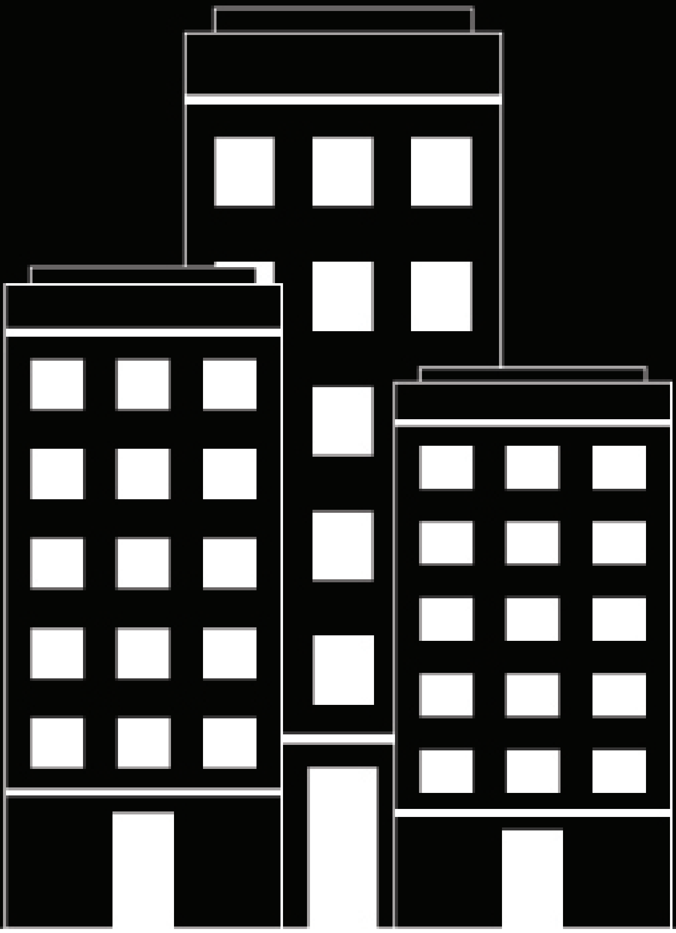

BlackBerry Work, Notes, and Tasks

Administration Guide

3.2

Contents

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

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.

Feature	Description
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 Notes and BlackBerry Tasks 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 version 12.6 MR1 and later • BlackBerry Enterprise Mobility Server version 2.4 and later
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. Refer to 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 in the Administration content.

Downloading BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks

Users can download the latest version of these apps for each device type from the following locations:

Platform	Download location
For 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 Google Play store. Users require an access key to activate these apps.
For iOS devices	• For MDM managed devices, 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. Users require an access key to activate these apps.

Managing BlackBerry Work

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 the BlackBerry UEM administration content.

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:

- Update the app list.
- To allow users to install and activate BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks on their devices, assign them to user accounts or user groups.

Update the app list

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

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 2013 and 2016) environment: Make sure that the autodiscover URL routes to the latest version of the CAS servers (for example, the Microsoft Exchange Server 2016).
- 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.outlook.com). On the DNS admin portal, make sure a CNAME record is created

and that it redirects https://autodiscover.<*mydomain*>/autodiscover/autodiscover.xml to https://autodiscover.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.

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 app configuration settings for a description of all of the settings that you can configure.
7. Click **Save**.

app configuration settings

App Settings tab	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.

App Settings tab	Description
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.
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.
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, Skype for Business On-prem using trusted application mode, or Skype for Business Online. **Note:** If you want to configure Skype for Business Online, you must configure the Office 365 Settings on the Advanced Configuration tab. • 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.

App Settings tab	Description
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.
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 tab	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 (Android only): 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 tab	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.
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 tab	Description
Apple Watch app	Select the "Enable BlackBerry Workapp 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
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.

S/MIME tab	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.
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.
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.
Certificate Management	Specify when to clear the public certificate cache. By default, this setting is Weekly.

S/MIME tab	Description
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 tab	Description
Address Book Sync	Select the "Allow syncing BlackBerry Contacts to device" option to synchronize 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.
Caller ID (BETA)	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."

Interoperability	Description
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 (iOS only)	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 and file-based provisioning using BlackBerry Access, as well as CTF-based provisioning using a nativeRSA SecurID app. For more information about configuring RSA soft-token authentication and provisioning the token seed record your organization sends to users, see the BlackBerry Access Administration Guide.
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

Interoperability	Description
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. Select the "Enable Importing from 3rd-party native apps (iOS 12 and below and Android)" 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. Note that exceptions to importing apply only to iOS. Select 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.
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.

Docs and Attachments tab	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.
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 tab	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.

Basic Configurationtab	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.

Basic Configurationtab	Description
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.
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.

Basic Configurationtab	Description
Advanced Settings	Specify additional configuration parameters in this text area. Contact BlackBerry Support for more details.

Advanced Configuration tab	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.
Background Authorization (iOS only)	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 tab	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.
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 tab	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 Azure App ID field, specify the Microsoft Azure app ID for BlackBerry Work. For information on how obtain an Azure ID, see Obtain an Azure app ID for BlackBerry Work. • 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. If you do not specify a value, a value of "common" is used. • In the "Office 365 Resource" field, specify the URL of the Microsoft Exchange Online server. • In the Redirect URI field, specify the URI that you entered in the Microsoft Azure portal. • In 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 Presenceservice. The "Enable presence service" option must also be selected. • In the "Office 365 Presence Resource" field, enter the app ID for your Presenceservice. For more information about how to get an app ID for your Presence service, see Obtain an Azure app ID for the Connect, Presence, and Docs component 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

Performance Reporting tab	Description
Enable Performance Reporting	Select this option, to specify whether to monitor performance of the BlackBerry Work app.

Performance Reporting tab	Description
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.

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).

Deprecated tab	Description
Exchange ActiveSync 16.0 Protocol (Moved to the Deprecated tab)	If supported by your Microsoft Exchange server, specify whether to use Exchange ActiveSync version 16 for synchronization between Microsoft Exchange and BlackBerry Work version 2.14 or earlier. **Note:** This setting must be enabled if you want to allow users to be able to synchronize their Drafts folder to BlackBerry Work version 2.14 or earlier. For more information on how to synchronize the Drafts folder, visit support.blackberry.com/community to read article 50339. **Note:** This policy does not apply to BlackBerry Work version 2.15 or later as this version will automatically upgrade to Exchange ActiveSync version 16 if supported by your organization's Microsoft Exchange server. After upgrading to BlackBerry Work version 2.15, users will see a message that tells them that BlackBerry Work must resynchronize with their Microsoft Exchange server. Documents stored in Local Docs and user preferences are retained and are not impacted. After the resynchronization completes, users will be able to synchronize their Drafts folder to BlackBerry Work.
Security Settings	Select the "Disable SSL Cetificate Checking" option to disable SSL Certificate verification for Exchange ActiveSync/Microsoft Exchange Web Services in test environments.

Obtain an Azure app ID for BlackBerry Work

If you are configuring Office 365 settings in the app configuration for BlackBerry Work, you may need to obtain and copy the Azure app ID for BlackBerry Work. If you need to obtain multiple Azure app IDs (for example, Docs, BEMS, and BlackBerry Connect), it is recommended that you create a separate app ID for each app.

1. Log on to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for the app. This is the name that users will see.
6. Select a supported account type.
7. In the **Redirect URI** drop-down list, select **Public client (mobile & desktop)** and enter `com.blackberry.work://connect/o365/redirect`
8. Click **Register**.
9. In the **Manage** section, click **API permissions**.
10. Click **Add a permission**.
11. In the **Select an API** section, click the **Microsoft APIs** tab.
12. Complete one or more of the following tasks:

Environment	Permissions
If your environment is configured to use Microsoft Office 365	**a.** Click **Microsoft Graph**. If Microsoft Graph is not listed, add Microsoft Graph. **b.** Set the following permissions: • 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**) **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**.
If your environment is configured to use Microsoft Exchange Online for email	**a.** Click the **Exchange**. **b.** Set the following permissions: • In delegated permissions, select **Access mailboxes as the signed-in user via Exchange Web Services** checkbox (**EWS > EWS.AccessAsUser.All**). **c.** Click **Add permissions**.
If your environment is configured for Microsoft Exchange Online and uses Skype for Business Online for meetings	**a.** Click **Skype for Business**. **b.** Select all delegated permissions. **1.** Click **Delegated permissions**. **2.** Click **expand all**. Make sure that all options are selected. **c.** Click **Add permissions**.
If your environment is configured to use Microsoft SharePoint Online or Azure-IP to enable modern authentication for the BlackBerry Work client	**a.** Click the **APIs my organization uses** tab. **b.** Search for and click the BEMS app that you created in Obtain an Azure app ID for the BEMS-Connect, BEMS-Presence, and BEMS-Docs component service. For example, AzureAppIDforBEMS. **c.** Select all delegated permissions. **1.** Click **Delegated permissions**. **2.** Click **expand all**. Make sure that all options are selected. **d.** Click **Add permissions**.

13. Click **Grant admin consent for <Organization name>** to apply the permissions for the app. These settings will not be applied to the app until you have granted the updated permissions.
14. Click **Yes**.
15. You can now copy the Application ID for the app that you created. In the **Manage** section, click **Overview**. It is located under the name of the app, in the Application (client) ID field.

Allow 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 (iOS only)** , 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**.

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 in the BlackBerry Work administration content.

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**.

Set up support for creating and joining Skype for Business meetings

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 2010, Microsoft Lync Server 2013, Skype for Business, or Skype for Business Online for the Presence service topic in the BEMS Configuration Guide.

Before you begin: Also note the following considerations:

- 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 the Setting up network connections for BlackBerry Dynamics apps topic in the *BlackBerry UEM Administration Guide*.
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 the Configure BlackBerry Work app settings topic.

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.

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, 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. In the **Server** field, specify the FQDN of the Exchange ActiveSync server.
4. In the **Port** field, specify the port for the Exchange ActiveSync server. By default, the port number is 443.
5. In the **Primary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the primary cluster.
6. In the **Secondary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster
7. Click **Save**.
8. 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. Click **Save**. For more information about the Use heritage settings option, see 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**.

Configuration	Tasks
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**.

9. In the table for the app, click +.
10. In the **Server** field, specify the FQDN of the BlackBerry Enterprise Mobility Server.
11. 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.
12. In the **Priority** drop-down list, specify the priority of the BlackBerry Proxy cluster that must be used to reach the domain.
13. In the **Primary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the primary cluster.
14. In the **Secondary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
15. Click **Save**.
16. Click **Add** or **Save**.
17. 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.

    a) Assign the app directly by completing one of the following tasks:

    - 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. Complete one of the following tasks:
        - Assign the app group to a user group
        - Assign the app group to a user account

Configure BlackBerry Notes and BlackBerry Tasks 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 "Use explicit UPN" property. This requires BlackBerry UEM 12.11 or later. For more information, see the BlackBerry UEM Configuration content.

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 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. If you do not specify a value, a value of "common" is used.

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

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 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**.

Obtain an Azure app ID for BlackBerry Tasks and BlackBerry Notes

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

1. Log on to portal.azure.com.
2. In the left column, click **Azure Active Directory**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for BlackBerry Tasks. This is the name that users will see.
6. Select a supported account type.
7. In the **Redirect URI** drop-down list, select **Public client (mobile & desktop)**and enter `com.blackberry.work://connect/o365/redirect`
8. Click **Register**.
9. In the **Manage** section, click **API permissions**.
10. Click **Add a permission**.
11. In the **Select an API** section, click the **Microsoft APIs** tab.
12. If your environment is using Office 365 Exchange Online, set the following permissions:
    - Delegated permissions: Access mailboxes as the signed-in user via Exchange Web Services (**EWS > EWS.AccessAsUser.All**)
13. Click **Add permissions**.
14. Click **Grant Permissions** to apply the permissions for the app. These settings will not be applied to the app until you have granted the updated permissions.
15. Click **Yes**.
    You can now copy the Application ID for the app that you created for BlackBerry Tasks. In the **Manage** section, click **Overview**. It is located under the name of the app, in the Application (client) ID field. Repeat the steps for BlackBerry Notes.

Options for 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 the BlackBerry UEM administration content. for steps on how to configure your environment to support BlackBerry Dynamics apps.

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

- Install and activate the apps using the BlackBerry UEM Client: This option provides users with a consistent, streamlined activation experience. Users need only their email address and an activation password and do not require an access key. Users must install the UEM Client to activate their devices with MDM. For this option to be available to users, you must allow the UEM Client to manage the activation of BlackBerry Dynamics apps.
- Install and activate the apps using an activation key: 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 using the UEM Client on iOS devices

You can send the following instructions to iOS device users that are installing BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks using the BlackBerry UEM Client.

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 apps. 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 the name of the app to install.
3. Click **Allow** to allow the app to send notifications.
4. Tap **Set up using BlackBerry UEM Client**.
5. Enter your password for the UEM Client.
6. Wait while the activation completes and then click **I agree** to accept the license agreement.

Install and activate the apps using an access key on iOS devices

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

1. Use the access key that was provided by your administrator or generate an access key from your organization's self-service portal.
2. After you receive the email message with the access key information or have generated your own access key, download and install BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks from the App Store.
3. Open the app that you want to install.
4. 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.
5. In the **Access Key** 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 from the self-service portal. The access key is not case sensitive.

6. 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. Read the license agreement and, if you accept the terms, tap **Accept**.
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 in the lower-right of the screen to start using the app.

Install the apps using the UEM Client on Android devices

You can send the following instructions to Android device users that are installing BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks using the BlackBerry UEM Client.

1. If the app was not automatically pushed to your device by your administrator, open your work apps catalog and download the BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks apps. If you do not see the BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks app in your work apps catalog, contact your administrator to make the app available to you.
2. On your device, tap the app that you want to install.
3. Click **Allow** to allow the app to send notifications.
4. Tap **Set up using BlackBerry UEM Client**.
5. Enter your password for the UEM Client.
6. Wait while the activation completes and then click **I agree** to accept the license agreement.

Install BlackBerry Work and activate using an access key on Android devices

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

1. Request an access key from your administrator or generate an access key from your organization's self-service portal.
2. After you receive the email message with the access key information or have generated your own access key, download and install BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks from Google Play.
3. Open the app that you want to install.
4. 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.
5. In the **Access Key** 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 from the self-service portal. The access key is not case sensitive.
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. Read the license agreement and, if you accept the terms, tap **Accept**.
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 in the lower-right of the screen to start using the app.

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>
```

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 Administration Guide.
- Ensure that your organization’s app configuration is set up for Modern Authentication, Microsoft Exchange Online endpoints (Exchange ActiveSync, Exchange Web Services) and Autodiscover. For more information, see the Administration Guide, and the Modern Authentication Guide.

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. o set an expiry time, enter a date in the **Migration Flow Expiration Date** field. After the date that you enter has passed, the Migration Flow Enabled setting is ignored.
6. Click **Save**.

7. Assign the new app configuration to users who will be migrated to Microsoft Exchange Online. If you are migrating users in batches, assign the new configuration prior to migrating users.

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

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

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

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

Troubleshooting mailbox migration

After the mailbox migration is complete, if some of your organization's users encounter any issues such as the Azure 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.

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.

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