BlackBerry Enterprise Mobility Server

Configuring BlackBerry Push Notifications

3.9

Contents

BlackBerry Mail (BEMS Push Notifications service)

The BlackBerry Mail service accepts push registration requests from devices, such as iOS and Android, and then communicates with the Microsoft Exchange Server using its Microsoft Exchange Web Services protocol to monitor the user's enterprise mailbox for changes. When you configure BEMS for Push Notifications support of the BlackBerry Work app, which includes mail, contacts, and calendar, you perform the following actions:

- Configure the Mail service in the BEMS dashboard
- Optionally, configure the Push Notifications service for high availability

Steps to configure Push Notifications

When you configure the Mail service, you perform the following actions:

Important: Complete the configuration in the following order to avoid connectivity issues.

Step	Action
1	Configure the database.
2	Configure the Microsoft Exchange Server.
3	Optionally, configure Microsoft Graph.
4	Configure stop notifications.
5	Configure user Directory Lookup.
6	Configure the certificate Directory Lookup.
7	Optionally, configure the Active Directory password expiry settings.

Configure the Microsoft SQL Server database for Push Notifications service

If the Mail service is installed on separate computers, but uses the same database name, this task needs to be completed only once.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Mail**.
2. Click **Database**.
3. In the **Server** field, verify the SQL Server host name and instance. This field is prepopulated with the information you provided during the BEMS installation. The SQL Server must be in the following format: <*SQLServer_hostname*>\<*instance_name*>.

If you configured the database for an AlwaysOn Availability Group, set the server to the AlwaysOn Listener FQDN. Do not use the cluster name or host name of the server in the cluster.

4. In the **Database** field, verify the database name. For example, BEMS-Core.

   If you configured the database for an AlwaysOn Availability Group, set the database to the name of the database added to the AlwaysOn Availability Group.

5. In the **Authentication Type** drop-down list, complete one of the following tasks:

   - If you select **Windows Authentication**, the Push Notifications service uses the Windows credentials to access the Microsoft SQL Server database.
   - If you select **SQL Server Login**, type the username and password used to access the SQL Server database.

6. By default, the "encrypt=false" property is prepopulated in the Additional properties field, so data between the BEMS and the SQL Server is not encrypted. Existing properties that you have configured are retained. If your environment requires data to be encrypted, and requires verification of the TLS certificate, complete the following:

   Note: If you enable encryption for all data that is sent between BEMS and the SQL Server, it may cause higher than normal CPU usage.

   a. Import the CA certificate that is signing your SQL Server certificate into the Java certificate store. For more information, see Import the CA certificate into the Java certificate store.
   b. Change the encrypt property to true and add trustServerCertificate=false separated by a semicolon (no space before or after the semicolon).

   If your organization uses AlwaysOn support for SQL Server, type `MultiSubnetFailover=true`.

7. Click **Test**.
8. Click **Save**.
9. Restart the Good Technology Common Services service in the Windows Services Manager.

Best practice: Enabling autodiscovery

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

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

Note: All autodiscover URLs must be whitelisted on BlackBerry UEM. For more information on how to use third-party tools to test autodiscover, see KB 40351.

Configure BEMS to communicate with a Microsoft Exchange Online environment using Microsoft Graph API

Before BEMS can send email notifications to users' devices, it must subscribe to changes on a user's mailbox. You can configure BEMS to subscribe to mailboxes using Microsoft Graph API. Microsoft Graph push notifications are sent (or pushed) from Microsoft 365 to the reverse proxy server to the BEMS instance. BEMS then accesses the user's mailbox and sends email notifications to the user's device. For more information, see Architecture: BEMS notification flow using the Microsoft Graph API. BEMS subscribes to the Microsoft Graph API change notifications using webhooks. You can configure BEMS to use the Microsoft Graph API in the following scenarios:

- Your BEMS is configured to use modern authentication.
- Your BEMS connects with Microsoft Exchange Online mailboxes.

If you have an existing BEMS instance that is configured to use Microsoft Exchange Web Services (EWS) for Exchange Online to access Microsoft 365 mailboxes, when you enable "Use Microsoft Graph", BEMS will automatically migrate all Microsoft 365 users from using EWS to Microsoft Graph at a rate of 50 users every 5 minutes.

For information on configuring email notifications for BlackBerry Work using BEMS Cloud, see the BlackBerry Work Administration content.

Before you begin: Verify that you obtained the following:

- If you use Client secret authentication: Obtain a copy of the key **Value**. This is used as the **Client Secret**. For instructions, see Obtain an Entra app ID for BEMS with client secret authentication.
- If you use Client certificate authentication:
  - Obtain a copy of the **Application (client) ID**. This is used as the **Client Application ID**.
  - Request and export a .pfx certificate with the Entra app ID for BEMS
- In environments where the metadata endpoint is protected by mutual TLS authentication, make sure that you imported the mutual TLS certificate into the BEMS keystore. For instructions, see Import the trusted mutual TLS certificates into the BEMS keystore.

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

Authentication type	Description	Task
Client Certificate	This option uses a client certificate to allow the BEMS service account to authenticate to Microsoft Exchange Online.	**a.** For the **Upload PFX file**, click **Choose File** and select the client certificate file. For instructions on obtaining the .PFX file, see Associate a certificate with the Entra app ID for BEMS **b.** In the **Enter PFX file Password** field, enter the password for the client certificate.

Authentication type	Description	Task
Client Secret	This option uses a client secret to allow the BEMS service account to authenticate to Microsoft Exchange Online. The client secret is created during the application registration process.	In the **Client Secret** field, enter the Client secret Value.

5. In the **Authentication Authority** field, enter the Authentication Server URL that BEMS accesses and retrieve the OAuth token for authentication with Microsoft Exchange Online. The authentication server URL must be in the format of https://login.microsoftonline.com/*tenantname* or https://login.microsoftonline.com/*tenantid*.
6. In the **Client Application ID** field, enter the Entra app.
7. In the **Server Name** field, enter the FQDN of the Microsoft Graph server. By default, the field is prepopulated with https://graph.microsoft.com
8. In the **External Notification URL** field, enter the URL that your IT provided. Enter https://<*BEMS_server_name*:*port*>/notificationClient (for example, bems.example.com:443/notificationClient). The External Notification URL is an externally routable address, such as a reverse proxy, where Graph will send the notifications. For more information, see the Port requirements in the BEMS Installation content.
9. In the **End User Email Address** field, type an email address to test connectivity to Microsoft Exchange Online using the service account. Click **Test**. You can delete the email address after you complete the test.
10. Click **Save**.
11. Configure the Autodiscover and Exchange Options. For instructions see one of the following:
    - In on-premises BEMS environment: see Configure BEMS to communicate with the Microsoft Exchange Server, Microsoft Exchange Online, or hybrid environment. This environment supports Credential, Credentials + Modern Authentication, and Client Certificate + Modern authentication types.
    - In a Microsoft Exchange Online and hybrid Microsoft Exchange Online environments: see Configure BEMS to communicate with a Microsoft 365 environment using Microsoft Graph API. This environment supports Client and Client Certificate +Modern authentication types.

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

- Subject
- Issuer
- Validation period
- Serial number

Obtain an Entra app ID for BEMS with client secret authentication

1. Sign in to entra.microsoft.com.
2. In the left column, click **Applications > App registrations**.
3. Click **New registration**.
4. In the **Name** field, enter a name for the app.
5. Select a supported account type.
6. Click **Register**.
7. In the **Manage** section, click **API permissions**.
8. Click **Add a permission**.
9. Click **Microsoft Graph**.

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

      The Contacts.ReadWrite permission is only required if you require the Contact Service API to use third-party apps to query, retrieve, create, and update contact information from a user's contact folder. For more information, see the Contact Service API reference content.
11. Click **Add permissions**.
12. Click **Grant admin consent**. Click **Yes**.
13. Add a client secret.
    a) In the **Manage** section, click **Certificates & secrets**.
    b) Click **New client secret**.
    c) In the **Description** field, enter a key description up to a maximum of 16 characters, including spaces.
    d) Set an expiration date.
    e) Click **Add**.
    f) Copy the key **Value**.

       Important: The Value is available only when you create it. You cannot access it after you leave the page. This is used as the **Client secret** in the BEMS Dashboard when you enable Microsoft Exchange Online and configure BEMS to communicate with Microsoft Exchange Online.

Configure BEMS to communicate with the Microsoft Exchange Server, Microsoft Exchange Online, or hybrid environment

If your BEMS environment uses Microsoft Graph to communicate with Microsoft Exchange Online, see Configure BEMS to communicate with a Microsoft Exchange Online environment using Microsoft Graph API. You must allow BEMS to authenticate to Microsoft Exchange Server or Microsoft Exchange Online to access users' mailboxes and send notifications to users' devices when new email is received on the device. A hybrid modern authentication environment (for example, both on-premises Microsoft Exchange Server and Microsoft Exchange Online), allows the on-premises Microsoft Exchange Server to use a more secure user authentication and authorization by consuming OAuth access tokens obtained from the cloud. For more information, see the Microsoft resource How to configure Exchange Server on-premises to use Hybrid Modern Authentication.

Note: For information on configuring email notifications for BlackBerry Work using BEMS Cloud, see the BlackBerry Work administration content.

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

- In an on-premises Microsoft Exchange Server environment: Verify that the service account has impersonation rights on the Microsoft Exchange Server. For instructions, see "Grant application impersonation permission to the BEMS service account" in the Installation content.
- In a Microsoft Exchange Online environment, verify that you have enabled Modern Authentication using a Client Certificate.
  - Obtain the Client Application ID with certificate based authentication
  - Request and associate the .pfx certificate with the Entra app ID for BEMS

  In environments where the metadata endpoint is protected by mutual TLS authentication, make sure that you imported the mutual TLS certificate into the BEMS keystore. For instructions, see Import the trusted mutual TLS certificates into the BEMS keystore. This feature requires that you enable modern authentication using a Credential or Client Certificate.
- In a hybrid environment, if you enable Modern Authentication, make sure that the on-premises Microsoft Exchange Server is configured to use hybrid modern authentication. For more information, see the Microsoft

resource How to configure Exchange Server on-premises to use Hybrid Modern Authentication. If the Microsoft Exchange Server is not configured appropriately, users won't receive email notifications.

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

   Note: The Passive authentication type has been deprecated due to Microsoft's deprecation of the Application Impersonation permission in Microsoft Exchange Online environments. To avoid email notifications interruptions for users in the environment, you must configure BEMS to use certificate-based authentication for modern authentication, or Microsoft Graph to communicate to user's mailboxes. The passive authentication type will be removed in a future release. For more information, see BEMS: Customers using Office 365 and EWS with Credential or Passive Authentication will stop receiving notifications.

Authentication type	Environment	Description	Task
Integrated	On-premises Microsoft Exchange Server	This option uses the Windows authentication credentials Good Technology Common Services service to authenticate to the Microsoft Exchange Server using Basic Authentication.	No additional actions are required.
Credential	On-premises Microsoft Exchange Server	This option uses a defined BEMS username and password to authenticate to the Microsoft Exchange Server using Basic Authentication.	**a.** In the **Username** field, enter the username of the BEMS service account. Use the format <*domain*>/<*username*>. **b.** In the **Password** field, enter the password for the service account.

Authentication type	Environment	Description	Task
Client Certificate	• On-premises Microsoft Exchange Server • Microsoft Exchange Online • In a hybrid environment, on-premises Microsoft Exchange Server must be configured to use hybrid modern authentication. For more information, see the Microsoft resource How to configure Exchange Server on-premises to use Hybrid Modern Authentication.	This option uses a client certificate to allow the BEMS service account to authenticate to the Microsoft Exchange Server or Microsoft Exchange Online.	**a.** For the **Upload PFX** file, click **Choose File** and select the client certificate file. For instructions on obtaining the .PFX file, see Associate a certificate with the Entra app ID for BEMS. **b.** In the **Enter PFX file Password** field, enter the password for the client certificate.

4. In a Microsoft Exchange Online environment that uses Client certificate authentication, enable Modern Authentication and use mutual TLS authentication. When you configure Modern Authentication, all nodes use the specified configuration. Note that the "use Credentials if Modern authentication fails" option has been deprecated due to Microsoft's deprecation of the Application Impersonation permission for users' mailboxes that are on Microsoft Exchange Online, enabled for modern authentication, and configured to use credential or passive authentication methods. The option will be removed in a future release. For more information, see BEMS: Customers using Office 365 and EWS with Credential or Passive Authentication will stop receiving notifications. Complete the following steps:
   a) Select the **Enable Modern Authentication** checkbox.
   b) In the **Authentication Authority** field, enter the Authentication Server URL that BEMS accesses and retrieve the OAuth token for authentication with Microsoft Exchange Online (for example, https://login.microsoftonline.com/<tenantname> or https://login.microsoftonline.com/<*tenantid*>). By default, the field is prepopulated with https:// login.microsoftonline.com/common.
   c) In the **Client Application ID** field, enter the Entra app ID. For instructions, see Obtain an Entra app ID for BEMS with certificate-based authentication.
   d) In the **Server Name** field, enter the FQDN of the Microsoft Exchange Online. By default, the field is prepopulated with https://outlook.office365.com.
   e) Optionally, select the **Use Mutual TLS Authentication** check box to allow BEMS to respond to mutual TLS authentication requests. This step requires that the mutual TLS certificate is imported into BEMS. For instructions, see Import the trusted mutual TLS certificates into the BEMS keystore.
5. Under the **Autodiscover and Exchange Options** section, complete one of the following actions:

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

6. In the **End User Email Address** field, type an email address to test connectivity to the Microsoft Exchange Server or Microsoft Exchange Online using the service account. Click **Test**. You can delete the email address after you complete the test.

If the service account is correctly configured and the test fails, BEMS is attempting to communicate with a Microsoft Exchange Server that is not using a trusted SSL Certificate. If your Microsoft Exchange Server is not set up to use a trusted SSL certificate, see "Importing CA certificates for BEMS" in the BEM-Core content.

7. Click **Save**.

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

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

1. Sign in to entra.microsoft.com.
2. In the left column, click **Applications > App registrations**.
3. Click **New registration**.
4. In the **Name** field, enter a name for the app.
5. Select a supported account type.
6. Click **Register**. The new registered app appears.
7. In the **Manage** section, click **API permissions**.
8. Click **Add a permission**.
9. In the **Select an API** section, click **APIs my organization uses**.
10. Search for and click **Office 365 Exchange Online**.
11. Click **Application permission** and select the **full_access_as_app** (Use Exchange Web Service with full access to all mailboxes) permission.
12. Click **Add permissions**.
13. In the **Configured permissions** section, click **Microsoft Graph**.
14. Click **Application permissions** and select the following permissions:
    - **Contacts.ReadWrite** (Have full access to user contacts)
    - **Mail.Read** (Read user mail)
    - **User.Read.All** (Read all users' full profiles)
15. Click **Add permissions**.
16. Click **Grant admin consent**.
17. Click **Yes**.
18. Click **Overview** to view the app that you created in step 5. Copy the **Application (client) ID**. The Application (client) ID is displayed in the main **Overview** page for the specified app. This is used as the **Client application ID** in the BEMS dashboard when you enable modern authentication and configure BEMS to communicate with Microsoft Exchange Online.

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

Associate a certificate with the Entra app ID for BEMS

You can request and export a new client certificate from your CA server or use a self-signed certificate. The private key must be in .pfx format to upload to the BEMS dashboard. The public key can be exported as a .cer or .pem file to upload to Microsoft Entra ID. For more information, see 'Enable modern authentication for the Mail service in BEMS' in the Microsoft Exchange Online and hybrid Microsoft Exchange Online environments Modern Authentication for BlackBerry Dynamics apps content.

1. Complete one of the following tasks:

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

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

2. Upload the public certificate (.pem or .cer file) that you exported in step 1 to associate the certificate credentials with the Entra app ID for BEMS.

a) In entra.microsoft.com, open the <*app name*> you assigned the app in step 5 of Obtain an Entra app ID for BEMS with certificate-based authentication.

b) Click **Certificates & secrets**.
c) In the **Certificates** section, click **Upload certificate**.
d) In the **Select a file** search field, navigate to the location where you exported the certificate in step 1.
e) Click **Add**.

Import the trusted mutual TLS certificates into the BEMS keystore

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

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

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

Configure Stop Notifications

By default, notifications are sent to a user's device and are regulated by timers. The Stop Notifications feature allows you to immediately stop notification for all devices associated with a particular user. A user can resubscribe to notifications, but only if the user is entitled to an app that can subscribe to notification services.

Before you begin: If you want to stop notifications for multiple users, verify that you have a .csv file that includes all of the users' email addresses.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Mail**.
2. Click **Stop Notifications**.
3. Complete one of the following:

Notifications	Steps
Stop notifications for a single user.	**a.** In the **Stop Notifications** section, select **Single user**. **b.** In the **User Email Address** field, type the email address of the user you want to stop notifications for. **c.** Click **Save**.

Notifications	Steps
Stop notifications for multiple users.	**a.** In the **Stop Notifications** section, select **Multiple users.** **b.** Click **Choose File**. Navigate to and select the .csv file that contains the users' email addresses. **c.** Click **Save**. **d.** Verify that the .csv file content uploaded successfully. Click **Get Results**. Resolve any errors that might be identified. **e.** Click **Save**.

4. Click **Save**.

After you finish: Users can resubscribe by completing one of the following actions:

- BlackBerry Work for iOS users: Force quit the app and reopen it.
- BlackBerry Work for Android users: Restart the Android device and the app will re-register with BEMS.

Configure User Directory Lookup

The User Directory Lookup service allows client apps to look up first name, last name, and the associated photo or avatar from your company directory. A User ID Property Name determines whether query results from various sources, such as Microsoft Exchange Web Services (EWS) and LDAP, correspond to the same user and may therefore be consolidated into a single result.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Mail**.
2. Click **User Directory Lookup**.
3. In the **User ID Property Name** field, type the name of the property that identifies the user. By default, this is "Alias".
4. Select the **Enable GAL Lookup** checkbox, the **Enable LDAP Lookup** checkbox, or both.
5. If you enable LDAP lookup, you can use it to validate digital certificate connections to the LDAP server.
   a) In the **LDAP Server Name** field, type the name of the LDAP Server. For example, ldap.<*DNS_domain_name*>.
   b) In the **LDAP Server port** field, type the port number of the LDAP Server. By default, the port number is 389.
   c) Optionally, select the **Enable SSL LDAP** checkbox to tunnel data through an SSL-encrypted connection. If you enable SSL LDAP, the port number defaults to 636. This step requires you to import the LDAP certificate chain into the BEMS dashboard. For more information, see "Upload the SSL certificate to the BEMS database" in the BEMS-Core configuration content.
   d) Optionally, edit the **LDAP User Name Query Template** field. The LDAP user name query searches for a user by their user name. BEMS replaces the "{key}" with the user name when performing the query. By default, the template is

```
 (&(|(mail=*{key}*)(name=*{key}*)(displayName=*{key}*)
(sAMAccountName=*{key}*) (givenName=*{key}*)(sn=*{key}*))(objectClass=user)
(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
```

   e) Optionally, in the **LDAP Base DN** field, provide a base DN for the LDAP search. If this field is not completed, BEMS tries to find the base DN in the namingContexts attribute.
   f) In the **Authentication Type** drop-down list, select an authentication type. By default the Authentication Type is Anonymous.
      - If you select **Basic**, enter the LDAP Logon User name and password. In a Microsoft Active Directory environment, enter the username in the format **domain\username** or User Principal Name (UPN) **username@domain**.

- If you selected the **Enable SSL LDAP** checkbox, and select **Certificate** authentication, enter the keystore password and add the certificate file.

g) Optionally, specify the timeout before the BEMS connection attempt to the LDAP server times out. In the **LDAP Connection Timeout** field, increase or decrease the value, in seconds, as required. The default value is 30 seconds. You can specify between zero and 300 seconds.
h) Optionally, specify the timeout before the BEMS search for users from your organization's Global Address List and their password expiry details times out. In the **LDAP Search Timeout** field, increase or decrease the value, in seconds, as required. The default value is 30 seconds. You can specify between zero and 300 seconds.
i) In the **User search key** field, type a username or email address to search for.
j) Click **Test**.

6. Click **Save**.

Configure the Certificate Directory Lookup

The Certificate Directory Lookup service retrieves S/MIME digital certificates from the user's Microsoft Active Directory. These certificates enable email encryption and signature functionality in BlackBerry Work apps. For more information about configuring and using S/MIME on devices, see the BlackBerry Work Tasks, and Notes Administration Guide.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Mail**.
2. Click **Certificate Directory Lookup**.
3. Optionally, select the **Include expired certificates in results** checkbox.
4. By default, the **Enable Contact Lookup** checkbox and **Enable GAL Lookup** checkbox are selected. If you clear the **Enable GAL Lookup** checkbox, users can't send encrypted email messages to public distribution lists and private or personal distribution lists (for example, distribution lists in the user's contact folder).
5. Optionally, select the **Enable LDAP Lookup** checkbox to use LDAP lookup to validate digital certificate connections to the LDAP server.
   a) In the **LDAP Server Name** field, type the name of the LDAP Server. For example, ldap.<*DNS_domain_name*>.
   b) In the **LDAP Server port** field, type the port number of the LDAP Server. By default, the port number is 389.
   c) Optionally, select the **Enable SSL LDAP** checkbox to tunnel data through an SSL-encrypted connection. If you enable SSL LDAP, the port number defaults to 636. This step requires you to import the LDAP certificate chain into the BEMS dashboard. For instructions, see "Upload the SSL certificate to the BEMS database" in the BEMS-Core configuration content.
   d) Optionally, edit the **LDAP User Name Query Template** field. The LDAP user name query searches for a user by their user name. BEMS replaces the "{key}" with the user name when performing the query. The default template is

```
(&(|(mail=*{key}*)(name=*{key}*)(displayName=*{key}*)(sAMAccountName=*{key}*)
 (givenName=*{key}*)(sn=*{key}*))(objectClass=user)(objectCategory=person)(!
(userAccountControl:1.2.840.113556.1.4.803:=2)))
```

   e) Optionally, in the **LDAP Base DN** field, provide a base DN for the LDAP search. BEMS will try to find the base DN in the namingContexts attribute if this entry is not set. If this field is not completed, BEMS tries to find the base DN in the namingContexts attribute.
   f) In the **Authentication Type** drop-down list, select an authentication type. By default, the Authentication Type is Anonymous.
      - If you select **Basic**, enter the LDAP Logon User name and password. In a Microsoft Active Directory environment, enter the username in the format **domain\username** or User Principal Name (UPN) **username@domain**.

- If you selected the **Enable SSL LDAP** checkbox and select **Client Certificate** authentication, enter the keystore password and certificate file.

g) Optionally, specify the timeout before the BEMS connection attempt to the LDAP server times out. In the **LDAP Connection Timeout** field, increase or decrease the value, in seconds, as required. The default value is 30 seconds. You can specify between zero and 300 seconds.
h) Optionally, specify the timeout before the BEMS search for users and their S/MIME digital certificates from the users' Active Directory times out. In the **LDAP Search Timeout** field, increase or decrease the value, in seconds, as required. The default value is 30 seconds. You can specify between zero and 300 seconds.
i) In the **End User Email Address** field, type an end-user email address to search for.
j) Click **Test**.

6. Click **Save**.

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

- Subject
- Issuer
- Validation period
- Serial number

Configure the password expiration warning message

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

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

Before you begin:

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

1. Complete one of the following tasks:

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

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

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

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

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

Changing users' SMTP addresses

BEMS supports changing users' SMTP addresses without requiring the user to provision their BlackBerry Work app. Previously, if a user changed their primary email address the user needed to reprovision their BlackBerry Work app if they missed email notifications and notifications for email marked as VIP, were unable to access repositories using BlackBerry Work Docs, or could not change other settings on their device. BEMS now detects the primary SMTP address change and updates the BEMS database with the new SMTP address automatically.

Set the detailed Notifications Cutoff Time

If BlackBerry Work has not been unlocked and actively used on a device after a specified time, the BEMS Push Notifications service removes details about individual email messages from Notifications that are displayed on the device. Message details in Notifications sent by the BEMS Push Notifications service resumes the next time BlackBerry Work is unlocked and used on the device.

1. Open a browser and go to the Apache Karaf Web Console Configuration web site located at `https://<fqdn_of_the_bems_host>:8443/system/console/configMgr` and login as administrator with the appropriate Microsoft Active Directory credentials.
2. On the menu, click **OSGi > Configuration**.
3. Click **com.good.server.notifications.vip.service.CoalescingPushServiceImpl.name**.
4. In the **com.good.server.notifications.vip.service.CoalescingPushServiceImpl.pushDowngradeCutoffSec.name** field, increase or decrease the value, in seconds, as required. The default value is 172800 seconds or 48 hours. The maximum value is 259200 seconds, or 3 days.
5. Click **Save**.
6. Repeat the previous steps on each BEMS instance in your environment.

Configuring the Push Notifications service for high availability

High availability for the Push Notifications service is based on clustering. The Push Notifications service supports high availability by adding additional servers running Push Notifications. The BEMS instances that host the Push Notifications services that you designate to participate in high availability must share the same database. If a BEMS instance is unavailable, other instances in the high availability environment perform a check approximately every minute to verify whether all of the instances are available. If a BEMS instance is offline, users are distributed among the available instances. Consider the following scenario:

Your BEMS environment is configured for high availability and includes four BEMS instances which support 10000 users. BEMS_name1 is taken offline for maintenance. The other BEMS instances routinely perform a search of available BEMS.

- If the BEMS instance is available, the log files display the instance with a state of GOOD:

```
<YYYY-MM-DD>T14:16:59.385-0500 CEF:1 | pushnotify-ha-dbwatcher | pushnotify-
ha-dbwatcher | 0.13.21 | INFO | unknown | 5 | ID=297 THR=DbWatcher-0
 CAT=ProducerTasksRunner MSG=Worker BEMS_name1 is in state GOOD with 1/10000
 users (0.01% capacity). Last status was updated at "<YYYY-MM-DD> T19:16:59.359
 UTC". FeatureSet:AgingStaleUser, RichPush, VIPNotification, apnsPayload2k,
 badgeCount, subFolderNotification, pushSettings, smimeCertificateLookup,
 soundSettings, badgeCount2, autodiscover, notificationsSettings,
 localizedPush, delayWriteSyncState, RightToDisconnect, FCMRelayService updated
 at "1532523850857"
```

- If the BEMS instance is unavailable, the log files display the instance with a state of BAD and users are distributed as required. In the following log example, two BEMS instances, BEMS_name1 and BEMS_name2, are checked and the BEMS_name1 instance that is unavailable is flagged as BAD.

```
<YYYY-MM-DD>T14:42:33.874+0100 CEF:1 | pushnotify-ha-comm | pushnotify-ha-comm
 | 0.15.3 | INFO | unknown | 5 | ID=309 THR=DbWatcher-0 CAT=HaProducerImpl
 MSG=BAD!! Last known status of HaWorker "BEMS_name1" is "<YYYY-MM-
DD>T10:45:47.831 UTC". It is before cut-off time "<YYYY-MM-DD> T13:37:33.860
 UTC"

<YYYY-MM-DD>T14:42:33.874+0100 CEF:1 | pushnotify-ha-dbwatcher | pushnotify-
ha-dbwatcher | 0.15.3 | INFO | unknown | 5 | ID=310 THR=DbWatcher-0
 CAT=ProducerTasksRunner MSG=Got status of 2 workers

<YYYY-MM-DD>T14:42:33.874+0100 CEF:1 | pushnotify-ha-dbwatcher | pushnotify-
ha-dbwatcher | 0.15.3 | INFO | unknown | 5 | ID=310 THR=DbWatcher-0
 CAT=ProducerTasksRunner MSG=Worker BEMS_name2 is in state GOOD with 359/10000
 users (3.59% capacity). Last status was updated at "<YYYY-MM-DD> T13:42:33.693
 UTC". FeatureSet:AgingStaleUser, RichPush, VIPNotification, apnsPayload2k,
 badgeCount, subFolderNotification, pushSettings, smimeCertificateLookup,
 soundSettings, badgeCount2, autodiscover, notificationsSettings,
 localizedPush, delayWriteSyncState, RightToDisconnect, FCMRelayService,
 Delegate updated at "1545046557729"

<YYYY-MM-DD>T14:42:33.875+0100 CEF:1 | pushnotify-ha-dbwatcher | pushnotify-
ha-dbwatcher | 0.15.3 | INFO | unknown | 5 | ID=310 THR=DbWatcher-0
 CAT=ProducerTasksRunner MSG=Worker BEMS_name2 is idle 359/10000 (3.59%
 capacity)

<YYYY-MM-DD>T14:42:33.875+0100 CEF:1 | pushnotify-ha-dbwatcher | pushnotify-
ha-dbwatcher | 0.15.3 | INFO | unknown | 5 | ID=310 THR=DbWatcher-0
```

```
CAT=ProducerTasksRunner MSG=Worker BEMS_name1 is in state BAD with 0 users.
Last status was updated at "<YYYY-MM-DD> T10:45:47.831 UTC"
```

When you configure the Push Notifications service for high availability, you complete the following actions:

1. During the installation of additional Push Notifications service instances, on the Database Information screen specify the same database for each instance. For example, BEMS-Core.
2. Configure the BlackBerry Work connection settings. For instructions, see "Configure BlackBerry Work connection settings" in the BlackBerry Work, Notes, and Tasks Administration content. If you have the Mail service installed on multiple computers, repeat this step for each computer that hosts the service.

Disaster recovery

You can configure your BEMS environment so that it continues to function in the event of a severe disruption. For more information about disaster recovery for BEMS, see the Disaster recovery content.

Troubleshooting the BlackBerry Mail (Push Notification Service)

The Mail service log files contain diagnostic information to assist in troubleshooting and monitoring the service. For information about the location of the Mail service logs and to view relevant logs, see the BEMS Monitoring and reporting content.

Next steps

After you complete the tasks to configure the Mail (Push Notifications) service, see to the following guides to configure the necessary services and install and configure BlackBerry Dynamics apps:

- Configure BlackBerry UEM for BlackBerry Work. The BlackBerry Work app integrates all your business collaboration and keeps the organization's data secure. The app allows users to stay on top of work email and calendar, view online presence, manage contacts and easily work on documents. To support the BlackBerry Work app in your environment, configure the application. For information, see the BlackBerry Work Administration content.
- BlackBerry Docs service: This service lets your BlackBerry Dynamics app users access, synchronize, and share documents using their work file server, SharePoint, Box, and content management systems supporting CMIS, without the need for VPN software, firewall reconfiguration, or duplicate data stores. For more information, see the BlackBerry Docs service.
- BlackBerry Connect service: This service provides secure instant messaging, company directory lookup, and user presence information to iOS and Android devices.
- BlackBerry Presence service: This service provides real-time presence status to BlackBerry Work, BlackBerry Dynamics Launcher, and third-party BlackBerry Dynamics apps. For more information.

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada