BlackBerry Work, Notes, and Tasks

Administration Guide

3.15

Contents

What are BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks?

BlackBerry Work makes your mobile workforce more productive, while keeping your company's data secure – regardless of device. Stay on top of business email and calendar, view online presence, manage contacts and easily work on documents. Unlike built-in email clients, BlackBerry Work integrates all your business collaboration into one integrated, easy-to-use app.

BlackBerry Notes provides you with a secure, synchronized connection to the notes in your work email account.

BlackBerry Tasks provides you with a secure, synchronized connection to your tasks in your work email account so that you can create and manage your tasks while you are away from your desk

What is BlackBerry Work?

Make your mobile workforce more productive, while keeping your company's data secure – regardless of device. Stay on top of business email and calendar, view online presence, manage contacts and easily work on documents. Unlike built-in email clients, BlackBerry Work integrates all your business collaboration into one integrated, easy-to-use app.

BlackBerry Work provides the following features:

Feature	Description
Business-class email	Securely access business email. View, send and edit attachments. Be instantly notified of key messages, and manage your inbox with smart folders and more.
Personal and shared calendar management	Easily manage your calendar with business-class capabilities. Manage and schedule meetings, check availability, attach files to invites, and quickly join conference calls and web conferences. Quickly pull up all your obligations for the day with agenda view. Never miss a meeting again. Manage shared calendars alongside your personal calendars. Effectively coordinate schedules to stay on top of important business meetings and avoid delays.
Rich contacts and one-click communication	See mobile presence and then reach colleagues using the best way, whether by phone, text message, instant message, or email.
Document access and editing	Access documents while you're on the go from native Microsoft Office Web Apps, Microsoft SharePoint, or other popular cloud storage options within the app. View, edit, and convert documents to PDF straight from your device.

What is BlackBerry Notes?

BlackBerry Notes provides you with a secure, synchronized connection to the notes in your work email account. You can use BlackBerry Notes to create and manage your notes while you're away from your desk.

BlackBerry Notes provides the following features:

Feature	Description
Rich-text editing	Create notes with a full set of rich-text editing features.
Organize and categorize	• Sort notes by title, last modified, or creation date • Organize your notes: Find a note by title, body, or both with the search tool, search in individual rich-text notes • Assign categories to your notes for an added level of organization • Synchronize your root notes folder
Secure sharing and storing of data	• Share your notes as email messages (requires BlackBerry Work) • Keep your data secure with FIPS-validated cryptography

What is BlackBerry Tasks?

BlackBerry Tasks provides you with a secure, synchronized connection to your tasks in your work email account so that you can create and manage your tasks while you are away from your desk. BlackBerry Tasks uses push notifications to make sure that changes to your tasks are synchronized and up to date on your device and in your work email account.

BlackBerry Tasks provides the following features:

Feature	Description
Rich-text editing	Use rich-text to highlight important points.
Easy management of tasks	• Experience a tabbed UI to easily manage current and future tasks • Boost engagement with recurring tasks, alerts, and sorting options • Create and view tasks directly from your calendar to easily manage deadlines • Convert an email into a task to stay on top of projects
Secure sharing and storing of data	Keep your data secure with FIPS-validated cryptography.

Steps to manage BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks with BlackBerry UEM

Step	Action
1	Review the system requirements.
2	Install and configure the BlackBerry Enterprise Mobility Server. As part of the installation and configuration of BEMS, you must configure BEMS for Push Notifications to support the BlackBerry Work app.
3	Configure your BlackBerry UEM environment to support BlackBerry Dynamics apps.
4	Make BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks available to users.
5	Configure BlackBerry Work app settings.
6	Configure BlackBerry Tasks and BlackBerry Notes app settings.
7	Configure BlackBerry Work connection settings.
8	Instruct users to activate BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks on their devices.

System requirements

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

Item	Requirement
Server requirements	• BlackBerry UEM • BlackBerry Enterprise Mobility Server
Devices	For device OS compatibility, see the Mobile/DesktopOS and Enterprise Applications Compatibility Matrix.
Skype for Business	If you plan to support Skype for Business for calendar and meeting features in BlackBerry Work, you require the following: • An on-premises Skype for Business 2015 Server and later • An on-premises Microsoft Exchange server supported by BlackBerry Work. See the Compatibility Matrix for Mobile/Desktop OS and Enterprise Applications for a list of supported Microsoft Exchange servers. • The Skype for Business client must be installed on devices for users to be able to join meetings from a calendar event It is also assumed that you have your Skype for Business environment configured and running.
Threat protection	Spoofed emails are not recognized by BlackBerry Work. It is recommended that you use Office 365 Advanced Threat Protection (ATP) or similar solutions to protect against malicious emails.

Configuring your BlackBerry UEM environment to support BlackBerry Dynamics apps

If you have not configured your BlackBerry UEM environment, you must complete configuration tasks before you can continue with the tasks in this guide. For complete steps on how to configure your BlackBerry UEM environment to support BlackBerry Dynamics apps, see Managing BlackBerry Dynamics apps.

Make BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks available to users

To manage BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks in BlackBerry UEM, you must add these apps to the app list. To add them to the app list in BlackBerry UEM, your organization must be entitled to use BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks in the BlackBerry Marketplace for Enterprise Software. After your organization is entitled to use the app, you can update the app list to synchronize the apps with BlackBerry UEM right away or wait until it synchronizes automatically. BlackBerry UEM synchronizes BlackBerry Dynamics apps every 24 hours. After the apps have been added to the app list, they can be assigned to users.

For a complete description of how to manage BlackBerry Dynamics apps in BlackBerry UEM, see Managing BlackBerry Dynamics apps.

1. Log in to your account at https://marketplace.blackberry.com/pce/#/apps.
2. Locate the app in the BlackBerry Marketplace for Enterprise Software and request a trial. The app will be made available to your organization and can be assigned to users after the app has been synchronized to BlackBerry UEM.
3. To purchase the app, follow the instructions provided by the app developer.

After you finish: To allow users to install and activate BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks on their devices, assign the apps to user accounts or user groups .

Managing BlackBerry Work

Configure BlackBerry Work app settings

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

If you enable auto discover in your environment, see Best practice: Enabling autodiscovery.

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 **Basic Configuration** tab, under **Exchange ActiveSync Settings** configure the following settings:
   a) In the **Default Domain** field, specify the default Windows NT Domain that BlackBerry Work will automatically attempt to connect to when users log in to BlackBerry Work. If your server uses the newer UPN (email@host.com) style login instead of the older (domain\user) style login, leave this field blank.
   b) In the **Active Sync Server** field, specify the default Exchange ActiveSync server that BlackBerry Work will attempt to connect to when users log in to BlackBerry Work (for example, cas.mydomain.com).
   c) In the **Autodiscover URL** field, specify the auto discover URL if known. This will speed up the auto discover setup process (for example, https://autodiscover.<*mydomain*>.com/autodiscover/autodiscover.xml).
   d) In the **Autodiscover Connection Timeout in Seconds (iOS only)** field, specify the auto discover connection timeout in seconds.
6. Optionally, configure any other settings. See BlackBerry Work app configuration settings for a description of all of the settings that you can configure.
7. Click **Save**.

BlackBerry Work app configuration settings

App Settings	Description
Autodiscover	If you select the "Enable automated Autodiscover" option, BlackBerry Work automatically discovers the Exchange ActiveSync server. **Note:** Due to possible security vulnerabilities, it is not recommended that you select this option.
Authorized Email Domains	Select the "Display warning while sending message if the number of unauthorized recipient email domain(s) is" option if you want to display a warning message to users that attempt to send a message to the number of unauthorized domains specified in the drop-down list. Select the "Display warning for received messages if the sender's email domain is unauthorized" option if you want to display a warning to users when they receive messages from senders that are not listed in the Authorized email domains list. If you select either of the options above, specify a list of authorized email domains. Use a comma separated list, with no spaces, to specify authorized email domains. You can edit the sample text displayed in the warning message field.

App Settings	Description
External Email Marking	If you select the "Prepend tag to subject on external mails" option, the subject lines of email messages sent outside of the user's domain are prepended with the text specified in the Text to prepend field.
Data Leakage Prevention Watermark	If you select the "Enable DLP Watermark" option, a watermark is added to all BlackBerry Dynamics app screens (for example, BlackBerry Work, BlackBerry Work Docs, Calendar, and Contacts). The watermark shows the user's username and current date and time. Note: If users print a file, the watermarks are not displayed in the output.
Screenshot Prevention (iOS Only)	If you select the "Prevent screenshots on iOS" option, users cannot take screenshots in the BlackBerry Work app. This setting is applied to devices the next time that a user closes and reopens the app.
Avatar Photos	If you select the "Enable avatar photos" option, contact photographs are displayed in BlackBerry Work. If this option is not selected, the user's initials are displayed instead of a photograph.
Presence Service	If you select the "Enable presence service" option, users can see the online status of their instant messaging contacts. Available settings: • Other Platforms: Select this option if your environment is configured to use Microsoft Lync, Cisco Jabber, or Skype for Business On-prem using trusted application mode. • Skype for Business On-Prem - Non-trusted Application Mode If this setting was enabled previously, the default setting is "Other platforms" and the drop-down shows "Select". For more information about setting up the BEMS-Presence service, refer to the Set up support for the BEMS-Presence in non-trusted application mode topic.
Email Search	If you select the "Enable searching emails on server" option, users can search email messages on the server.
Diagnostics	If you select the "Allow users to perform app diagnostics" option, users can perform app diagnostics from the BlackBerry Dynamics Launcher on their devices.
BlackBerry Gatekeeping Service	If you select the "Use BlackBerry Gatekeeping Service" option, unauthorized devices are prevented from using Exchange ActiveSync unless they are explicitly added to the allowed list using the BlackBerry Gatekeeping Service. To use the BlackBerry Gatekeeping Service, you must create a gatekeeping configuration for the Microsoft Exchange Server or Microsoft Office 365 and assign an email profile to users that has the automatic gatekeeping server selected. For details on how to configure the BlackBerry Gatekeeping Service, see Controlling which devices can access Exchange ActiveSync.

App Settings	Description
Genoa Transformer Service for Domino	If you select the "Use Genoa Transformer Service to connect to IBM Domino" option, meeting invitations are received on devices as meetings.ics files instead of invite.ics.
Disable Out of Office	If you select this option, you will turn off Out Of Office and disable the setting in the BlackBerry Work client.

Notifications	Description
Select level of detail in Email notification	Select the level of detail that users see in email notifications. Available settings: • No notifications: Users don't receive notifications when email messages are received. • No details in notification: Users see the default message notifications, "You have received a new message" and "You have received an invitation," in the email preview. • Sender only: Users see the sender's name in clear text with the default message notification in the email preview. • Sender and Message: Users see the sender's name and a preview of the email message. • Sender, Subject, and Preview: Users see the Sender name, Subject of the email message, and a preview of the email message. The default setting is "Sender and Subject."

Notifications	Description
Select level of detail in Calendar notifications	Select the level of detail that users see in calendar notifications. Available settings: • No notifications: Users don't receive notifications when calendar invitations are received. • No details in notification: Users see the default message notifications, "You have received a new message" and "You have received an invitation," in the email preview. • Meeting Time only: Users see the meeting time in clear text with the default message notification. • Meeting Time and Subject: Users see the meeting time and subject of the meeting in the email preview. • Meeting Time, Subject and Location: Users see the meeting time, subject, and location of the meeting in the email preview. • Meeting Time, Subject, Location, and Preview (Android only): Users see the meeting time, subject, location, and a preview of the meeting description in the email preview. The default setting is "Meeting Time, Subject, and Location." Select the "Show only generic notifications when app is locked (Android only)" option to show only generic information in notifications if the app is locked. Select the "Show notifications on connected wearable devices (Android Wear only) option to display notifications on wearable Android devices. Select the "Enable widgets for BlackBerry Work app" to allow users to add widgets to iOS and Android devices. By default, this setting is enabled. If the widget policy is blocked and then unblocked, users must remove and then add the widget again to unblock it.
Email subfolder notifications	Select the "Enable visual notifications for subscribed subfolders" option to allow users to receive email notifications for subfolders.
Additional options for notifications on Android Wear devices	Select whether there are additional notifications for Android Wear devices. Available settings: • Notification for VIP Contacts • Notification for anyone • Notification with voice reply for anyone When using a device outside of a controlled wireless network, wearables require higher communications security with respect to encryption, information integrity, and non-repudiation. Since wearable computers are quite small, most do not come equipped with higher security features and any data that is sent and received is vulnerable. Consequently, BlackBerry Work's support for wearables is confined to notifications and reminders.

Notifications	Description
iOS App Icon Badge	Select the "Allow user to choose between “Unread Mails” and "New Mails" as their default Badge count on the App Icon" option to allow users to choose between displaying a badge count for unread and new email messages as their default badge count on the app icon. If this option is not selected, the app icon badge reflects the number of new email messages that were received since the user last closed the app, and the user cannot select “Unread Mails” as a badge count preference.
High priority notifications (Android only)	Select the “Enable high priority notifications for regular incoming emails (Android only)” option to enable high-priority notifications for regular (non-VIP) incoming email messages. Messages will be delivered with an audible sound even when the device is in Sleep mode. If this option is enabled, a user cannot turn off this feature on their device. If this option is not enabled, a user can choose to turn on this feature on their device. This feature requires BEMS 3.7.

S/MIME	Description
Enhanced Security	Select the "Periodically require PIN entry to access SMIME capabilities" option if you want users to be required to periodically enter a PIN to use S/MIME. • Set the period after which a user must enter their PIN. • Set the minimum number of digits that a user must use for their PIN. If a user enters an incorrect PIN three times, they will be required to reset the PIN. To complete the reset, an unlock code or QR code must be sent to the user. For more information, see Send a BlackBerry Dynamics app unlock key and QR code to a user.
Sending	In the "Default signing algorithm" drop-down list, select the algorithm to use for signing sent messages. In the "Default encryption algorithm" drop-down list, select the encryption algorithm to use. Select the "Require all emails to be signed" and "Require all emails to be encrypted" if you require that emails must be signed and/or encrypted. Select the "Perform name checking for outgoing encrypted emails (verify email address in certificate matches recipient email address)" option to perform name checking. Name checking verifies that the email address in the certificate matches recipient's account.

S/MIME	Description
Receiving	In the "Automatically download the body of S/MIME emails" drop-down list, select how the body of S/MIME email messages is downloaded. Wi-Fi is supported on Android devices only. If you select this option, iOS devices are set to "Never." Select the "Perform name checking (verify email address in certificate matches user's account)" option to perform name checking. Name checking verifies that the email address in the certificate matches user's account.
Opening	Select the "Enable certificate check before opening old S/MIME email" option if you want BlackBerry Work to check if the certificate used to encrypt an email message is still available for the user. Select "Block access to signed messages when no certificate is available" if you want BlackBerry Work to block access if no certificate is available.
Certificate Management	Specify when to clear the public certificate cache. By default, this setting is Weekly.
Revocation Checking when the OCSP server is available	Select the "Enable revocation checking" option to enable revocation checks and specify the depth of certificate checking. Available settings: • Check entire certificate chain • Check user / client certificate only Select the "Use AIA extension in certificate if present" option to use the AIA extension in certificates if present. In the "Default OCSP URL" field, specify the default OCSP URL to use if the AIA extension cannot be used or it is not present in a certificate.

Address Book	Description
Address Book Sync	Select the "Allow syncing BlackBerry Contacts to device" option to enable synchronizing contacts to devices and choose the fields that are synchronized. In the "Maximum length for notes" field, specify the maximum length for the notes field. By default, the maximum is 1024 characters. Select the "Even if iCloud is enabled, allow syncing BlackBerry Contacts to device" option to allow synchronization to occur when iCloud is enabled. To turn on 'Enable contact sync to native' to take advantage of this feature on a device, see Change contact settings for BlackBerry Work for Android or in Change BlackBerry Work for iOS settings, see the "Manage your your Contacts settings" section.

Address Book	Description
Caller ID	Select the "Allow device to use BlackBerry Contacts for Caller ID" option if you want to allow BlackBerry Work to access the user's BlackBerry Work contact list to display contact name for incoming and outgoing phone calls.
GAL Search	Specify the maximum number of results to display when searching the global address list (GAL).
Recipients	Specify whether caching is enabled. When caching is enabled, the cache is used to offer autocomplete suggestions for recipients during email composition.

Interoperability	Description
Camera and Device Photo Gallery permissions	Specify whether to allow access to the device camera, the photo gallery, or both. Available settings: • Allow access to camera and device photo gallery • Allow access to camera only • No access to camera or device photo gallery The default value is "Allow access to camera and device photo gallery."
Voice	Select the "Tap a phone number to dial using native phone" option to allow users to use the native phone app on a device or select the "Tap a phone number to dial using entitled and installed GD VOIP apps" option to allow VOIP apps.
SMS	Select the "Tap SMS icon to initiate SMS using native SMS apps" option to specify whether to allow users to initiate their native SMS apps by tapping the SMS icon or select the "Tap SMS icon to initiate SMS using entitled and installed GD SMS apps" option to specify that users must use BlackBerry Dynamics SMS apps.
Misc	Specify whether to allow access to the user's native browser or native maps app.
Launch 3rd Party App	Select the "Enable integration with 3rd party RSA SecurID app using CTF token seed" to enable two-factor authentication integration with a third-party RSA SecurID app using a CTF token seed. Select the "Enable launching to 3rd party native apps (iOS only policy)" option to enable launching third-party native apps. When you enable native apps, enter the App URL scheme in the field. **Note:** BlackBerry Work supports CTF-based provisioning using a nativeRSA SecurID app. For more information about configuring RSA soft-token authentication, see the BlackBerry Access Administration Guide.

Interoperability	Description
Launch 3rd Party App Universal link (iOS only)	Universal links allow iOS users to be automatically redirected to an installed app without going through Safari when they click links in a website. If the app isn't installed on the device, the link opens the website in Safari. You can specify a list of universal links that users can open from BlackBerry Work for iOS. If you add a universal link to this list, the link will redirect to the appropriate app if it is installed on a user's device. If a user clicks on a universal link that is not added to this list, the link will not be redirected to an app and will open in Safari, even if the app is installed on a user's device. To add multiple URLs, insert a carriage return between each URL that you want to add.
Allow 3rd Party App to Send Mail	Select the "Enable sending mail from BlackBerry Work via mailto:/ gmmmailto:/gwmailto:" option to specify whether email messages can be sent using mailto:/gmmmailto:/gwmailto
File Transfer Privileges	Select the "Enable exporting to 3rd-party native apps" option to specify whether to allow the transfer of files to third-party native apps on the user's device. You can allow and disallow specific apps by app ID and app share extensions. If your environment includes iOS devices that run iOS 14 or later, add both the app ID and app share extension for a specific app to make sure that BlackBerry Work for iOS contains the necessary information to compare the app against the blacklists or whitelists configured in BlackBerry UEM. If the necessary information is not included, users running iOS 14 and later might be unable to transfer a file and receive an error message. For more information, visit support.blackberry.com/community to read article 69436. Select the "Enable Importing from 3rd-party native apps (iOS 12 and below and Android)" option or the "Enable Importing from 3rd-party native apps (iOS 13 and above only)" option to allow the import of files from third-party native apps on the user's device. You can allow and disallow specific apps by app ID and app share extensions. Note that exceptions to importing apply only to iOS. The combined size of the imported files cannot exceed 120 MB.

Docs and Attachments	Description
Docs Repository	Specify whether to enable a file repository on the device, local or server docs repositories, and Box, and whether to force users to save pending uploads. **Note:** Note: By default users are alerted about any pending uploads every 24 hours. If Forced Pending Uploads Policy is selected, users are blocked from taking any document related actions in BlackBerry Work until all files are successfully uploaded to the server.

Docs and Attachments	Description
Sending Attachments	Specify whether to allow outgoing attachments and specify the maximum size and the file extensions that are allowed or disallowed.
Receiving/Opening Attachments	Specify whether to allow incoming attachments and specify a maximum size and the file extensions that are allowed or disallowed.

Classification	Description
Email classification	Specify whether to enable email classification markings, such as INTERNAL, CONFIDENTIAL, NO FORWARD, and/or NO REPLY. To edit the XML classes, select and delete the code that you want to remove. For more information on classifications, including an example, see Email classifications . After you have enabled email classifications, you can select the "Require all emails to have Email Classification" option to force all email messages to include a classification setting.
Event classification	Specify whether to enable event classifications markings such as INTERNAL, CONFIDENTIAL, NO FORWARD, and/or NO REPLY. After you have enabled event classifications, you can select the "Require all events to have Event Classification" option to force all events to include a classification setting. Note that the classifications for calendar events are applicable only when email classifications are enabled.

Calendar	Description
Time Zone Info	If you select the "Disable display of time zone information in meeting and contact card" option, BlackBerry Work will not retrieve the time zone information from Microsoft Exchange that is displayed in the calendar and contacts for users.
Conference links	Select one or more of the conference platform options to enable users to click a Join button in a meeting request to quickly join a meeting on their device using the associated platform, such as Zoom.
External Calendars Preview	Select the “External Calendars Preview” option to display a preview of external calendar events in the day view. You can choose from two levels of data presentation: **Placeholders only** displays solid vertical placeholders with no event data **Details** displays external calendar events as standard event blocks with an event title and the recurrence status icon.
Calendar Event New Time Proposal	Select this option to allow users to use the propose new meeting time feature.

Basic Configuration	Description
Security Settings	Select the "Use Kerberos Constrained Delegation in place of login/password" option to specify whether Kerberos Constrained Delegation will be used for logging in to Microsoft Exchange. If this option is not selected, NTLM/Basic authentication will be used. Select the "Use client certificate in place of login/password" option to specify whether clients must have individual login certificates (SSL) uploaded to the BlackBerry UEM management console. These certificates are used for login instead of basic credentials (username/password).
Enterprise Server Settings	In the Server List Reshuffle Period (minutes) field, specify the frequency that the server list, if present, is reshuffled for load balancing purposes. In the Server List Quarantine Period (minutes) field, specify how long BlackBerry Work waits before retrying if BlackBerry UEM is not working.
Client Settings	In the Sync Email Body Size (Kb) field, specify the size, in KB, of the partial message body downloaded from the server if the user selects the option to download partial message content. Select the "Use BEMS to perform AutoDiscover of the EAS/EWS endpoint for the user" option to specify that the client will use the BlackBerry Server Autodiscover service to determine the EAS/EWS endpoint for the user. Select the "Create and consume rights-managed email messages option" to specify that Information Rights Managements (IRM) must be enabled for user mailboxes on Microsoft Exchange.
Other Settings	In the Send Feedback Email Address field, specify the email address where client feedback email messages are sent. Add multiple comma delimited recipients as needed. In the Report Phishing Email Address field, specify whether users can report emails as phishing. The reported emails are forwarded to the email address provided in this field then moved to Trash folder.
Account Setup	When the "Skip Email Short Form Setup" option is selected, users must input their Microsoft Active Directory usernames, passwords, and domains during device activation.
ActiveSync and Auto Discover Authentication Methods (iOS Only)	Specify the authentication methods to use. If only certain authentication methods are supported from Microsoft Exchange, set those values to minimize the user setup time. (For example, if Auto Discover and ActiveSync IIS Auth Settings are set to allow only NTLM and Basic, then de-select Negotiate in above app setting.) If none are selected, the default Microsoft Exchange setting is used. If using client-based authentication, check none of the options.

Basic Configuration	Description
Exchange Web Services Authentication Methods (iOS Only)	Specify the authentication methods to use. If only certain authentication methods are supported from Microsoft Exchange, set those values to minimize the user setup time. (For example, if EWS IIS Auth Setting is set to allow only NTLM, then select only NTLM above for an optimal setup experience.) If none are selected above, the default Microsoft Exchange setting is used. If using client-based authentication, check none of the options.
Exchange Web Services Settings	Specify the Microsoft Exchange Web Services URL endpoint (for example, https://mydomain.com/EWS/Exchange.asmx). If you select the "Disable Exchange Web Services" option, all Microsoft Exchange Web Services activities, including calendar forward and calendar attachment, are disabled.
Exchange ActiveSync Settings	In the Default Domain field, specify the Windows NT Domain to try automatically when logging in. If your server uses newer UPN (email@host.com) style login instead of the older (domain\user) style login, this field should be left blank. In the ActiveSync Server field, specify the default Microsoft Exchange Server to connect to (for example, cas.mydomain.com). In the Autodiscover URL field, specify the auto discover URL if known. This speeds up the auto discover setup process (for example, https://autodiscover.<*mydomain*>.com/autodiscover/autodiscover.xml). In the Autodiscover Connection Timeout in Seconds (iOS only) field, specify the timeout setting for iOS devices.
Enforce App Configuration	Select the "Enforce App Configuration" option to ensure that modern authentication, EAS/EWS endpoints, and Microsoft Office 365 settings configured in the BlackBerry Dynamics connectivity profile are applied. This option is useful when you are troubleshooting issues after you have migrated a BlackBerry Work mailbox from an on-premises Microsoft Exchange Server to Microsoft Office 365. **Note:** BlackBerry recommends that you copy your organization's app configuration, select the Enforce App Configuration option, and apply the app configuration only to the affected users.
Advanced Settings	Specify additional configuration parameters in this text area. Contact BlackBerry Support for more details.

Advanced Configuration	Description
UPN Settings	In the "UPN type" drop-down list, select "Explicit UPN" to override the default UPN setting in the Dynamics Global properties.

Advanced Configuration	Description
ActiveSync User Name Formats (iOS Only)	Select the username formats that can be used to authenticate with your Exchange ActiveSync server. Available settings: • UPN • Domain\UserId • SMTP To simplify user setup time, select only the username formats that are supported by your Exchange ActiveSync server. If you do not select an option, all options are allowed.
Exchange Web Services User Name Formats (iOS Only)	Select the username formats that can be used to authenticate with Microsoft Exchange Web Services. Available settings: • UPN • Domain\UserId • SMTP To simplify user setup, select only the username formats that are supported by Microsoft Exchange Web Services. If you do not select an option, all options are allowed.
TLS Certificate Settings	Specify the user credential profile that contains the TLS certificate to be used to connect to Microsoft Exchange. The name of the profile that you specify here must match the name of the user credential profile that was created in the BlackBerry UEM management console. For more information on user credential profiles, see Using user credential profiles to send certificates to devices.
Email Sync Window	In the "Maximum Email Sync Window Allowed" drop-down list, specify the number of days in the past to synchronize email messages to devices. If the setting on a device allows for more days than the server setting, the server setting is used and email messages that are older than the server setting are removed from the device. If the setting on the device allows fewer days than the server setting, the setting on the device remains the same. The user can change the setting on the device to fewer days than the server setting.
Draft Folder Syncing	Prevent a user from deselecting the Drafts folder which keeps it from being automatically synchronized.
Background Authorization	Select a time to allow the BlackBerry Work app to synchronize email in the background periodically. Decreasing the duration between the time that email synchronizes ensures that the user's inbox is up to date when they open the app.

Advanced Configuration	Description
Shared Mailboxes	Select the "Enable access to Shared Mailboxes" option if you want to allow users to add a user mailbox that they are a delegate for, or a shared mailbox that they have been granted access to, in BlackBerry Work. If this option is disabled after shared mailboxes have been added, existing shared mailboxes are removed, and they are not restored if the setting is enabled again. Also, if a user attempts to add a shared mailbox when this option is disabled, they will not be able to add the mailbox and will see a message in the BlackBerry Work app stating that they must contact their administrator. **Note:** For users to be able to receive notifications for user mailboxes that have been delegated, BEMS 2.10 or later is required. For users to be able to receive notifications from their shared mailboxes, BEMS 2.12 or later is required.
Shared Calendar Periodic Sync	Select the "Enable Calendar Periodic Syncing " option to allow a shared calendar to be refreshed every 10 minutes while it is onscreen in the foreground. This feature applies to all views: Agenda, Day, Week, and Month.
Mailbox Migration	Select the "Migration Flow Enabled" option when you are planning to migrate a BlackBerry Work mailbox from an on-premises Microsoft Exchange Server to Office 365. 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.

Advanced Configuration	Description
Office 365 Settings	Select the "Use Office 365 Settings" option to configure options for Microsoft Office 365. If selected, specify the following: • 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. • In the Entra App ID field, specify the Microsoft Entra ID app ID for BlackBerry Work. For information on how obtain an Entra ID, see Obtain an Entra app ID for BlackBerry Work. • 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 the "Office 365 Tenant ID" field, specify the tenant ID of Office 365 server that you want BlackBerry Work to connect to during setup. **Note:** The default value "common" will only work when your Entra app is configured for multitenant. • 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 Entra ID portal. • In the "Exchange User Name Format" section, select UPN to use a UPN user name format instead of SMTP when authenticating with Microsoft Exchange Online. Depending on your environment, if your users are configured with UPNs that are different from their email address, you might need to enable "Use explicit UPN" property. This requires BlackBerry UEM 12.11 or later. For more information, see the BlackBerry UEM Configuration content. To enable the UPN feature for BlackBerry Work Docs, this feature requires BlackBerry Work 2.21 or later. • Select the "Use Office 365 Modern Authentication for Presence" option to use modern authentication with the Presence service. The "Enable presence service" option must also be selected. • In the "Office 365 Presence Resource" field, enter the app ID for your Presence service. • 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 • In the "Modern Authentication" section, specify the UPN configuration that will be used to obtain a modern authentication token.
Upgrade Exchange ActiveSync Protocol	Select the "Upgrade to latest supported Exchange Active Sync protocol" setting to enable BlackBerry Work clients to check and upgrade to the latest supported Exchange Active Sync Protocol, if required.

Performance Reporting	Description
Enable Performance Reporting	Select this option, to specify whether to monitor performance of the BlackBerry Work app.
HTTP Connection Error	Select the "Enable reporting of HTTP connection errors" options to specify whether to report HTTP connection errors between BlackBerry Work and the specified application servers.
HTTP Response Time	Select the "Report HTTP responses taking long time" option to specify whether to report HTTP responses that are taking longer than the specified time. Enter the application server addresses to monitor.
HTTP Status Code	Select the "Report HTTP status codes received" option to specify whether to report a specified HTTP status code. Enter the application server addresses to monitor
Don't send reports for duration (in seconds)	Specify the amount of time to wait before sending another report.

Beta Features	Description
Genoa Transformer Service	Select the "Use Genoa Transformer Service to connect to Google Suite (BETA)" option to allow interoperability between Google Suite and BlackBerry Work.
Active Directory Password Expiration Warning	Select the number of days to display a warning to the user before their Microsoft Active Directory password expires, and select a Password Expiration Data Provider (EWS or LDAP). In the Custom Message field, you can add additional information to display to the user. **Note:** You can use this feature for users that are using both, the GPO (Global Policy Object) method and PSO (Password Settings Object) method to set the maximum password age.
Office 365 Brokered Authentication	Select the "Use Office 365 Brokered Authentication" to require users to use brokered authentication to authenticate to BlackBerry Work and access BlackBerry Work Docs repository content (for example, Microsoft SharePoint Online) to ensure that settings configured in Entra ID Conditional Access are applied. To use this feature, • Your environment must be enabled for Entra ID conditional access. For more information, see Configure Entra ID conditional access in the BlackBerry UEM Configuration content. • The "Office 365 Settings" (Advanced tab) must be enabled and configured for modern authentication. • Users must have the Microsoft Authenticator app installed. By default, this setting is disabled.

Beta Features	Description
Sending Emails From Aliases	Select the "Enable sending from aliases" option to allow users to send email messages from email accounts that have aliases.
Contact Sharing	Select the "Enabled support for shared contact folders" option to allow delegates of a Microsoft Exchange user's mailbox to access all shared contacts.
Microsoft Teams	Select the "Allow users to add a Microsoft Teams meeting when creating a calendar event" option to allow users to create Microsoft Teams meetings. This feature works with Office 365 and requires modern authentication to be configured. Select the "Allow Microsoft Teams calls/chat from contact" option to allow Microsoft Teams calls and chats to launch from BlackBerry Work Contacts. In the "Specify additional domains that support Microsoft Teams call/chat" field, enter additional email domains that support Microsoft Teams in a comma separated list.
Handling External Images	Select the "Don't allow to download external images" option to block downloading images from external sources.

Deprecated tab	Description
Skype for Business	If you are currently using Skype for Business 2015 or later in your environment, you can allow users to add meetings and join meetings directly from their calendars. Select the "Allow to create Skype For Business meetings in calendar" option to allow users to add Skype for Business meetings to their calendars. Select the "Allow launching into Skype for Business app on mobile" option to allow users to make voice and video calls and to be able to join Skype for Business meetings directly from a calendar invitation. The meeting is automatically opened in the Skype for Business client and users must have the Skype for Business client installed on their devices. In the **Domain of Skype for Business meeting link** field, enter the fully qualified domain name or the domain-only portion of the Skype for Business meeting server to allow internal users to use the Join meeting button in the event details. For example, meet.example.com or example.com. By entering this domain name, BlackBerry Work can locate which meeting link to capture from the meeting invitation if it is different from the user's email address domain.
Opening S/MIME (iOS only)	Select the "Disable email decryption with legacy certificates" option to disable using legacy certificates when decrypting email messages. This option cannot be selected if the “Enable certificate check before opening old SMIME email” option is also selected.

Deprecated tab	Description
Use heritage settings	Select the "Devices should use values described below for Presence and Docs servers". Selecting this option requires that the following configurations are completed: • BlackBerry Work is added to the BlackBerry Dynamics Connectivity Profile App Servers section. For more information, visit support.blackberry.com/community to read article 47950. • Specifying the preferred Presence Server configuration • Specifying preferred Docs Server configuration
Preferred Presence Server Configuration	Type the FQDN of the computers that host the BEMS-Presence service. If you have multiple servers, separate the names using commas, not spaces (for example, domain01.example.com:8443,domain02.example.com:8443).
Preferred Docs Server Configuration	Type the FQDN of the computers that host the BEMS-Docs service. If you have multiple servers, separate the names using commas, not spaces (for example, domain01.example.com:8443,domain02.example.com:8443).
Microsoft Authentication Library	Disabling this policy will result in using legacy Microsoft Entra ID Active Directory Authentication Library when logging into Work mailbox account. (iOS Only)
Legacy proxy Office 365 Modern Authentication	Select the "Use legacy Proxy Office 365 Modern Authentication requests" option to use legacy proxy requests through the BlackBerry Dynamics Proxy server. (Android only)
Security Settings	Select the "Disable SSL Certificate Checking" option to disable SSL Certificate verification for Exchange ActiveSync/Microsoft Exchange Web Services in test environments.
Apple Watch app	Select the "Enable BlackBerry Work app on Apple Watch" option to communicate between the device and the Apple Watch **Note:** This feature doesn't use the BlackBerry Dynamics Secure Container to secure the storage or communication between the device and Apple Watch

Obtain an Entra 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 Entra app ID for BlackBerry Work. If you need to obtain multiple Entra app IDs (for example, BEMS-Mail and BEMS-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 **Microsoft Entra ID**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for the BlackBerry Work app. This is the name that users will see.

6. Select a supported account type. Although Multitenant is supported, in most cases this should be Single tenant.
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. Optionally, if you are enabling Entra ID conditional access, perform the following actions:
   - Click on the **Redirect URIs** link (i.e. '0 web, 0 spa, 1 public client').
   - For iOS devices, under the existing **Mobile and desktop applications** section, click **Add URI**, and enter:

     ```
     x-msauth-work://com.good.gcs.g3
     ```
   - For Android devices:
     a. Click **Add a platform > Android**.
     b. In the **Package name** field, enter:

     ```
     com.good.gcs
     ```
     c. In the **Signature hash** field, enter:

     ```
     zRsXTl1cL/Seb6GumLzvoecPA8w=
     ```
10. In the **Manage** section, click **API permissions**.
11. Click **Add a permission**.
12. In the **Select an API** section, click the **Microsoft APIs** tab.
13. Complete one or more of the following tasks:

Environment	Permissions
If your environment is configured to use Microsoft Office 365	a. Click **Microsoft Graph**. If Microsoft Graph is not listed, add Microsoft Graph. b. In delegated permissions, select the following permissions: • **Sign in and read user profile** checkbox (**User > User.Read**) • **Send mail as a user** checkbox (**Mail > Mail.Send**) • **Access mailboxes as the signed-in user via Exchange Web Services** checkbox (**EWS > EWS.AccessAsUser.All**). • **Have full access to user calendars** checkbox (**Calendars > Calendars.ReadWrite**) c. Click one of the following: • If Microsoft Graph existed in the API permissions, click **Update permissions**. • If you needed to add Microsoft Graph, click **Create**. d. Click **Add permissions**.

Environment	Permissions
If your environment is configured to use Microsoft SharePoint Online or Entra-IP to enable modern authentication for the BlackBerry Work client	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-Docs component service. For example, AzureAppIDforBEMS. c. Select all delegated permissions. 1. Click **Delegated permissions**. 2. Click **expand all**. Make sure that all options are selected. d. Click **Add permissions**.

14. 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.
15. Click **Yes**.
16. 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. You use the Application ID in the app configuration settings for BlackBerry Work. For more information about the app configuration, see BlackBerry Work app configuration settings.

Configure BlackBerry Work connection settings

When you configure your environment for BlackBerry Work, you must add the necessary Exchange ActiveSync servers and BlackBerry Enterprise Mobility Server instances to the connectivity profiles that you have assigned to users that will install BlackBerry Work

You can use one of the following two methods to specify the BEMS instances for use by BlackBerry Work:

- Disable the **Use heritage settings** in the BlackBerry Work App Config. This is the preferred method. When you disable this setting, you must add the following entitlements to the BlackBerry Dynamics Connectivity profile:
  - BlackBerry Core and Mail Services (com.blackberry.gdservice-entitlement.coreandmail)
  - BlackBerry Presence Service (com.blackberry.gdservice-entitlement.presence)

  You would use this configuration if you have a larger environment that has several BEMS instances running different BEMS services (for example, one computer running one service).
- Enable the **Use heritage settings** option in the BlackBerry Work App Config. When you enable this setting, BlackBerry Work app searches for entries in the App Servers section of the BlackBerry Dynamics Connectivity profile. You might use this configuration if you have a smaller environment that is configured with all or most of the BEMS services installed on a single BEMS instance (for example, BEMS-Core, BEMS-Mail, and BEMS-Presence are installed on one computer, BEMS-Docs is installed on a separate computer, and the BEMS-Connect service is installed on another computer.

For more information about the heritage settings see, BlackBerry Work app configuration settings.

1. On the menu bar, click **Policies and Profiles** > **Networks and Connections**.
2. Click + beside **BlackBerry Dynamics Connectivity profile** to create a new connectivity profile or click on the Default connectivity profile to edit it.
3. Type a name and description for the profile.
4. In the **Additional servers** section, click +.
5. In the **Server** field, specify the FQDN of the Exchange ActiveSync server.
6. In the **Port** field, specify the port for the Exchange ActiveSync server. By default, the port number is 443.

7. Select a **Route Type**.
   - BlackBerry Proxy cluster: Select this option to specify the BlackBerry Proxy clusters that must be used to reach the domain
   - Direct: Select this option to route traffic from the app to the server without going through BlackBerry Proxy.
   - Deny: Select this option to block the app from connecting to the server.
8. In the **Primary** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the primary cluster.
9. In the **Secondary** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster
10. Click **Save**.
11. In the **App servers** section, click **Add** and complete one or more of the following tasks:

Configuration	Tasks
If **Use heritage settings** is enabled in the BlackBerry Work App Config	**a.** Search for and select BlackBerry Work. **b.** Click **Save**. For more information about the Use heritage settings option, see BlackBerry Work app configuration settings.
If **Use heritage settings** is disabled in the BlackBerry Work App Config	**a.** Search for and select **BlackBerry Core and Mail Services** (com.blackberry.gdservice-entitlement.coreandmail). Click **Save**. **b.** If you installed the BEMS-Presence service, search for and select **BlackBerry Presence Service** (com.blackberry.gdservice-entitlement.presence). Click **Save**.
If the BEMS-Docs service is installed in your environment	**a.** Search for and select **Feature - Docs Service Entitlement** (com.good.feature.share). **b.** Click **Save**.

12. In the table for the app, click +.
13. In the **Server** field, specify the FQDN of the BlackBerry Enterprise Mobility Server.
14. In the **Port** field, specify the port of the BlackBerry Proxy cluster that is used to access the BlackBerry Enterprise Mobility Server. By default, the port number is 8443.
15. In the **Priority** drop-down list, specify the priority for the BlackBerry Enterprise Mobility Server instance that BlackBerry Work will use.
16. Select a **Route type**. If the BlackBerry Enterprise Mobility Server server is on-premises, select **BlackBerry Proxy cluster**. If you are using UEM Cloud with BEMS Cloud, select **Direct**.
17. In the **Primary** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the primary cluster.
18. In the **Secondary** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
19. Click **Save**.
20. Click **Add** or **Save**.

After you finish: Assign the entitlement apps that you added in step 8 above to users or user groups. You can use one or more of the following options. For instructions, see the see the BlackBerry UEM Administration content.

- Assign 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 by completing one of the following tasks:
    - Assign the app group to a user group
    - Assign the app group to a user account

Configuring Kerberos for BlackBerry Work

You can configure Kerberos Constrained Delegation (KCD) or Kerberos PKINIT for the BlackBerry Work app.

- When you configure KCD, you allow users to provision the BlackBerry Work app without requiring users to enter their network credentials.
- When you configure Kerberos PKINIT, you allow a trust directly between the BlackBerry Work app and Windows KCD. Users authenticate using certificates issued by Microsoft Active Directory Certificate Services.

Allow BlackBerry Work to synchronize with your mail server when BlackBerry Work is in the background

You can allow BlackBerry Work to synchronize email messages with your mail server when BlackBerry Work is in the background. The user does not have to enter their password to initiate the synchronization. BlackBerry Work is notified in the background when new email messages arrive, is unlocked in the background, and then synchronized with your mail server. When the user opens BlackBerry Work in the foreground, the user must enter their password but they do not have to wait for BlackBerry Work to synchronize and populate the latest data.

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 the app configuration that you want to update or click + to add a new one.
4. On the **Advanced Configuration** tab, under **Background Authorization**, select how long you want to allow BlackBerry Work to be able to synchronize with your mail server in the background before you require the user to bring BlackBerry Work to the foreground and enter their password.
5. Click **Save**.

Steps to configure email notifications for BlackBerry Work

To configure email notifications, you perform the following actions:

Step	Action
1	Configure email notifications for BlackBerry Work.
2	In a new BEMS Cloud environment, Enable Microsoft Graph API to allow BEMS Cloud to communicate with Microsoft Office 365.

Step	Action
3	One of the following: • Associate a certificate with the Entra app ID for BEMS • Create a trusted connection between BEMS Cloud and Microsoft Exchange Server
4	Optionally, if your environment uses LDAP and has configured Active Directory users and user groups that use PSO method to set the maximum password age, see Configure the password expiration warning message.

Configure email notifications for BlackBerry Work

BEMS Cloud accepts push registration requests from devices, such as iOS and Android, and then communicates with the on-premises Microsoft Exchange Server or Microsoft Office 365 server to check the user's mailbox for changes. When you specify the on-premises Microsoft Exchange Server or Microsoft Office 365 server information, you specify the settings to create the BEMS Cloud tenant for your organization.

When the tenant is created, the following services are automatically enabled:

- BlackBerry Directory Lookup: This service allows users to look up other users by first name, last name, and associated photo or avatar from the company directory.
- BlackBerry Follow-Me: This feature supports the BlackBerry Dynamics Launcher on BlackBerry Work.

A hybrid modern authentication environment (for example, on-premises Microsoft Exchange Server and Microsoft Office 365), 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, see How to configure Exchange Server on-premises to use Hybrid Modern Authentication.

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

- Verify that the service account has application impersonation permissions applied.
- 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, see How to configure Exchange Server on-premises to use Hybrid Modern Authentication. If the Microsoft Exchange Server is not configured appropriately, users won't receive email notifications.
- In a Microsoft Office 365 environment, if you plan to enable modern authentication, verify that you completed the following:
  - If you enable modern authentication using credential authentication, obtain the client application ID.
  - If you enable modern authentication using client-certificate authentication, do one of the following:
    - Obtain the client application ID with certificate-based authentication
    - Create and associate a self-signed .pfx certificate to the Azure app ID for BEMS
  - If you have configured Entra ID conditional access for your organization, make sure that the BlackBerry Connectivity Node is installed and configured in your environment.
  - Configure email notifications for BlackBerry Work
  - In an on-premises Microsoft Exchange environment, make sure that the Microsoft Exchange Server is updated to support TLS 1.2 or push notifications will fail. Weaker cipher suites such as TLSv1 or TLS 1.0 are disabled by default. Disabling the cipher suites provides enhanced security.
- If you use Passive Authentication, verify that you have the App ID for BEMS using credential authentication.
- If you use SSL for SCP lookup, verify that you exported the Microsoft Active Directory SSL certificate.

1. In the management console, click **Settings > BlackBerry Dynamics > Email notifications**.

2. In the **Authentication type** section, select an authentication type based on your environment and complete the associated tasks to allow BEMS to communicate with the Microsoft Exchange Server or Microsoft Office 365:

Authentication type	Description	Steps
Credential	This option uses a defined BEMS username and password to authenticate to the Microsoft Exchange Server or Microsoft Office 365 using Basic Authentication.	**a.** In the **Service account username** field, enter the username of the BEMS service account. • For Microsoft Office 365, enter the service account's User Principal Name (UPN). • For on-premises Microsoft Exchange Server, use the format <*domain*>\<*username*>. **b.** In the **Service account password** field, enter the password for the service account.
Client Certificate	This option uses a client certificate to allow the BEMS service account to authenticate to the Microsoft Exchange Server or Microsoft Office 365.	**a.** Beside the **Certificate file (.pfx)** field, click **Browse**. Navigate to and select the client certificate file. **b.** In the **Password** field, enter the password for the client certificate.

Authentication type	Description	Steps
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*.	**a.** In the **Authentication Authority** field, enter the Authentication Server URL that BEMS accesses and retrieves the OAuth token for authentication with Microsoft Office 365 (for example, https://login.microsoftonline.com/common). **b.** In the **Client Application ID** field, enter the Entra app ID for the credential authentication. For instructions, see Obtain an Entra app ID for BEMS with credential or passive authentication . **c.** In the **Server Name** field, enter the FQDN of the Microsoft Office 365 server. By default, the the server name is https://outlook.office365.com. **d.** The **Redirect URI** field displays the URL that the IDP redirects the administrator to when the client app ID is authorized and the authentication tokens are provided. This field is prepopulated with the partition information and can't be modified. **e.** Click **Login**. **f.** Enter the credentials for the service account. **g.** Click **OK** to acknowledge that the authentication tokens were obtained. **h.** Important: BEMS Cloud doesn't automatically refresh the OAuth tokens. Repeat steps e to g 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.

3. If you connect to a Microsoft Office 365 environment, do the following to enable modern authentication:
   a) Select the **Enable Modern Authentication** check box.
   b) In the **Authentication authority** field, enter the Authentication Server URL that BEMS accesses to retrieve the OAuth token for authentication with Microsoft Office 365 (for example, https://login.microsoftonline.com/*tenantname* or https://login.microsoftonline.com/*tenantid*).
   c) In the **Client application ID** field, enter one of the following Entra app IDs depending on the authentication type you selected. Do one of the following to obtain an Entra app ID:
      - Obtain an Entra app ID for BEMS with credential or passive authentication
      - Obtain the client application ID with certificate-based authentication
   d) In the **Server name** field, enter the FQDN of the Microsoft Office 365 server (for example, https://outlook.office365.com).
   e) Optionally, select the **Use credentials if modern authentication fails** check box to allow BEMS to communicate with Microsoft Office 365 in the event that BEMS can't access the modern authentication source. When you select this check box, you must provide the BEMS service account credentials.

   Note: When you configure modern authentication, all nodes use the specified configuration.
4. In the **Service account username** field, enter the username that is used to log in to the Microsoft Exchange Server or Microsoft Office 365 server. The username must be in one of the following formats:
   - If your environment uses an on-premises Microsoft Exchange Server, use <*Domain*>\<*Username*> or UPN.

- If your environment uses Microsoft Office 365, use <*username*>@<*domain*>.com.

5. In the **Service account password** field, enter the password for the service account username you provided.
6. Optionally, in the **Autodiscover URL override** field, enter the Autodiscover URL to allow BEMS to obtain user information from the Microsoft Exchange Server or Microsoft Office 365 server when it discovers users for BlackBerry Push Notifications.

   Note: If you don't enter a URL, BEMS uses Autodiscover to locate the Microsoft Exchange Server or Microsoft Office 365 server to obtain user information.
7. Select the **Allow HTTP redirection and DNS SRV record** check box to allow HTTP Redirection and DNS SRV lookups for retrieving the Autodiscover URL when discovering users for BlackBerry Push Notifications. By default, this feature is enabled.
8. Select the **Use BlackBerry Connectivity Node route** to allow BEMS Cloud to connect to the Microsoft Exchange Server or Microsoft Office 365 using the corporate network rather than using a direct connection from the BlackBerry BEMS Cloud infrastructure. This setting requires that the BlackBerry Connectivity Node is installed and configured in your environment. If your environment uses Entra ID conditional access, make sure that this option is selected.
9. If your environment uses an internal URL to access and communicate with an on-premises Microsoft Exchange Server, select the **Use internal Exchange Web Services URL** check box. This setting requires that the "Use BlackBerry Connectivity Node route" setting is enabled. This option is not available if modern authentication is enabled.
10. Optionally, select the **Enable SCP Lookup** check box to query Microsoft Active Directory using LDAP and locate Autodiscover endpoint URLs. This setting is valid only if the "Credential" authentication is selected and that a BlackBerry Connectivity Node is installed and configured in your environment. This option is not available when the "Autodiscover URL override" is specified.
11. Select the **Enable SSL for SCP** check box. This allows BEMS to communicate with the Microsoft Active Directory using SSL. This setting requires that the "Enable SCP Lookup" is selected. If you enable this feature, you must add the Microsoft Active Directory SSL certificate to the BEMS Cloud database. For information on how to add the certificate, see Create a trusted connection between BEMS Cloud and Microsoft Exchange Server.
12. If you enabled **Enable SCP Lookup** or **Enable SCP Lookup** and **Enable SSL for SCP**, specify the **Domain Controllers for SCP** to configure LDAP over SCP. If you have multiple domain controllers, separate the domain controllers using commas (for example, domaincontroller1.example.com,domaincontroller2.example.com, and so forth).
13. Optionally, in the **User email address** field, enter an email address to test the connection to the Microsoft Exchange Server or Microsoft Office 365 server. Click **Test connection**. If the test fails, resolve the issues that are identified and try the test again. You can delete the email address after you complete the test.
14. Click **Save**.

After you finish:

- Test the connection to the on-premises Microsoft Exchange Server or Microsoft Office 365 server and Autodiscover. Refresh or reopen the Email notifications screen. Click **Test connection**.
  Note: Make sure that the connection test is successful before provisioning devices to avoid any Autodiscover issues. If devices are activated prior to configuring the email notification service, have users log out of BlackBerry Work and then log in. If the test returns an error message, complete the tasks to resolve the issue and test the connection again.
- Assign the BlackBerry Cloud Enterprise Services (com.blackberry.gdservice-entitlement.cloud) entitlement to users to receive email notifications for BlackBerry Work. For instructions, see the following administration content:
  - Assign an app to a user group
  - Assign an app group to a user group

    - Assign an app to a user account
    - Assign an app group to a user account
- Optionally, create a trusted connection between the BEMS Cloud and Microsoft Exchange Server. For instructions, see Create a trusted connection between BEMS Cloud and Microsoft Exchange Server.
- Optionally, configure the BEMS-Docs service. For instructions, see Enable the BEMS-Docs service.

Grant application impersonation permission to the service account

For the BlackBerry Push Notifications service to monitor mailboxes for updates, the BlackBerry Push Notifications service account, must have impersonation permissions.

Complete one of the following actions to apply Application Impersonation permissions to the service account:

Grant application impersonation permissions	Steps
Microsoft Office 365 using the Exchange Administration Center console	**a.** Sign in to https://admin.exchange.microsoft.com/. **b.** Click **Roles > Admin roles**. **c.** Click **Add role group**. **d.** Type a name for the role. **e.** In the **Write scope** drop-down list, click **Default**. **f.** Click **Next**. **g.** In the Search field, search for the **ApplicationImpersonation** role. Click the checkbox next to the role. **h.** Click **Next**. **i.** In the text field, type the member name or the service account that will process the notifications. **j.** Click **Next**. **k.** Click **Add role group**. **l.** Click **Done**.
On-premises Microsoft Exchange using the Exchange Administration Center	**a.** In a browser window, type `https://<url_to_on-premises_client_access_server>/ecp` and sign in with a valid account. **b.** Click **permissions**. **c.** Click +. **d.** Type a name and description for the role group. **e.** In the **Roles** section, click +. Click **ApplicationImpersonation > add > OK**. **f.** In the **Members** section, click +. Click an account to add and then click **add > OK**.

Grant application impersonation permissions	Steps
Using Microsoft Exchange Management Shell	**a.** Open Microsoft Exchange Management Shell. **b.** Type `New-ManagementRoleAssignment -Name:<ImpersonationAssignmentName> -Role:ApplicationImpersonation -User:<ServiceAccount>`. For example, `New-ManagementRoleAssignment -Name:BlackBerryAppImpersonation -Role:ApplicationImpersonation -User:BEMSAdmin`. For more information on how to restrict Application Impersonation rights to specific users, organizational units, or security groups, visit the MSDN Library to see How to: Configure impersonation.

Enable Microsoft Graph API to allow BEMS Cloud to communicate with Microsoft Office 365

Important: Complete this task only if your BEMS Cloud environment requires new client app registrations.

You must can use BEMS Cloud to access Microsoft Office 365 to access users' mailboxes and send notifications to users' devices when new email is received in the user's mailbox using Microsoft Graph API. When you configure the Microsoft Graph API, your environment is using modern authentication. After you configure the Microsoft Graph API, you must configure the autodiscover.

In 2022, Microsoft started to deprecate the Microsoft Exchange Web Services (EWS) for Microsoft Exchange Online APIs and replacing the EWS with the Microsoft Graph API. For more information, visit techcommunity.microsoft.com and read 'Upcoming API Deprecations in Exchange Web Services for Exchange Online'.

Before you begin:

- Configure the email notifications for BlackBerry Work. For instructions, see Configure email notifications for BlackBerry Work.
- If you enable Microsoft Graph using Client Secret, obtain the **Client secret**.
- If you enable Microsoft Graph using a Client Certificate:
  - Obtain an Entra app ID for BEMS with certificate-based authentication.
  - Request and associate the .pfx certificate with the Azure app ID for BEMS.

1. In the management console, click **Settings > BlackBerry Dynamics > Email notifications**.
2. Click the **Microsoft Graph** tab.
3. Click .
4. Select the **Use Microsoft Graph client** check box.
5. In the **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
Client Secret	This option uses a client secret to allow the BEMS service account to authenticate to Microsoft Office 365. The client secret is created during the application registration process.	In the **Client Secret** field, enter the **Value**for the client secret. For instructions on obtaining a client secret, see Obtain an Entra app ID for BEMS with client secret authentication.
Client Certificate	This option uses a client certificate to allow the BEMS service account to authenticate to Microsoft Office 365.	**a.** For the **Certificate file (.pfx)**, click **Browse** and select the client certificate file. For instructions on obtaining the .PFX file, see Associate a certificate with the Entra app ID for BEMS **b.** In the **Password** field, enter the password for the client certificate.

6. In the **Authentication Authority** field, enter the Authentication Server URL that BEMS accesses and retrieve the OAuth token for authentication with Microsoft Office 365. By default, the field is prepopulated with https://login.microsoftonline.com/common.

   Note: The authentication server URL must be in the format of https://login.microsoftonline.com/*tenantname* or https://login.microsoftonline.com/*tenantid*.
7. In the **Client App ID** field, enter the Entra app ID for the credential authentication. For instructions, see Obtain an Entra app ID for BEMS with credential or passive authentication.
8. In the **Server Name** field, type `https://graph.microsoft.com`.
9. In the **End User Email Address** field, type an email address to test connectivity to Microsoft Office 365 using the service account. Click **Test connection**. You can delete the email address after you complete the test.
10. Click **Save**.
11. Configure the Autodiscover and Exchange Options in Configure email notifications for BlackBerry Work. You can configure the settings using one of the following authentication types: Credential, Credentials + Modern Authentication, Client Certificate + Modern Authentication, or Passive Authentication type.

Obtain an Entra app ID for BEMS with client secret authentication

1. Sign in to portal.azure.com.
2. In the left column, click **Microsoft Entra ID**.
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. If you use passive authentication for users to authenticate to the identity provider (IDP), in the **Redirect URI** drop-down list, select **Public/client (mobile & desktop)** and enter `https://localhost:8443`. The Redirect URI is the URL that the user is redirected to after they successfully authenticate to the IDP. **Important**: Make sure that the Redirect URL matches the URL to the dashboard or authentication might not work as expected.
8. Click **Register**. The new registered app appears.
9. In the **Manage** section, click **API permissions**.
10. Click **Add a permission**.
11. Click **Microsoft Graph**.

12. Click **Application permissions** and set the following permissions:
    - Read mail in all mailboxes (**Mail > Mail.Read**)
    - Read all user's full profile (**User > User.Read.All**)
    - Read and write contacts in all mailboxes (**Contacts > Contacts.ReadWrite**)*

      Note: * This permission is only required if you require the Contact Service API to use third-party apps to query, retrieve, create, and update contact information from a user's contact folder. For more information on the BEMS Contact Service API, see Contact Service API reference content.
13. Click **Update permissions**.
14. Click **Grant admin consent**. Click **Yes**.
15. Add a client secret.
    a) In the **Manage** section, click **Certificates & secrets**.
    b) Click **New client secret**.
    c) In the **Description** field, enter a key description up to a maximum of 16 characters including spaces.
    d) Set an expiration date (for example, 3 months, 12 months, custom).
    e) Click **Add**.
    f) 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 **Client secret** in the BEMS Dashboard when you enable Microsoft Office 365 and configure BEMS to communicate with Microsoft Office 365.

Obtain an Entra app ID for BEMS with credential or passive authentication

1. Sign in to portal.azure.com.
2. In the left column, click **Microsoft Entra ID**.
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, click **Microsoft Graph**.
11. Set the following permissions:
    - For Microsoft Exchange Web Services: Access mailboxes as the signed-in user via Exchange Web Services (**EWS > EWS.AccessAsUser.All**)

Note: In 2022, Microsoft started to deprecate the Microsoft Exchange Web Services (EWS) for Microsoft Exchange Online APIs replacing the EWS with **Microsoft Graph** and this permission may not be available. For more information, visit techcommunity.microsoft.com and read 'Upcoming API Deprecations in Exchange Web Services for Exchange Online'.

- For Microsoft Graph: For Sign in and read user profile (**User > User.Read**).

12. Click **Update permissions**.
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 **Allow public client flows** section, select **Yes** to **Enable the following mobile and desktop flows**.
    c) 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 Entra app ID for BEMS with certificate-based authentication

1. Sign in to portal.azure.com.
2. In the left column, click **Microsoft Entra ID**.
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. Click **Register**. The new registered app appears.
8. In the **Manage** section, click **API permissions**.
9. Click **Add a permission**.
10. In the **Select an API** section, click **APIs my organization uses**.
11. Click **Office 365 Exchange Online**.
12. Set the following Application permissions for Office 365 Exchange Online:

    - Use Exchange Web Service with full access to all mailboxes (**full_access_as_app**)

13. Click **Add permissions**.
14. Click **Microsoft Graph**.
15. Set the following Application permissions for Microsoft Graph.

    - Read and write contacts in all mailboxes (**Contacts > Contacts.ReadWrite**)
    - Send mail as any user (**Mail > Mail.Send**)
    - Read all user's full profile (**User > User.Read.All**)

16. Click **Add permissions**.
17. Click **Grant admin consent**.
18. Click **Yes**.
19. 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 Entra app ID for BEMS

You can use an existing certificate from your CA server or the New-SelfSignedCertificate command to create a self-signed certificate. For more information, visit docs.microsoft.com and read New-SelfSignedCertificate.

Before you begin: Verify that you have the app name you assigned in BEMS with certificate-based authentication.

1. If you have a certificate issued by a CA server, go to step 2. Create a self-signed certificate.
   a) On the computer running Microsoft Windows, open the Windows PowerShell.
   b) 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 Entra app ID for BEMS with certificate-based authentication.
   c) Press **Enter**.
2. Export the certificate from the Certificate Manager. This creates the public certificate. Make sure to save the public certificate as a .CER or .PEM.
   a) On the computer running Windows, open the Certificate Manager for the logged in user.
   b) Expand **Personal**.
   c) Click **Certificates**.
   d) Right-click the <*user*>@<*domain*> and click **All Tasks > Export**.
   e) In the **Certificate Export Wizard**, click **No, do not export private key.**.
   f) Click **Next**.
   g) Select **Base-64 encoded X.509 (.CER)**. Click **Next**.
   h) Provide a name for the certificate and save it to your desktop.
   i) Click **Next**.
   j) Click **Finish**.
   k) Click **OK**.
3. Upload the public certificate to associate the certificate credentials with the Entra app ID for BEMS.
   a) In portal.azure.com, open the <*app name*> you assigned the app in step 5 of Obtain an Entra app ID for BEMS with certificate-based authentication.
   b) Click **Settings > Keys**.
   c) Click **Upload Public Key**.
   d) Click and navigate to the location where you exported the certificate in step 2.
   e) Click **Open**.
   f) Click **Save**.

After you finish: Export the certificate in .pfx format using the Manage User Certificate MMC snap-in. Make sure to include the private key. For instructions, visit docs.microsoft.com and read Export a Certificate with the Private Key.

Create a trusted connection between BEMS Cloud and Microsoft Exchange Server

By default, BEMS is only aware of public CA certificates. If you enable email notifications for BlackBerry Work and your organization's Microsoft Exchange Server doesn't use an SSL certificate issued by a trusted CA, the connection between BEMS Cloud and Microsoft Exchange Server isn't trusted. To create a trusted connection to the Microsoft Exchange Server upload the server's SSL certificate (or the root or intermediate certificate chain) to the BEMS Cloud database. You can upload a base64-encoded or binary-encoded file that includes one or more SSL certificates. When you upload a single file that includes multiple SSL certificates, the certificates are displayed in the management console and can be deleted and replaced individually as required. BEMS Cloud supports the following file extensions: .der, .cer, .pem, and .crt.

Before you begin:

- Configure the email notifications for BlackBerry Work. For instructions, see Configure email notifications for BlackBerry Work.
- Export the SSL certificate from the Microsoft Exchange Server in a base64-encoded or binary-encoded format and store it in a network location that you can access from the management console. For more information about digital certificates and encryption in Microsoft Exchange Server, visit https://docs.microsoft.com/en-us/exchange/architecture/client-access/certificates?view=exchserver-2016

1. On the menu bar, click **Settings > BlackBerry Dynamics**.
2. Click **Email notifications**.
3. Click the **Certificates** tab.
4. Click .
5. Click **Add**.
6. Click **Browse** and navigate to the location of the certificate file that you want to upload.
7. Click **Add**.
8. If you upload individual SSL certificates, repeat steps 5 to 7 for each additional file.

Replace or delete the trusted connection SSL certificates

When you replace the SSL certificates (for example, when the certificates expire), you replace all of the existing SSL certificates in the BEMS database. You can chose to upload individual SSL certificates as required or include multiple SSL certificates in a single file. The following file types are supported: .der, .cer, .pem, and .crt.

Before you begin:

- Export the new SSL certificates from the Microsoft Exchange Server in a base64-encoded or binary-encoded format and store it in a network location that you can access from the management console. For more information about digital certificates and encryption in Microsoft Exchange Server, visit https://docs.microsoft.com/en-us/exchange/architecture/client-access/certificates?view=exchserver-2016

1. On the menu bar, click **Settings > BlackBerry Dynamics**.
2. Click **Email notifications**.
3. Click the **Certificates** tab.
4. Click .
5. Click **Remove** under the certificate that you want to delete.
6. Click **Remove** to confirm the deletion.
7. Add the new certificate. For instructions, see Create a trusted connection between BEMS Cloud and Microsoft Exchange Server.

Configure the password expiration warning message

For Active Directory users and user groups that use the PSO (Password Settings Object) method to set the maximum password age, you can configure the BEMS dashboard and BEMS Cloud to allow users' BlackBerry Work apps to display a warning message when their Active Directory password is about to expire. By default, this feature is disabled.

Note: In a BEMS Cloud environment, you must configure the Email notifications for BlackBerry Work in the BlackBerry UEM management console using the Credential authentication type to display the Password expiry tab.

For information on displaying a warning message for users that use the GPO (Global Policy Object) method to set the maximum password age, see Configure BlackBerry Work app settings.

Before you begin:

- Make sure that you have the following information:
  - Logon credentials for the service account that is used to authenticate to the domain controller.
  - LDAP server name and port number. The LDAP server name must be one of the Domain Controllers.
- Verify that the service account has READ permissions to the "Password Settings Container". For instructions, see Add Read permission to the account used to authenticate to the LDAP server.
- In a BEMS Cloud environment, also verify that a BlackBerry Connectivity Node is installed and configured. For more information, see Steps to install and activate the blackberry connectivity node.
- Verify that administrators use the PSO method to set the maximum password age for the users.
- Verify that users in your environment are running BlackBerry Work 3.8 or later.

1. Complete one of the following tasks:

Environment	Steps
BEMSon-premises	**a.** In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Configuration**, click **Mail**. **b.** Click **Password Expiry Settings**. **c.** Select the **Enable LDAP Lookup** checkbox to allow BEMS to query Active Directory for password expiry details for the users. **d.** In the **LDAP Server Name** field, type the name of the LDAP Server (for example, ldap.<*DNS_domain_name*>). **e.** In the **LDAP Server Port** field, type the port number of the LDAP server. By default, the port number is 389. **f.** Optionally, select the **Enable SSL LDAP** checkbox to tunnel data through an SSL-encrypted connection. If you enable SSL LDAP, the default port is to 636. This step requires you to import the LDAP certificate into the BEMS keystore. For instructions, see "Upload the Microsoft Exchange Server SSL certificate to the BEMS database" in the BEMS-Core configuration content. **g.** In the **LDAP Base DN** field, enter the base DN for the LDAP search. If this entry is not set, BEMS tries to find the base DN in the namingContexts attribute.

Environment	Steps
BEMSCloud	a. In the BlackBerry UEM Cloud management console, click **Settings > BlackBerry Dynamics > Email notifications**. b. Click the **Password expiry** tab. c. Click ✎. d. Select the **Enable password expiry** checkbox to allow BEMS to query Active Directory for password expiry details for the users. e. In the **LDAP server name** field, type the name of the LDAP Server (for example, ldap.<*DNS_domain_name*>). f. In the **LDAP port** field, type the port number of the LDAP computer. The default port is 389. g. Enter the LDAP logon account and password. You can enter the logon account in the format `domain\username` or User Principal Name (UPN) `username@domain`. h. In the **Base DN (Domain controller)** field, enter the base DN for the LDAP search. If this entry is not set, BEMS tries to find the base DN in the namingContexts attribute. i. Optionally, select the **Enable SSL LDAP** checkbox to tunnel data through an SSL-encrypted connection. If you enable SSL LDAP, type the port number to the LDAP computer that you used in step 6. The default port for is 636. This step requires you to import the LDAP certificate into the BEMS keystore. For instructions, see Create a trusted connection between BEMS Cloud and Microsoft Exchange Server.

2. Click **Test** to test the connection to the LDAP server.
3. Click **Save**.

Add Read permission to the account used to authenticate to the LDAP server

You can use the Windows Server ADSI Edit tool to add Read permissions to the account that is used to authenticate to the LDAP server. You must have a membership in the Domain Admins group or equivalent permissions to complete this task.

1. Start the ADSI Edit utility.
2. Right click the **ADSI Editor** icon and click **Connect to**.
3. In the **Connection Settings** screen, in the **Connection Point** section, select **Select a well known Naming Context** and from the drop-down list, select **Default naming context**.
4. Click **OK**.
5. Click your domain.
6. Navigate to and expand **CN=System**.
7. Right-click **CN=Password Settings Container** and click **Properties**.
8. On the **Security** tab, click **Add** to add the account, or the user group that the account is a member of, that is used to authenticate to the LDAP server.
9. Under **Group or user names**, with the added account or user group selected, select the **Read** checkbox in the **Allow** column.
10. Click **Apply**.
11. Click **OK**.

Migrating a BlackBerry Work mailbox from an on-premises Microsoft Exchange Server to Microsoft Office 365

You can migrate a BlackBerry Work mailbox from an on-premises Microsoft Exchange Server to Microsoft Office 365 with minimal user interaction. Before you start the migration, BlackBerry recommends that you select the “Migration Flow Enabled” option on the Advanced Configuration tab of your organization’s app configuration for BlackBerry Work. The benefit of updating the app configuration before you perform the backend migration of the user’s mailbox is that the user’s email will continue to be synchronized and the app will not switch to offline mode during the migration. The user might be required to enter their credentials during or after the migration. This feature requires BlackBerry Work 3.2 or later.

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 Managing apps content.
- 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 BlackBerry Work app configuration settings, 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 version, see Export BlackBerry Dynamics app reports to a CSV file in the BlackBerry UEM Monitoring and reporting content.

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.

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.

Troubleshooting mailbox migration

After the mailbox migration is complete, if some of your organization's users encounter any issues such as the Entra Active Directory Authentication Libraries (ADAL) form not displaying, you can try to enforce app configuration. In the app configuration for BlackBerry Work, on the Basic Configuration tab, select the Enforce App Configuration option. This option ensures that Modern Authentication, EAS/EWS endpoints, and the Microsoft Office 365 settings configured in the app configuration profile are applied.

Note: BlackBerry recommends that you copy your organization's app configuration, select the **Enforce App Configuration** option, and apply the app configuration only to the affected users.

Turning off notifications outside of work hours

You can use Do not disturb profiles to block device notifications outside of work hours in BlackBerry Work for Android and BlackBerry Work for iOS. This feature requires BEMS 2.8 or later.

Create a Do not disturb profile

Before you begin:

- BEMS 2.8 or later is installed and configured in your environment. For instructions, see the BEMS installation and configuration guides.
- BlackBerry Work is added to the BlackBerry Dynamics connectivity profile. See Configure BlackBerry Work connection settings.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Protection > Do not disturb**
3. Click +.
4. Type a name and description for the profile.
5. Enter a message to display on devices when BlackBerry Work notifications are blocked . If you leave this field blank, a default message is displayed.
6. Do one of the following:

Task	Steps
Specify common work days and hours.	**a.** Click the **Select common work days and hours** option. **b.** In the **From** drop-down lists, specify the time that work days start. **c.** In the **To** drop-down lists, specify the time that work days end. **d.** In the **Work days** list, select the days of the week that are work days.
Specify custom work hours for specific days.	**a.** Click the **Select custom work days and hours** option. **b.** Select a day of the week. **c.** In the **From** drop-down lists, specify the time that the work day starts. **d.** In the **To** drop-down lists, specify the time that the work day ends. **e.** Repeat steps 2 to 4 for each day of the week that is a work day.

7. Click **Add**.

Best practice: Enabling autodiscovery

When you enable autodiscovery to automatically discover the Microsoft Exchange ActiveSync server in your environment, consider the following guidelines:

- Make sure that Microsoft Exchange Autodiscover is set up correctly. For more information, see the Microsoft documentation for Microsoft Exchange.
- In a Microsoft Exchange environment: Make sure that the autodiscover URL routes to one of the Exchange client access server (CAS) servers. If your environment uses a load balancer, make sure that the Auto Discover URL routes to the load balancer and then route it to your group of CAS servers.
- In a mixed Microsoft Exchange environment (for example, Microsoft Exchange Server 2016 and 2019) environment: Make sure that the autodiscover URL routes to the latest version of the CAS servers (for example, the Microsoft Exchange Server 2019).
- In a cloud-based Microsoft Exchange environment: the autodiscover URLs are typically managed by Microsoft, however if your environment migrated your domain to a cloud-based Microsoft Exchange, make sure that the domain autodiscover URL routes to Microsoft's autodiscover URL (for example, https://autodiscover-s.outlook.com). In the DNS admin portal, make sure a CNAME record is created and that it redirects https://autodiscover.<*mydomain*>/autodiscover/autodiscover.xml to https://autodiscover-s.outlook.com.
- In a cloud-based Microsoft Exchange hybrid environment: mailboxes can exist in both on-premises Microsoft Exchange and cloud-based Microsoft Exchange. Make sure that the autodiscover URL routes to the on-premises Microsoft Exchange Server.

Note: All autodiscover URLs must be whitelisted on BlackBerry UEM. For more information on how to use third-party tools to test autodiscover, visit support.blackberry.com/community to read article 40351.

File types supported by BlackBerry Work

The following file types are supported as mail attachments (some require third-party applications to view):

- goodsharefile
- .doc, Docx
- .ppt, PPTx

- .xls, XLSX
- .sheet
- .pdf
- .rtfd
- webarchive
- image
- .jpeg
- .tiff
- .apple.pict
- .compuserve.gif
- .png
- .quicktime-image
- .bmp
- .camera-raw-image
- .svg-image
- .text
- plain-text
- .utf8-plain-text
- .utf16-plain-text
- .rtf
- .html
- .xml
- .xhtml
- .htm
- .data
- .content
- .zip

Media Files (iOS only)

- .3gp
- .mp3
- .mp4
- .m4a
- .m4v
- .wav
- .caf
- .aac
- .adts
- .aif
- .aiff
- .aifc
- .au
- .snd
- .sd2
- .mov

Configure BlackBerry Tasks and BlackBerry Notes app settings

BlackBerry Tasks and BlackBerry Notes use Microsoft Exchange Web Services and do not use Exchange ActiveSync like BlackBerry Work. This means that BlackBerry Tasks and BlackBerry Notes may have different authentication configurations than BlackBerry Work.

Before you begin: Depending on your environment, if your users are configured with UPNs that are different from their email address, you might need to enable the "Use explicit UPN" property. This requires BlackBerry UEM 12.11 or later. For more information, see BlackBerry Dynamics global properties.

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. For the BlackBerry Tasks app only, on the **Notifications** tab, in the **Select level or detail in Tasks reminders** drop-down list, select whether to turn off task notifications on the user's device, to display a generic notification, or to display the title of the task in the notification.
6. On the **Configurations Settings** tab, in the **Security Settings** section, configure the following settings:
   a) Select the **Use of Kerberos Constrained Delegation in place of login/password** option to use Kerberos Constrained Delegation as the login type for users. When Kerberos Contrained Delegation is used, users do not have to enter a password for Exchange ActiveSync.
   b) Select the **Use client certificate in place of login/password** option to require the use of certificates for login instead of a username and password. This is a requirement if certificate-based authentication is required for Microsoft Exchange Web Services.
7. In the **Embedded Hyperlink Support** drop-down list, select the allowed behavior when a user opens a hyperlink.
8. In the **Enterprise Mobility Server** section, configure the following:
   a) In the **Server List Reshuffle Period (minutes)** field, specify the frequency that the BEMS server list is reshuffled (if present), for load balancing purposes. The default setting is 10 minutes.
   b) In the **Server List Quarantine Period (minutes)** field, if a BEMS server is not working, BlackBerry Tasks will wait this period before it retries. The default setting is 10 minutes.
9. On the **Exchange Settings** tab, configure the following:
   a) In the **Exchange Web Services Authentication Methods (iOS only)** section, choose the authentication methods to be used: Negotiate, NTLM, or Basic. If only certain authentication methods are supported from Microsoft Exchange, set those values to minimize the user setup time. (For example, if the EWS IIS Auth Setting is set to allow only NTLM, then select only NTLM above for an optimal setup experience.) If none are selected above, the default Microsoft Exchange setting will be used.
   b) In the **Microsoft Exchange Settings** section, in the **Exchange Domain** field, specify the default Windows NT domain that BlackBerry Tasks will try to connect to automatically when users log in to BlackBerry Notes or BlackBerry Tasks. If your server uses newer UPN (email@host.com) style login instead of the older (domain \user) style login, leave this field blank. In the **Exchange Server** field, specify the FQDN of the server, CAS Array, or Load Balancer that is responsible for providing Microsoft Exchange Web Services. If you leave this field blank, BlackBerry Notes or BlackBerry Tasks uses assisted autodiscover through BEMS if BEMS is configured, and if BEMS is listed in the application server list for BlackBerry Notes or BlackBerry Tasks. Enter only the FQDN of the Microsoft Exchange server. Do not include a protocol prefix such as https:// or a URI suffix.
10. On the **Exchange settings** tab, configure the following settings:
    a) In the **Exchange Web Services User Name Formats (iOS only)** section, choose which of the following user name formats to use to authenticate with Microsoft Exchange Web Services: UPN, Domain\UserId,

or SMTP. If only certain user name formats are supported from Microsoft Exchange, set those values to minimize the user setup time. (For example, if the EWS Auth Settings are set to allow only SMTP but not UPN, then deselect UPN in the app setting.) If none are selected above, authentication with all user name formats will be attempted.

b) In the **TLS Certificate Settings** section, specify the user credential profile that contains the TLS certificate to be used to connect to Microsoft Exchange. The name of the profile that you specify here must match the name of the user credential profile that was created in the BlackBerry UEM management console. For more information on user credential profiles, see Sending client certificates to devices and apps using user credential profiles Using user credential profiles to send certificates to devices.

11. In the **Microsoft Office 365 Modern Auth Settings (Beta)** 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.

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.

d) In the **Azure App ID** field, specify the Microsoft Entra ID app ID for BlackBerry Notes or BlackBerry Tasks. For information on how obtain an Entra app ID, see Obtain an Azure app ID for BlackBerry Work.

e) In the **Office 365 Resource** field, specify the URL of the Microsoft Exchange Online server.

f) In the **Redirect URI** field, specify the URI that you entered in the Microsoft Entra ID portal.

g) Select the **Proxy Modern Authentication requests (only)** setting to force all Office 365 Modern Authentication requests to go through the BlackBerry Proxy instead of connecting directly to the Internet.

12. In the **Exchange User Name** section, select UPN to use a UPN user name format instead of SMTP when authenticating with Microsoft Exchange.

13. On the **App Settings** tab, configure the following:

a) Select the **Allow users to perform app diagnostics** option, to allow users to generate a diagnostics report and then email the results to their administrator.

b) Select the **Enable DLP Watermark** option to display a user's username and the date and time as a watermark on all screens in BlackBerry Notes or BlackBerry Tasks.

14. For BlackBerry Notes only, select the **Store the Title of the Notes in the Note body** option to save the note title with the note body. This option requires Microsoft Exchange 2016 or later.

15. On the **Interoperability** tab, configure the following:

a) For BlackBerry Tasks for iOS and BlackBerry Notes for iOS only, select the **Tap a phone number to dial using native phone** option to allow users to tap a phone number to dial using the device's native phone.

b) For BlackBerry Tasks for Android and BlackBerry Notes for Android, select the **Grant permission to use the Tasks list widget (Android only)** option to specify whether the list widget can be used on Android devices.

16. On the **Attachments** tab, configure the following:

a) Specify whether to allow incoming and outgoing attachments.

b) Specify the maximum size.

c) Specify the file extensions that are allowed or disallowed.

17. On the **Deprecated** tab, select the **Disable SSL Certificate Checking** option to disable SSL certificate verification for Microsoft Exchange Web Services servers in test environments.

18. Click **Save**.

BlackBerry Tasks and Notes app configuration settings

Notifications	Description
Select level of detail in Tasks reminders (Tasks only)	Select the level of detail that users see in tasks reminders. Available settings: • No notifications • Show generic notification • Show task title

Configuration Settings	Description
Security settings	Select the "Use Kerberos Constrained Delegation in place of login/password" option to specify whether Kerberos Constrained Delegation will be used for logging in to Microsoft Exchange. If this option is not selected, NTLM/Basic authentication will be used. Select the "Use client certificate in place of login/password" option to specify whether clients must have individual login certificates (SSL) uploaded to the BlackBerry UEM management console. These certificates are used for login instead of basic credentials (username/password).
Embedded Hyperlink Support	Administrators can select any of the following settings: • Do not allow user to open hyperlinks • Only allow secure browser • Prefer secure browser but allow device browser
Enterprise Mobility Server	In the Server List Reshuffle Period (minutes) field, specify the frequency that the server list, if present, is reshuffled for load balancing purposes. In the Server List Quarantine Period (minutes) field, specify how long BlackBerry Tasks or BlackBerry Notes waits before retrying if BlackBerry UEM is not working.

Exchange settings	Description
Exchange web services authentication methods (iOS only)	Specify the authentication methods to use. If only certain authentication methods are supported in Microsoft Exchange, set those values to minimize the user setup time. (For example, if EWS IIS Auth Setting is set to allow only NTLM, then select only NTLM above for an optimal setup experience.) If none are selected above, the default Microsoft Exchange setting is used. If using client-based authentication, check none of the options.
Microsoft Exchange settings	Specify the Exchange domain or the Exchange server you want to use.

Exchange settings	Description
Exchange web services user name formats (iOS only)	Select the username formats that can be used to authenticate with Microsoft Exchange Web Services. Available settings: • UPN • Domain\UserId • SMTP To simplify user setup, select only the username formats that are supported by Microsoft Exchange Web Services. If you do not select an option, all options are allowed.
TLS certificate settings	Specify the user credential profile that contains the TLS certificate to be used to connect to Microsoft Exchange. The name of the profile that you specify must match the name of the user credential profile that was created in the BlackBerry UEM management console. For more information on user credential profiles, see Sending client certificates to devices and apps using user credential profiles.
Office 365 modern auth settings	• Select the "Use Office 365 Modern Authentication" option to use modern authentication instead of basic authentication. Modern authentication enables BlackBerry Tasks or BlackBerry Notes to use sign-in features such as Multi-Factor Authentication, SAML-based third-party Identity Providers, and smart card and certificate-based authentication. • In the "Office 365 Sign On URL" field, specify the web address that BlackBerry Tasks or BlackBerry Notes should use when signing in to Office 365. If you do not specify a value, BlackBerry Tasks and BlackBerry Notes will use https://login.microsoftonline.com during setup. • In the "Office 365 Tenant ID" field, specify the tenant ID of Office 365 server that you want BlackBerry Tasks or BlackBerry Notes to connect to during setup. • In the "Entra App ID" field, specify the Microsoft Entra ID app ID for BlackBerry Tasks or BlackBerry Notes. For information on how obtain an Entra ID, see Obtain an Azure app ID for BlackBerry Tasks and BlackBerry Notes. • 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 Entra ID portal. • Select the "Use Office 365 Brokered Authentication" setting to use brokered authentication when using Modern Authentication. This setting is required for Entra Conditional Access. • 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.
Exchange User Name Format	In the "Exchange User Name Format" section, select UPN to use a UPN user name format instead of SMTP when authenticating with Microsoft Exchange Online. Depending on your environment, if your users are configured with UPNs that are different from their email address, you might need to enable "Use explicit UPN" property. For more information, see BlackBerry Dynamics global properties.

App settings	Description
Data leakage prevention watermark	If you select the "Enable DLP Watermark" option, a watermark is added to all BlackBerry Dynamics app screens (for example, BlackBerry Work, BlackBerry Work Docs, Calendar, and Contacts). The watermark shows the user's username and current date and time. **Note**: If users print a file, the watermarks are not displayed in the output.
Screenshot Prevention (iOS Only)	Select the "Prevent Screenshots on iOS" option to prevent screenshots of BlackBerry Tasks or BlackBerry Notes from being taken on an iOS device.
Diagnostics	If you select the "Allow users to perform app diagnostics" option, users can perform app diagnostics from the BlackBerry Dynamics Launcher on their devices.
Notes setup (Notes only)	• Select "Store the title of the note in the note body" to include the title of the note in the body content. • Select the "Disable note editing for OWA" option to disable editing notes in OWA. Notes created in BlackBerry Notes will not be presented as drafts and users will not be able to add attachments, inline images, or make any edits using OWA.

Interoperability	Description
Camera and Device Photo Gallery Permissions	Specify whether to allow access to the device camera, the photo gallery, or both. Available settings: • Allow access to camera and device photo gallery • Allow access to camera only • No access to camera or device photo gallery The default value is "Allow access to camera and device photo gallery."
Voice	Select the "Tap a phone number to dial using native phone" option to allow users to use the native phone app.
Widget (Tasks only)	Select the "Grant permission to use the Tasks list widget (Android only)" option to allow users to use the Tasks list widget.

Attachments	Description
Receiving/opening attachments	Specify whether to allow incoming attachments and specify a maximum size and the file extensions that are allowed or disallowed.

Attachments	Description
Block receiving attachments with total size larger than	Select a size from the drop-down list to block attachments larger than that size. Blocked attachment sizes can be any of the following: • 25KB • 100KB • 500KB • 1MB • 2MB • 4MB • 6MB • 8MB • 10MB • 12MB • 24MB • 36MB
Block/Only allow receiving attachments by file extension	Select if you want to block or only allow receiving attachments by file extensions and specify the file extensions.

Deprecated	Description
Microsoft Authentication Library	Disabling this policy will result in using legacy Microsoft Azure Active Directory Authentication Library when logging into Notes mailbox account. (iOS Only)
Security settings	Select the "Disable SSL Certificate Checking" option to disable SSL Certificate verification for Exchange ActiveSync/Microsoft Exchange Web Services in test environments.

Obtain an Entra 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 Entra app IDs for BlackBerry Tasks and BlackBerry Notes.

Tip: You will need to perform these steps 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 BlackBerry Tasks or BlackBerry Notes 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.tasks://connect/o365/redirect` or `com.blackberry.notes://connect/o365/redirect`

8. Click **Register**.
9. Optionally, if you are enabling Entra ID conditional access:
   a) Click on the **Redirect URIs** link (i.e. '0 web, 0 spa, 1 public client').
   b) Perform one of the following actions:

Task	Steps
Enable Entra ID conditional access for an iOS device	1. Under the existing **Mobile and desktop applications** section, click **Add URI**. 2. Enter one of the following URIs: • `x-msauth-tasks://com.blackberry.gd.tasks` • `x-msauth-notes://com.blackberry.gd.notes`
Enable Entra ID conditional access for an Android device	1. Click **Add a platform > Android**. 2. In the **Package name** field, enter one of the following package names: • `com.blackberry.gd.tasks` • `com.blackberry.gd.notes` 3. In the **Signature hash** field, enter: `zRsXTl1cL/Seb6GumLzvoecPA8w=`

10. In the **Manage** section, click **API permissions**.
11. Click **Add a permission**.
12. In the **Select an API** section, click the **Microsoft APIs** tab.
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 **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.
16. 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.

Installing and activating BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks

Before users can begin using BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks, they must be activated. The steps that users take to install these apps depend on how you have configured your environment. If you have not yet configured your activation settings, see Activating devices with BlackBerry UEM for steps on how to configure your environment to support BlackBerry Dynamics apps.

The following options are available for installing the apps on iOS and Android devices:

- For MDM managed devices, using BlackBerry UEM, you can push BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks to users or you can make the app available to their work catalogs. No access key is required to activate BlackBerry Dynamics apps.
- For devices that are not MDM managed, users can download BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks from the App Store or the Google Play store. Users require an access key to activate these apps.

The following options are available for activating the apps on iOS and Android devices:

- Activate the apps using the BlackBerry UEM Client or another BlackBerry Dynamics app that is already installed on the device: This option provides users with a consistent, streamlined activation experience. Users need only their email address and an activation password and do not require an access key. Users must install the UEM Client to activate their devices with MDM. For this option to be available to users, you must allow the UEM Client to manage the activation of BlackBerry Dynamics apps.
- Activate the apps using an activation key, activation password, or QR code: Users would choose this option if they have not installed the UEM Client on their device or if you have not allowed the to manage the activation of BlackBerry Dynamics apps.

Install the apps when the BlackBerry UEM Client or another BlackBerry Dynamics app is already activated on the iOS device

You can send the following instructions to iOS device users that are installing BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks when the BlackBerry UEM Client or another BlackBerry Dynamics app is already activated on the iOS device and the app acts as an easy activation delegate.

1. If the app was not automatically pushed to your device by your administrator, open your Work Apps app and install the BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks app. If you do not see the BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks apps in your Work Apps app, contact your administrator to make the app available to you.
2. On your device, tap <name of app>.
3. Click **Allow** to allow the app to send notifications.
4. Tap **Client End User License Agreement** to read the license agreement and, if you accept the terms, tap **I Agree**.
5. Tap **Set up using <BlackBerry UEM Client or existing BlackBerry Dynamics app>**.
6. Enter your password for the BlackBerry UEM Client or the existing BlackBerry Dynamics app. Tap **Enter** on the device.
7. If prompted, create and confirm a password for the app. If your device is equipped with Touch ID, you can turn on this option to use instead of the password, except on initial startup.
8. If prompted, allow the app to use your location history to establish trusted locations.

9. If other devices, including your principal workstation, are also signed in, you will receive a notice advising you of this condition. Tap **OK**.

Install and activate the apps using an access key, activation password, or QR code on an iOS device

You can send the following instructions to iOS device users that are installing BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks using an access key, activation password, or QR code.

1. Use the access key, activation password, or QR code that was provided by your administrator or generate an access key or QR code from your organization's self-service portal.
2. After you receive the email message with the activation details or have generated your own access key, activation password, or QR code, download and install the app from the App Store.
3. Tap <name of app>.
4. Tap **Client End User License Agreement** to read the license agreement and, if you accept the terms, tap **I Agree**.
5. Complete one of the following tasks:

Activation method	Steps
Access key*	**a.** In the **Email Address** field, type the email address located in the activation email message that you received from your administrator or type your work email address if you generated your own access key. **b.** In the **Activation password** field, enter the access key, without hyphens, located in your activation email message that you received from your administrator or enter the access key that you generated in the BlackBerry UEM Self-Service. The access key is not case sensitive. **c.** Tap **Enter** on the device.
Activation password*	**a.** In the **Email Address** field, type the email address that is in the activation email message that you received from your administrator or type your work email address if you generated your own activation password. **b.** In the **Activation password** field, enter the activation password that is in the activation email message that you received from your administrator or enter the activation password that is generated in the BlackBerry UEM Self-Service. **c.** Tap **Enter** on the device.
QR code	**a.** Tap **Use QR code**. **b.** Tap **Allow** to give the app access the camera. **c.** Scan the QR code in the activation email that you received from your administrator or that you generated in the BlackBerry UEM Self-Service.

* Optionally, you can tap **Advanced Settings** and enter your email address, access key or activation password, and the BlackBerry UEM address.

6. If prompted, create and confirm a password for the app. If your device is equipped with Touch ID, you can turn on this option to use instead of the password, except on initial startup.
7. If prompted, allow the app to use your location history to establish trusted locations.
8. If other devices, including your principal workstation, are also signed in, you will receive a notice advising you of this condition. Tap **OK**.
9. Tap the BlackBerry Dynamics Launcher or tap the screen to start using the app.

Install the apps when the BlackBerry UEM Client or another BlackBerry Dynamics app is already activated on an Android device

You can send the following instructions to Android device users that are installing BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks when the BlackBerry UEM Client or another BlackBerry Dynamics app is already activated on Android device and the app acts as an easy activation delegate.

1. If the app was not automatically pushed to your device by your administrator, open your work apps catalog and download the app. If you do not see the app in your work apps catalog, contact your administrator to make the app available to you.
2. On your device, tap <name of app>.
3. Tap **Client End User License Agreement** to read the license agreement and, if you accept the terms, tap **I Accept**.
4. Tap **Set up using <BlackBerry UEM Client or existing BlackBerry Dynamics app>**.
5. Enter your password for the BlackBerry UEM Client or the existing BlackBerry Dynamics app. Tap **Enter** on the device.
6. If prompted, enter and confirm a new password for the app.
7. If prompted, allow the app to use your location history to establish trusted locations.
8. Tap the BlackBerry Dynamics Launcher or tap the screen to start using the app.

Install and activate the app using an access key, activation password, or QR code on the Android device

You can send the following instructions to Android device users that are installing BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks using an access key, activation password, or QR code.

1. Request an access key, activation password, or QR code from your administrator or generate an access key and QR code from your organization's self-service portal.
2. After you receive the email message with the activation details or have generated your own access key, activation password, or QR code, download and install BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks from Google Play.
3. Tap <name of app>.
4. Tap **Client End User License Agreement** to read the license agreement and, if you accept the terms, tap **I Accept**.
5. Complete one of the following tasks:

Activation method	Steps
Access key*	**a.** In the **Email Address** field, type the email address located in the activation email message that you received from your administrator or type your work email address if you generated your own access key. **b.** In the **Activation password** field, enter the access key, without hyphens, that is in your activation email message that you received from your administrator or enter the access key that you generated from the BlackBerry UEM Self-Service. The access key is not case sensitive. **c.** Tap **Enter** on the device.
Activation password*	**a.** In the **Email Address** field, type the email address that is in the activation email message that you received from your administrator or type your work email address if you generated your own activation password. **b.** In the **Activation password** field, enter the the activation password that is in your activation email message that you received from your administrator or enter the activation password that you generated in the BlackBerry UEM Self-Service. **c.** Tap **Enter** on the device.
QR code	**a.** Tap Use QR code. **b.** Tap **Allow** to give the app access to the camera. **c.** Scan the QR code in the activation email that you received from your administrator or that you generated in the BlackBerry UEM Self-Service.

* Optionally, you can tap **Advanced Settings** and enter your email address, access key or activation password, and the BlackBerry UEM address.

6. Create and confirm a password for the app. If your device is equipped with fingerprint authentication, you can turn on this option to use instead of the password, except on initial startup.
7. If prompted, allow the app to use your location history to establish trusted locations.
8. If other devices, including your principal workstation, are also signed in, you will receive a notice advising you of this condition. Tap **OK**.
9. Tap the BlackBerry Dynamics Launcher or tap the screen to start using the app.

Configure a third-party identity provider for activating BlackBerry Dynamics apps on a device

You can configure a third-party identity provider so that users can sign-in with their directory credentials to activate BlackBerry Dynamics apps on a device. They can also use it to unlock an app or reset their BlackBerry Dynamics app password.

Before you begin: To configure this feature, you need the following:

- BlackBerry Dynamics apps compiled with a supported version of the BlackBerry Dynamics SDK.
- BlackBerry Enterprise Identity is enabled.

1. Configure your organization's third-party identity provider to work with BlackBerry Enterprise Identity.
   - For information about configuring Okta and BlackBerry Enterprise Identity, see the BlackBerry Enterprise Identity Administration Guide. Ensure that the Microsoft Active Directory that your organization's Okta instance uses is also configured in BlackBerry UEM through **Settings > External Integration > Company Directory**.
   - For information about configuring PingFederate and BlackBerry Enterprise Identity, see the BlackBerry Enterprise Identity Administration Guide.
2. Do one of the following:
   - If you are using PingFederate or Okta, enable **Dynamics Activation via Enterprise IDP** as an OpenID Connect app.
   - If you are using Active Directory as the identity provider, add the **Dynamics Active Directory Activation** as an OpenID Connect app.

   For more information, see the BlackBerry Enterprise Identity Administration Guide.
3. In BlackBerry UEM, set up your organization's identity provider. For more information, see the BlackBerry Enterprise Identity Administration Guide PingFederate and Okta instructions.
4. In BlackBerry UEM, create a BlackBerry Enterprise Identity Authentication policy. Ensure you select **Manage service exceptions**, and add the **Dynamics Activation via Enterprise IDP** service. For more information, see the BlackBerry Enterprise Identity Administration Guide.
5. Assign the BlackBerry Enterprise Identity Authentication policy to users. For more information, see the BlackBerry Enterprise Identity Administration Guide.

After you finish:

- During the activation process, users need to select the **Sign in with your organization if instructed by your administrator** option and sign in using your organization's identity provider.
- For more information, see the UEM Client for Android User Guide.

Set up support for Skype for Business

Before you begin:

If you plan to support Skype for Business for calendar and meeting features in BlackBerry Work, you require the following:

- An on-premises Skype for Business Server 2015 and later
- An on-premises Microsoft Exchange server supported by BlackBerry Work. See the Compatibility Matrix for Mobile/Desktop OS and Enterprise Applications for a list of supported Microsoft Exchange servers.
- The Skype for Business client must be installed on devices for users to be able to join meetings from a calendar event.

Before you begin: Also note the following considerations:

- The Skype for Business account and the Microsoft Exchange server must be in the same domain.
- Skype for Business does not support shared calendars.

1. Ensure that the following DNS names are added to the DNS server:
   - lyncdiscoverinternal.<domain>
   - lyncdiscover.<domain>
   - meet.<domain>

   For details, see:
   - https://docs.microsoft.com/en-us/skypeforbusiness/deploy/install/create-dns-records
   - https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/dns
2. Add these FQDN names to the connectivity profile in the Additional Servers section. For details on configuring the connectivity profile, see Configure BlackBerry Work connection settings.
3. Enable Skype for Business in the app configuration for BlackBerry Work. For details, see Configure BlackBerry Work app settings.
   - Select the **Allow to create Skype for Business meetings in calendar** option to allow users to add Skype for Business meetings to their calendars.
   - Select the **Allow launching into Skype for Business app on mobile** option to allow users to make voice and video calls and to be able to join Skype for Business meetings directly from a calendar invitation. The meeting is automatically opened in the Skype for Business client and users must have the Skype for Business client installed on their devices.
   - In the **Domain of Skype for Business meeting link** field, enter the fully qualified domain name or the domain-only portion of the Skype for Business meeting server to allow internal users to use the Join meeting button in the event details. For example, meet.example.com or example.com. By entering this domain name, BlackBerry Work can locate which meeting link to capture from the meeting invitation if it is different from the user's email address domain.

Set up support for the BEMS-Presence service in Non-trusted Application Mode

Before you begin:

If you plan to support the BEMS-Presence service configured for on-premises Skype for Business using Non-trusted Application Mode, you require the following:

- An on-premises Skype for Business Server 2015
- An on-premises Microsoft Exchange server supported by BlackBerry Work. See the Compatibility Matrix for Mobile/Desktop OS and Enterprise Applications for a list of supported Microsoft Exchange servers.
- BEMS 2.10 and later, BEMS-Presence service installed and configured for Skype for Business in non-trusted application mode. For more information, refer to the Configure Microsoft Lync Server 2013 or Skype for Business for the Presence service topic in the BEMS Configuration Guide.

Also note that the Skype for Business account and the Microsoft Exchange server must be in the same domain.

1. Ensure that the following DNS names are added to the DNS server:

   - lyncdiscoverinternal.<domain>
   - lyncdiscover.<domain>

   For details, see:

   - - https://docs.microsoft.com/en-us/skypeforbusiness/deploy/install/create-dns-records
     - https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/dns
2. Add these FQDN names to the connectivity profile in the **Additional Servers** section. For more information on configuring the connectivity profile, see Configure BlackBerry Work connection settings.
3. Ensure BlackBerry Work or BEMS-Presence service entitlements are listed correctly in the Connectivity Profile > App Servers section, and configured to direct to the BEMS-Presence server. For more information, see Setting up network connections for BlackBerry Dynamics apps.
4. In the app configuration for BlackBerry Work, on the App settings tab, in the Presence Service section, select the **Enable presence service** option and choose **Skype for Business On-Prem - Non-trusted Application Mode** in the list. For more information about the app configuration, see Configure BlackBerry Work app settings.

Configure Entra ID conditional access

Before you begin:

- Verify that you have a Microsoft account with an Intune license and with one of the following permissions in the Entra portal: global administrator, limited administrator with the Intune Service administrator role, or a custom role with the permissions described in KB 50341.
- In the Microsoft Endpoint Manager admin center, in the section for Partner Compliance Management, add **BlackBerry UEM Azure Conditional Access** as a compliance partner for iOS and Android devices and assign it to users and groups.
- To use this feature, device users must meet the following requirements:
  - Users must exist in Entra ID and must have a valid Intune license. For more information, see Microsoft Intune licenses.
  - If you synchronize your on-premises Active Directory with Entra ID, users' on-premises Active Directory UPN must match their Entra ID UPN.
  - Users must be added to UEM as directory users.
  - Users must have both the Microsoft Authenticator app and the UEM Client installed on their devices.

1. In the UEM management console, on the menu bar, click **Settings > External integration > Azure Active Directory Conditional Access**.
2. Click +.
3. Type a name for the configuration.
4. In the **Azure cloud** drop-down list, click **GLOBAL**.
5. In the **Azure tenant ID** field, type your organization's tenant name in FQDN format or unique tenant ID in GUID format.
6. Under **Device mapping override**, click **UPN** or **Email**.

   If you choose UPN, verify that the Entra ID tenant and all mapped directories share the same UPN value for users before you save the connection. After you save the connection, you cannot change the device mapping override.
7. In the **Available company directories** list, select and add the appropriate company directories.
8. Click **Save**.
9. Select the administrator account that you want to use to log in to your organization's Entra tenant.
10. Accept the Microsoft permission request.
11. On the menu bar, click **Policies and Profiles > Policy > BlackBerry Dynamics**. Perform the following steps for any BlackBerry Dynamics profile that you plan to assign to device users (for example, the default profile and any custom profiles).
    a) Open and edit the profile.
    b) Select **Enable UEM Client to enroll in BlackBerry Dynamics**.
    c) Click **Save**.
    d) Assign the profile to users and groups as necessary.
12. On the menu bar, click **Policies and Profiles > Networks and Connections > BlackBerry Dynamics connectivity**. Perform the following steps for any BlackBerry Dynamics connectivity profile that you plan to assign to device users (for example, the default profile and any custom profiles).
    a) Open and edit the profile.
    b) In the **App servers** section, click **Add**.
    c) Search for and click **Feature - Azure Conditional Access**.
    d) Click **Save**.

e) In the **Azure Conditional Access** table, click +.
f) In the **Server** field, type `gdas-<UEM_SRP_ID>.<region_code>.bbsecure.com`.
g) In the **Port** field, type 443.
h) Under **Route type**, click **Direct**.
i) Click **Save**.
j) Assign the profile to users and groups as necessary.

13. Assign the **Feature – Azure Conditional Access** app to users or groups. For more information, see Manage user accounts and Manage a user group.

After you finish:

- When a user activates their device, they are prompted to register with Active Directory conditional access. Users with activated devices are prompted to register with Active Directory conditional access the next time they open the UEM Client.
- When you remove a device from UEM, the device remains registered for Entra ID conditional access. Users can remove their Entra ID account from the account settings in the Microsoft Authenticator app, or you can remove the device from the Entra portal.

Configure the BlackBerry Work app configuration for Entra ID Conditional Access

After you configure BlackBerry UEM as a compliance partner for Entra ID Conditional Access, you must set up the BlackBerry Work app configuration to invoke the workflows that register the device with Microsoft Intune for Entra ID conditional access.

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 on the name of the app configuration.
4. On the **Advanced Configuration** tab, select the **Use Office 365 Settings** and **Use Office 365 Modern Authentication** options.
5. On the **Beta Features** tab, select the **Use Office 365 Brokered Authentication** option.
6. Click **Save**.

After you finish: Set up redirect URIs as outlined in Obtain an Entra app ID for BlackBerry Work.

Configuring email classifications

You create email classifications by editing the .xml file on the Classification tab in the BlackBerry Work app configuration as described in Configure BlackBerry Work app settings.

When a user forwards or replies to an email message with classifications, BlackBerry Work maintains the classifications and allows the user to change them if allowed. Classifications can be added to the email Subject end, email TopBody, and email BottomBody, and classifications can be parsed from the email Subject end and email TopBody.

If you are using BlackBerry Work 2.18 or later, you can create up to nine levels of classification. Levels can be configured as follows:

- Levels can use multiple choice values. You can customize these values, including setting a value as the default or ordering them in a specific way.
- Levels can have different parameters that determine how they are used or actions that occur when the value is selected. For example,you can specify a level as required.
- Levels can have a relation between them. For example, a choice made in one level can disable to enable values in other levels.

To see an example of a multi-level email classification xml configuration, see Email classification sample .

If you are using versions of BlackBerry Work that are earlier than 2.18, two levels of classifications are supported (Classifications and Caveats). Classifications can be added to the subject, email TopBody and email BottomBody, but classifications can only be parsed from the email Subject.

Email classifications XML element reference

Element	Description	Allowable values	Default value
multilevelEnabled	This value states whether multi-level support is turned on. Allowable values are Yes or No.	Yes No	
listSeparator	This is value separates multiselect values in classification strings. Default – when this is not defined it is		„/”
classificationSource	This value defines the source of parsing classifications in incoming emails.		tailSubject
levelId	This value defines the level number and order of levels in Classification selection menu.	1 to 9	
LevelState	This value defines the state of the level.	Required Enabled Disabled	

Element	Description	Allowable values	Default value
DefaultItem	This value defines the default value for the item.		
DowngradeAllowed	This value defines whether the user can downgrade this classification.	Yes No	
LevelTitle	This value defines the value that is displayed in UX		
bodyPrefix	This is added before values in classification string.		
bodyPostfix	This is added after values in classification string.		
SubjectPostfix	This value defines the subject value.		

Email classification sample

The following is a sample multilevel configuration. In this configuration, the organization is using 6 levels of classification:

```
<emailClassificationMarks>
        <options>
           <multilevelEnabled>yes</multilevelEnabled>
           <listSeparator> / </listSeparator>
           <classificationSource>topBody</classificationSource>
           <classifications>ON</classifications>
           <classificationDefault>Public</classificationDefault>
           <caveats>ON</caveats>
           <caveatDefault>Private</caveatDefault>
         </options>
          <classifications>
            <classification>
              <select>Public</select>
              <subject>[Public]</subject>
              <topBody>Classification: Public</topBody>
            </classification>
            <classification>
               <select>Privileged</select>
               <subject>[Privileged]</subject>
               <topBody>Classification: Privileged</topBody>
             </classification>
             <classification>
               <select>Confidential</select>
               <subject>[Confidential]</subject>
               <topBody>Classification: Confidential</topBody>
             </classification>
             <classification>
               <select>Secret</select>
```

```
              <subject>[Secret]</subject>
              <topBody>Classification: Secret</topBody>
            </classification>
        </classifications>
       <caveats>
         <caveat>
           <select>Private</select>
           <subject>[Private]</subject>
           <topBody>Ownership: Private</topBody>
         </caveat>
         <caveat>
           <select>Company</select>
           <subject>[Company]</subject>
           <topBody>Ownership: Company</topBody>
         </caveat>
       </caveats>
        <levels>
<!-- Level 1 – The following level is titled – “Classification:” It is set as
 mandatory, is configured as a single select, and after it has been set, it cannot
 be downgraded when replying or forwarding to this email message. This level can
 have following values : Public, Privileged, Confidential, Secret. -->
           <level>
              <levelId>1</levelId>
              <level-options>
                 <levelState>required</levelState>
                 <defaultItem>Public</defaultItem>
                 <downgradeAllowed>no</downgradeAllowed>
                 <levelTitle>Classification</levelTitle>
                 <bodyPrefix>Classification: </bodyPrefix>
                 <bodyPostfix></bodyPostfix>
                 <subjectPostfix></subjectPostfix>
              </level-options>
              <items>
                 <item>
                    <select>Public</select>
                    <subject>[Public]</subject>
                    <topBody>Public</topBody>
                    <itemId>1</itemId>
                 </item>
                 <item>
                    <select>Privileged</select>
                    <subject>[Privileged]</subject>
                    <topBody>Privileged</topBody>
                    <itemId>2</itemId>
                 </item>
                 <item>
                    <select>Confidential</select>
                    <subject>[Confidential]</subject>
                    <topBody>Confidential</topBody>
                    <itemId>3</itemId>
                 </item>
                 <item>
                    <select>Secret</select>
                    <subject>[Secret]</subject>
                    <topBody>Secret</topBody>
                    <itemId>4</itemId>
                 </item>
              </items>
           </level>
           <level>
```

```
<!-- Level 2. This level is titled “Ownership” It is configured as a single select
 and after it has been set, it cannot be downgraded when replying or forwarding to
 this email message. This level have following values : Private, Company. -->
              <levelId>2</levelId>
              <level-options>
                 <defaultItem>Private</defaultItem>
                 <downgradeAllowed>no</downgradeAllowed>
                 <levelTitle>Ownership</levelTitle>
                 <bodyPrefix> Ownership: </bodyPrefix>
                 <bodyPostfix></bodyPostfix>
                 <subjectPrefix> </subjectPrefix>
                 <subjectPostfix></subjectPostfix>
              </level-options>
              <items>
                 <item>
                    <select>Private</select>
                    <subject>[Private]</subject>
                    <topBody>Private</topBody>
                    <itemId>1</itemId>
                 </item>
                 <item>
                    <select>Company</select>
                    <subject>[Company]</subject>
                    <topBody>Company</topBody>
                    <itemId>2</itemId>
                 </item>
              </items>
           </level>
           <level>
<!-- Level 3 This level is titled “Releasability”.  Is is configured as a single
 select and is not mandatory.This level have following values : Internal ,
 External, Partners, Suppliers, and has suffix “Only”. -->
              <levelId>3</levelId>
              <level-options>
                 <defaultItem>Internal</defaultItem>
                 <levelTitle>Releasability</levelTitle>
                 <bodyPrefix>, Releaseability </bodyPrefix>
                 <bodyPostfix> Only</bodyPostfix>
                 <subjectPrefix></subjectPrefix>
                 <subjectPostfix></subjectPostfix>
              </level-options>
              <items>
                 <item>
                    <select>Internal</select>
                    <subject>[Internal]</subject>
                    <topBody>Internal</topBody>
                    <itemId>1</itemId>
                 </item>
                 <item>
                    <select>External</select>
                    <subject>[External]</subject>
                    <topBody>External</topBody>
                    <itemId>2</itemId>
                 </item>
                 <item>
                    <select>Partners</select>
                    <subject>[Partners]</subject>
                    <topBody>Partners</topBody>
                    <itemId>3</itemId>
                 </item>
                 <item>
```

```
                  <select>Suppliers</select>
                  <subject>[Suppliers]</subject>
                  <topBody>Suppliers</topBody>
<!-- Level 4. This level is disabled if "Internal” was selected in level 3. This
 level is active if any other option is selected in level 3.This level is titled
 “Available for”. It is a multi-select level and has the following values :
 Europe, APAC, Russia, Brazil, US and Canada, China, Latin America, All. -->
                  <itemId>4</itemId>
               </item>
            </items>
         </level>
         <level>
            <levelId>4</levelId>
            <level-options>
               <multipleSelect>yes</multipleSelect>
               <levelTitle>Available for</levelTitle>
               <bodyPrefix>&#10;Available for </bodyPrefix>
               <bodyPostfix></bodyPostfix>
               <subjectPrefix> [</subjectPrefix>
               <subjectPostfix>]</subjectPostfix>
               <enableList>
                  <enableForLevelId>3</enableForLevelId>
                  <enableForItems>
                     <enableForItemId>2</enableForItemId>
                     <enableForItemId>3</enableForItemId>
                     <enableForItemId>4</enableForItemId>
                  </enableForItems>
               </enableList>
                     </level-options>
            <items>
               <item>
                  <select>Europe</select>
                  <subject>Europe</subject>
                  <topBody>Europe</topBody>
                  <itemId>1</itemId>
               </item>
               <item>
                  <select>APAC</select>
                  <subject>APAC</subject>
                  <topBody>APAC</topBody>
                  <itemId>2</itemId>
               </item>
               <item>
                  <select>Russia</select>
                  <subject>Russia</subject>
                  <topBody>Russia</topBody>
                  <itemId>3</itemId>
               </item>
               <item>
                  <select>Brazil</select>
                  <subject>Brazil</subject>
                  <topBody>Brazil</topBody>
                  <itemId>4</itemId>
               </item>
               <item>
                  <select>US and Canada</select>
                  <subject>US and Canada</subject>
                  <topBody>US and Canada</topBody>
                  <itemId>5</itemId>
               </item>
               <item>
```

```
                  <select>China</select>
                  <subject>China</subject>
                  <topBody>China</topBody>
                  <itemId>6</itemId>
               </item>
               <item>
                  <select>Latin America</select>
                  <subject>Latin America</subject>
                  <topBody>Latin America</topBody>
                  <itemId>7</itemId>
               </item>
            </items>
         </level>
         <level>
<!--  Level 5. This level has no title and is optional. This level have following
 values: Limited, Not Limited -->
            <levelId>5</levelId>
            <level-options>
               <bodyPrefix> </bodyPrefix>
            </level-options>
            <items>
               <item>
                  <select>Limited</select>
                  <subject>Limited</subject>
                  <topBody>Limited</topBody>
                  <itemId>1</itemId>
               </item>
               <item>
                  <select>Not Limited</select>
                  <subject>Not Limited</subject>
                  <topBody>Not Limited</topBody>
                  <itemId>2</itemId>
               </item>
             </items>
         </level>
         <level>
<!--  Level 6 This level is titled : “Administrative Markings” and is optional.
 It is a multi-select level and has the following values: COMMERCIAL, BUSINESS,
 MANAGEMENT, MEDICAL, HR , MARKETING. -->
            <levelId>6</levelId>
            <level-options>
                  <multipleSelect>yes</multipleSelect>
               <levelTitle>Administrative Markings</levelTitle>
               <bodyPrefix>&#10;Administrative Markings: </bodyPrefix>
               <bodyPostfix></bodyPostfix>
               <subjectPrefix> [</subjectPrefix>
               <subjectPostfix>]</subjectPostfix>
            </level-options>
            <items>
               <item>
                  <select>None</select>
                  <subject>None</subject>
                  <topBody>None</topBody>
                  <itemId>1</itemId>
               </item>
               <item>
                  <select>COMMERCIAL</select>
                  <subject>COMMERCIAL</subject>
                  <topBody>COMMERCIAL</topBody>
                  <itemId>2</itemId>
               </item>
```

```
                <item>
                   <select>BUSINESS</select>
                   <subject>BUSINESS</subject>
                   <topBody>BUSINESS</topBody>
                   <itemId>3</itemId>
                </item>
                <item>
                   <select>MANAGEMENT</select>
                   <subject>MANAGEMENT</subject>
                   <topBody>MANAGEMENT</topBody>
                   <itemId>4</itemId>
                </item>
                <item>
                   <select>MEDICAL</select>
                   <subject>MEDICAL</subject>
                   <topBody>MEDICAL</topBody>
                   <itemId>5</itemId>
                </item>
                <item>
                   <select>HR</select>
                   <subject>HR</subject>
                   <topBody>HR</topBody>
                   <itemId>6</itemId>
                </item>
                <item>
                   <select>MARKETING</select>
                   <subject>MARKETING</subject>
                   <topBody>MARKETING</topBody>
                   <itemId>7</itemId>
                </item>
             </items>
          </level>
       </levels>
    </emailClassificationMarks>
```

Troubleshooting

Diagnostics

If a user is reporting an issue, you can ask them to perform app diagnostics.

You can use diagnostic tools to check the connection between BlackBerry Access and BlackBerry Proxy and other target servers.

BlackBerry Access for iOS also has a “Collect network summary” option that you can use to collect and display a summary of your internet usage. The summary, which can be used for diagnostics, displays information such as delays in connections, authentication handshakes, and proxy resolution.

Generate a diagnostics report on iOS devices

You can ask users to generate a diagnostics report and then email the results.

Before you begin: Provide the following instructions to users:

1. Tap to open the BlackBerry Dynamics Launcher.
2. Tap .
3. In the Support section, tap **Run Diagnostics**.
4. Tap **Start Diagnostic**.
5. Click **Start**.
6. When the diagnostics complete, click **Share logs** to send an email with the report details.

Generate a diagnostics report on Android devices

You can ask users to generate a diagnostics report and then email the results.

Before you begin: Provide the following instructions to users:

1. Tap to open the BlackBerry Dynamics Launcher.
2. Tap .
3. In the Support section, tap **Run Diagnostics**.
4. Tap **Start Diagnostics**.
5. When the diagnostics complete, click **Share Results** to send an email with the report details.

Upload log files to BlackBerry Support

If requested by BlackBerry Support, you can upload log files to help troubleshoot issues that your users are having with BlackBerry Dynamics apps.

Provide the following instructions to users:

1. Tap to open the BlackBerry Dynamics Launcher.
2. Tap .
3. In the **Support** section, click **Logs**.
4. Click **Upload Logs**.

Monitoring the performance of the BlackBerry Work app

You can monitor the performance of the BlackBerry Work app and choose the issues that you want to be reported.

Enable BlackBerry Work monitoring

To enable BlackBerry Work monitoring, you must configure the app configuration that is assigned to it.

1. On the menu bar, click **Apps**.
2. Click the BlackBerry Work app that you want to monitor.
3. On the BlackBerry Dynamics tab, in the App configuration table, click the name of the app configuration that you want to edit.
4. On the **Performance Reporting** tab, configure any of the following:
   - **Enable Performance Reporting**: Specify whether to monitor performance of the BlackBerry Work app.
   - **HTTP Connection Error**: Specify whether to report HTTP connection errors between BlackBerry Work and the specified application servers.
   - **HTTP Response Time**: Specify whether to report HTTP responses that are taking longer than the specified time. Enter the application server addresses to monitor.
   - **HTTP Status Code**: Specify whether to report a specified HTTP status code. Enter the application server addresses to monitor.
   - **Don't send reports for duration (in seconds)**: Specify the amount of time to wait before sending another report.
5. Click **Save**.

View device performance alert notifications

Before you begin:

- Enable BlackBerry Work monitoring

1. On the menu bar, click **Audit and logging** > **Device performance**.
2. Choose a category and date range. Click **Submit**.
3. Under **Filters**, click a category to expand it.
4. Select the filters that you want to apply and click **Submit**.
5. If necessary, do one of the following:
   - To remove a filter, click ✕ beside the filter that you want to remove.
   - To clear all filters, click **Clear all**.
6. To export the results to a .csv file, click  .

View a performance alert for a single device

Instead of viewing a list of performance alerts based on date and alert type, you can also view all of the performance alerts for a single device in the last 24 hours. If there are performance alerts for a device, a caution icon appears on the device tab and a message is displayed that tells you how many alerts have been detected on the device.

Before you begin:

- Enable BlackBerry Work monitoring

1. On the menu bar, click **Users > Managed devices**.

2. Search for a user account.
3. In the search results, click the name of the user account.
4. Select the device tab for the device that you want to view alerts for. A device with performance alerts or compliance violations is flagged with a caution icon.
5. If there are performance alerts for the device, click **View all** beside the performance alert message to view the list of performance alerts for that device.

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada