</p> <ul style="list-style-type: none"> autodiscover-s.outlook.com outlook.office365.com <ul style="list-style-type: none"> If the authentication and Microsoft Exchange Online can be accessed using the Internet, you can improve performance by specifying "Direct" when you add the authentication server and Microsoft Office 365 servers to the Additional servers list. Note: If your Default route is set to Direct, this is not required. <p>For more information on how to configure the BlackBerry Dynamics for Microsoft Exchange Online and modern authentication, visit support.blackberry.com/community to read article 64405.</p>
3	<p>Create a new BlackBerry Work app configuration with the modern authentication settings. The new app configuration must include the following:</p> <ul style="list-style-type: none"> Same settings as the original app configuration as well as the modern authentication settings Select the "Enable Flow Enabled" checkbox and set the expiration date to allow users to send and receive email messages during the migration. If your environment doesn't use Autodiscover, specify the ActiveSync Server and Exchange Web services URL endpoint fields. If your environment is configured for Kerberos Constrained delegation or uses certificate-based authentication for the on-premises Microsoft Exchange Server, but not for the modern authentication endpoint, clear the Security settings "Use Kerberos Constrained Delegation in place of login/password" and "Use client certificate in place of login/password" checkboxes or users are prompted for credentials.
4	<p>Assign the app configuration with the correct modern authentication settings to users. For instructions, see the content for your app:</p> <ul style="list-style-type: none"> 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.

Step	Action
5	<p>Migrate user mailboxes from your on-premises Microsoft Exchange server to Microsoft Exchange Online.</p> <p>After the migration completes, users 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.</p>

Configure and validate modern authentication

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

Item	Description
<input type="checkbox"/>	Make sure that your environment meets all of the prerequisites to enable modern authentication.
<input type="checkbox"/>	<p>Perform the following tasks using test accounts:</p> <ul style="list-style-type: none"> • 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.
<input type="checkbox"/>	<p>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.</p>

Enable the mailbox migration flow

Before you begin:

- Ensure that your BlackBerry Dynamics connectivity profile is configured to route traffic for your email and authentication servers. Depending on your organization's routing requirements, this might mean one of the following:
 - **The authentication and email traffic must route through your internal network:** If your organization requires traffic to be routed internally (for example, your authentication server is not accessible publicly, or security requirements or conditional access policies require internal routing), you should ensure that the following hosts are added to the "Additional Servers" section of the connectivity profile (ensure that the route entries are configured for BlackBerry Proxy):
 - Internal Microsoft Exchange Server
 - Microsoft Office 365 server (outlook.office365.com)
 - Microsoft's Content Distribution servers (such as aad.cdn.mstauth.net)

- Authentication server (such as your Active Directory Federation Services (ADFS) server, PingFederate server, or Okta server)
- **The authentication and email traffic does not have to route through your internal network:** If your organization does not require routing these connections internally, to improve performance have these connections routed Direct instead. If your Default Route is set to Direct, then you do not need to specify any servers. If the "Default Route" is set to "BlackBerry Proxy" or "Block", then you must add the servers specified above to the "Additional Servers" list, but specify the route type as "Direct" instead.

For more information, about the BlackBerry Dynamics connectivity profile settings, see the [BlackBerry UEM Administration Guide](#).

- Ensure that your organization's app configuration is set up for Modern Authentication, Microsoft Exchange Online endpoints (Exchange ActiveSync, Exchange Web Services) and Autodiscover. For more information, see the [Administration Guide](#), and the [Modern Authentication Guide](#).
- This feature requires BlackBerry Work version 3.2 or later. Older versions of the app will immediately have the Microsoft Office 365 settings applied to them. To view a list of installed BlackBerry Work client versions, see [Export BlackBerry Dynamics app reports to a .csv file](#) in the BlackBerry UEM Administration Guide.

1. On the menu bar, click **Apps**.
2. Click the BlackBerry Work app.
3. Click the name of your organization's app configuration.
4. On the **Advanced Configuration** tab, select the **Migration Flow Enabled** option.
5. To set an expiry time, enter a date in the **Migration Flow Expiration Date** field. After the date that you enter has passed, the Migration Flow Enabled setting is ignored.
6. Click **Save**.
7. Assign the new app configuration to users who will be migrated to Microsoft Exchange Online. If you are migrating users in batches, assign the new configuration prior to migrating users.

After you have migrated all of your users' mailboxes, you can deselect the **Migration Flow Enabled** option.

Note: To ensure that your environment is configured correctly, BlackBerry recommends performing a test migration with only a few users before you perform a larger migration of users.

Note: If a new BlackBerry Work user is activated against an app configuration that has the "Migration Flow Enabled" option set, the device will immediately pick up the modern authentication and Microsoft Exchange endpoint configurations.

BlackBerry recommends that you either create a new app configuration to apply to users who will be or already are migrated to Microsoft Office 365, and have a separate app configuration for users who will continue to use an on-premises Microsoft Exchange Server.

Legal notice

©2021 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada