BlackBerry Enterprise Mobility Server

Configuring BEMS-Core

3.9

Contents

BEMS Core service

BEMS Core provides the core functionality of BEMS. When you configure the core settings, you configure the shared settings for all of the BEMS services (for example, certificates, specifying custom BlackBerry Dynamics Launcher icons, and specifying database settings). You configure the core components in the BEMS Dashboard under the BEMS System Settings. For more configuration information for other BEMS services, see the appropriate service guide.

Steps to configure the BEMS-Core

When you configure BEMS-Core, you perform the following actions. If you installed the BEMS services on multiple computers, you must complete these tasks once for each cluster.

Step	Action
1	Install CA certificates.
2	Install the BEMS SSL certificate.
3	Add dashboard administrators.
4	Configure the BlackBerry Dynamics server in BEMS.
5	Configure Web Proxy.
6	Optionally, enable log file compression.
7	Configure Firebase Push Notifications.
8	Optionally, enable FIPS Mode.

Importing CA Certificates for BEMS

By default, BEMS is only aware of public CA certificates. If BEMS must communicate with a server that does not have a certificate issued by a public Certificate Authority (CA), then you must import the non-public CA root certificate from the server's certificate chain into the BEMS host Java keystore or BEMS database using the Dashboard. In this section, non-public CA certificates refers to a certificate that is not trusted by BEMS. BEMS may connect to the following servers in your environment:

- Microsoft Exchange Server
- Active Directory Federation Service (ADFS)
- BlackBerry Proxy
- Microsoft SharePoint
- Microsoft Office Web Apps
- Microsoft Office Online Server
- Microsoft SQL Server
- Microsoft Active Directory using LDAP/LDAPS

You can import the server's SSL certificates (or the root or intermediate certificate chain) to BEMS using the following methods:

- The BEMS Dashboard
- The Java keytool

Create a trusted connection with Microsoft Exchange and other servers that BEMS must communicate with

By default, BEMS is only aware of public CA certificates. If you enable email notifications for BlackBerry Work and your organization's Microsoft Exchange Server doesn't use an SSL certificate issued by a trusted CA, the connection between your BEMS instance and Microsoft Exchange Server isn't trusted. To create a trusted connection to the Microsoft Exchange Server upload the server's SSL certificates (or the root or intermediate certificate chain) to the BEMS database. You can upload a base64-encoded or binary-encoded file that includes one or more SSL certificates. BEMS verifies the validity of the certificates. If the certificate is revoked or its signature cannot be verified, the upload fails. When you upload a single file that includes multiple SSL certificates, the certificates are displayed in the dashboard and can be deleted and replaced individually as required. BEMS supports the following file extensions: .der, .cer, .pem, and .crt. For information about creating a .pem file that includes multiple certificates, see KB 57259. You import the certificates using one of the following methods:

- Upload the SSL certificate from Microsoft Exchange to the BEMS Dashboard
- Import the CA certificates into the JAVA certificate store

Upload the SSL certificate to the BEMS database

Before you begin:

- Make sure that the BEMS-Mail (Push Notifications) service is installed and configured in your environment.
- If you upload the Microsoft Exchange Server certificate, export the SSL certificate from the Microsoft Exchange Server in a base64-encoded or binary-encoded format and store it in a network location that you can access from the management console. For more information, see the Microsoft resource Digital certificates and encryption in Exchange Server

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **BEMS Configuration**.

2. Click **Upload Trust Certificate**.
3. Click **Choose File** and navigate to the location of the certificate file that you want to upload.
4. Click **Add**.
5. If you upload individual SSL certificates, repeat steps 3 and 4 for each additional file.

Replace or delete the trusted connection SSL certificates

When you replace the SSL certificate (for example, when the certificate expires), you replace the existing SSL certificates in the BEMS database. You can chose to upload individual SSL certificates or include multiple SSL certificates in a single file. If you uploaded a single file that includes multiple SSL certificates, the certificates are listed in the management console and can be removed individually. The following file types are supported: .der, .cer, .pem, and .crt.

Before you begin: Export the new SSL certificates from the Microsoft Exchange Server in a base64-encoded or binary-encoded format and store it in a network location that you can access from the management console. For more information, see the Microsoft resource Digital certificates and encryption in Exchange Server.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **BEMS Configuration**.
2. Click **Upload Trust Certificate**.
3. In the **Certificate Information** section, select the **Delete** checkbox beside each certificate that you want to delete. Click **Delete**.
4. Add the new certificate files as required. For instructions, see Create a trusted connection with Microsoft Exchange and other servers that BEMS must communicate with.

Import the CA certificate into the Java certificate store

You can use the following steps to import certificate authority certificates into the Java cacerts keystore as an alternative to uploading certificate authority certificates into the BEMS database using the Dashboard. Some BEMS features may not support verifying certificate trusts using certificates stored in the database (for example, the Presence service for on-premises Skype for Business using non-trusted application mode). If you use this method to import the CA certificate, you must complete the following steps on each BEMS instance in the cluster.

Before you begin: Save a copy of the exported certificate to a convenient location on the computer that hosts BEMS (for example, C:\bemscert). For instructions, see Export the BlackBerry Proxy CA certificate chain to your desktop.

1. If necessary, verify the Java bin directory is correctly specified in your environment PATH.
   a) In a command prompt, type `set | findstr "JAVA_HOME"`.
   b) Press **Enter**.
   c) In the command prompt, type `set | findstr "Path"`
   d) Press **Enter**.

   Verify that the JAVA_HOME System variable is set to the correct Java directory and that the PATH System variable includes the path to the same Java directory. For instructions about setting the JAVA_HOME and PATH system variables, see 'Set an environment variable for the Java location' in the installation content.
2. Obtain a copy of the non-public CA certificate and any necessary intermediate certificates from the server that BEMS must communicate with. For more information, contact your administrator of the servers that BEMS needs to have trusted SSL connections to.
3. On the BEMS host, make a backup of the Java keystore file. The Java keystore file is located at `%JAVA_HOME%\lib\security\cacerts`, where JAVA_HOME is confirmed in Step 1.

4. Copy the non-public CA certificate to a convenient location on the computer that hosts BEMS (for example, C:\bemscert).
5. Open a command prompt and change directory to the Java_HOME folder (for example, type `cd %JAVA_HOME%`).
6. Import the root certificate. Consider the following guidelines:
   - The -alias value must be unique in the destination keystore. If it is duplicated, you might experience import errors. You can output the cacerts keystore to a text file to manually confirm the existing certificates using a text editor. Type **keytool.exe -list -v -keystore lib\security\cacerts > c:\bemscert\cacertsoutput.txt**
   - Where the -file value is the path and the file name of the non-public certificate. If this is the path to the file, add quotation marks (" ") around the full path, filename, and extension.
   - The following is an example of importing the certificate using keystore commands: `keytool.exe -importcert -trustcacerts -file "c:\bemscert\cacert1.cer" -keystore lib\security\cacerts -alias myalias1 -storepass changeit`
   - There are no spaces between the dash (-) and the parameter name.
   - You must specify the -keystore parameter correctly. If it is incorrect or it is omitted, the keytool creates a new keystore. BEMS services do not use the new keystore.

   For more information about keystore commands, see Keystore commands.
7. Repeat step 6 for any additional certificates that you want to import into the Java keystore.
8. If you have Connect installed and configured, and did not import the BlackBerry Proxy root certificate into the Windows keystore, import it now. For instructions, see Import the BlackBerry Proxy CA certificate to the BEMS Windows keystore.
9. In the Windows Service Manager, restart the Good Technology Common Services service.

After you finish: Configure the Core BEMS service for communicating to BlackBerry Dynamics. For instructions, see Configure the BlackBerry Dynamics server in BEMS.

Importing and configuring certificates

Consider the following when you import certificates:

- If you want to replace the BEMS auto-generated SSL certificate, import a new SSL certificate.
- Import the BlackBerry Proxy and the BlackBerry UEM certificate chains into the BEMS Java keystore.
- If necessary, assign the BEMS SSL certificate to users using a CA certificate profile.

Replacing the autogenerated SSL certificate

By default, BEMS is remotely accessible using HTTPS only. During installation, a BEMS Java keystore called bems.pfx is created and located in `<drive>\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<version>\etc\keystores\`. If you previously replaced the self-signed certificate, then your existing certificate and certificate password are retained. You can replace the previously self-signed certificate using a SAN certificate or a Wildcard server certificate and assign the certificate to be used by all nodes in a cluster. When you replace the previously self-signed certificate with a SAN or Wildcard server certificate, makes sure that the certificate is trusted by all BlackBerry Dynamics apps that communicate with BEMS on port 8443. For instructions, see Assign the BEMS SSL certificate to users.

When you replace the auto-generated SSL certificate, you perform one of the following actions based on your organization's needs:

Environment	Action
One BEMS instance	Upload and replace the auto-generated SSL certificate with a SAN or Wildcard certificate and assign the certificate for use by all nodes in the cluster.
Multiple BEMS instances that share a cluster certificate.	Upload and replace the auto-generated SSL certificate with a SAN or Wildcard certificate and assign the certificate for use by all nodes in the cluster.
Multiple BEMS instances and each instance requires an independent certificate that is issued by a certificate authority.	Upload and replace the auto-generated SSL certificate with a self-signed certificate for a single node.

Steps to replace the autogenerated SSL certificate with a SAN or wildcard certificate for use by all nodes in a cluster

When you replace the autogenerated SSL certificate and assign the same certificate to all BEMS nodes in a cluster, you perform the following actions:

Step	Action
1	Create a SAN certificate or wildcard certificate and save it to your desktop. **Note:** If you create a SAN certificate, it must include all of the BEMS nodes's FQDNs in the Subject Alternative Names property.

Step	Action
2	Upload and replace the self-signed BEMS SSL certificate with a SAN or wildcard certificate for use by all nodes in a cluster.
3	In a BlackBerry UEM environment, Assign the BEMS SSL certificate to users.

Upload and replace the self-signed BEMS SSL certificate with a SAN or wildcard certificate for use by all nodes in a cluster

You can replace all of the self-signed SSL certificates with a SAN certificate or wildcard certificate using the BEMS dashboard (for example, when the certificates expire). The BEMS Dashboard can upload the SSL certificate to each BEMS node and enable the certificate to be used by all nodes in the cluster. The certificate file type must have a .pfx or .p12 extension. If you imported the certificate manually prior to upgrading BEMS, BEMS continues to use the previous certificate.

Before you begin: Verify that you obtained a SAN or wildcard certificate. Make sure that you know the password for the certificate file.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **SSL Certificate**.
2. In the **Upload SSL Certificate** section, click **Choose File**.
3. Navigate to the certificate file that you want to upload. Click **Open**.
4. In the **Password** field, enter the password for the certificate.
5. Select the **Use the uploaded Server SSL Certificate for all nodes in the cluster** check box. The BEMS Dashboard logs you out and all of the nodes in the cluster use the same certificate.

   Note: If this is the first time that you upload a certificate, this check box displays after the password is entered.

Steps to replace the autogenerated SSL certificate for one BEMS node

When you replace the autogenerated SSL certificate for one BEMS node, you perform the following actions.

Note: The browser may report that your SSL certificate is untrusted if you replace the BEMS self-signed certificate with another self-signed certificate.

Steps	Action
1	If you need to obtain a signed certificate for BEMS, Create a new keystore, generate a CSR request, and obtain a signed certificate from a CA.
2	If you have an existing certificate (.pfx), Import a previously issued certificate using a .pfx file
3	Move the certificate into the BEMS keystore.
4	Update the certificate passwords in BEMS.

Steps	Action
5	Assign the BEMS SSL certificate to users.

Create a new keystore, generate a CSR request, and obtain a signed certificate from a CA

1. If necessary, verify that the PATH system variable includes the path to the Java bin directory.
   a) In a command prompt, type `set | findstr "Path"`.
   b) Press **Enter**.

   For instructions to set the Path system variable, see "Set an environment variable for the Java location" in the installation content.
2. On the computer that hosts BEMS, create a temporary folder (for example, `C:\bemscert`).
3. Create a new Java keystore and key pair.
   a) Open a command prompt.
   b) Navigate to the folder that you created in step 1.
   c) Type `keytool -genkeypair -alias serverkey -keyalg RSA -keystore bemsnew.pfx -storetype PKCS12 -keysize 2048 -dname "CN=<FQDN of BEMS host>, OU=<BEMS name>, O=<domain>, L=<location>, S=<state or province>, C=<country>" -validity <number of days before the certificate expires> -storepass <mystorepassword>`.

   For example, `keytool -genkeypair -alias serverkey -keyalg RSA -keystore bemsnew.pfx -storetype PKCS12 -keysize 2048 -dname "CN=BEMShost.example.net, OU=BEMShost, O=example, L=Waterloo, S=Ontario, C=CA" -validity 730 -storepass mystorepasssword`

   For more information about keystore commands, see Keystore commands.
   d) Press **Enter**.
   e) Type a password for the serverkey certificate's private key. To set the serverkey password to be the same as the keystore password, press **Enter**.
   f) Optionally, to view the contents of the certificate before you submit it to a CA, type `keytool -list -v -keystore bemsnew.pfx -storetype PKCS12 -storepass <mystorepassword>`
4. Generate a CSR for the BEMS Java keystore. In the command prompt, type `keytool -certreq -alias serverkey -file bemsnewcert.csr -keystore bemsnew.pfx -storetype PKCS12 -storepass <mystorepassword> -keypass <mykeypassword>`

   If the serverkey password and the keystore password are the same, type `keytool -certreq -alias serverkey -file bemsnewcert.csr -keystore bemsnew.pfx -storetype PKCS12 -storepass <mystorepassword> -keypass <mystorepassword>`
5. Submit the CSR to a CA.
6. Receive the CA-signed certificate from the CA and save it to the folder that you created in step 1.
7. Import the CA-signed certificate to the request. In the command prompt, type `keytool -importcert -keystore bemsnew.pfx -storetype PKCS12 -storepass <mystorepassword> -file <"certificate filename received in step 5"> -alias serverkey`

   For example, `keytool -importcert -keystore bemsnew.pfx -storetype PKCS12 -storepass mystorepassword -file "bemsnew certnew.cer" -alias serverkey`
8. View the new contents of the keystore, type `keytool -list -v -keystore bemsnew.pfx -storetype PKCS12 -storepass <mystorepassword>`

After you finish: Move the certificate into the BEMS keystore.

Import a previously issued certificate using a .pfx file

Before you begin:

- Verify that you have the .pfx file for a previously issued certificate. Make sure that you know the password for the .pfx file.
- If necessary, make sure that you know the password for the private key of the certificate within the .pfx file.
- Make sure that the certificate entry in the source .pfx file has the alias of "serverkey".

1. If necessary, verify that the PATH system variable includes the path to the Java bin directory.
   a) In a command prompt, type `set | findstr "Path"`.
   b) Press **Enter**.
   For instructions to set the Path system variable, see Set an environment variable for the Java location in the Installation content.
2. On the computer that hosts BEMS, create a temporary folder (for example, `C:\bemscert`).
3. Copy the .pfx certificate into the temporary folder.
4. Open a command prompt and navigate to the temporary folder that you created in step 2.
5. Confirm the information of the existing certificate in the bems.pfx keystore. Type `keytool -list -keystore bems.pfx -storetype PKCS12 -storepass <password of the .pfx file>`.
   The BEMS Dashboard keystore only supports one certificate in the bems.pfx keystore file. For more information about keystore commands, see Keystore commands. The following is a sample output:

   ```
   Keystore type: PKCS12
   Keystore provider: SunJSSE
   Your keystore contains 1 entr
   serverkey, <month> <day>, <year>, PrivateKeyEntry,
   Certificate fingerprint (SHA1):
    EA:A2:57:AB:30:09:DC:2A:F5:0A:EA:D9:D0:7A:3D:EB:95:A2:4C:7D
   ```

6. If the certificate alias isn't "serverkey", change the alias. Type the following command and press enter: `keytool -changealias -alias <alias from previous output> -destalias "serverkey" -keystore "C:\bemscert\bemsnew.pfx" -storetype PKCS12 -storepass <password of the .pfx file>`.

After you finish: Move the certificate into the BEMS keystore.

Move the certificate into the BEMS keystore

1. Copy the keystore file to the BEMS keystore. The keystore filename is bems.pfx or a non bems.pfx filename (for example, bemsnew.pfx).
2. Stop the Good Technology Common Services service from the Windows Service Manager.
3. Navigate to `<drive>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<version>\etc\keystores`.
4. In the keystores folder, rename the bems.pfx file to bems_bak.pfx.
5. Copy the bems.pfx or the new keystore file (for example, bemsnew.pfx), file from `C:\bemscert` to `<drive>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<version>\etc\keystores`.
6. Rename the file to bems.pfx.

After you finish: Update the certificate passwords in BEMS

Update the certificate passwords in BEMS

For BEMS to access your certificate private key, you must include the challenge password in the jetty.xml file. The password must be obfuscated. This can be done with the Jetty Util. For more information, see KB 41823.

Before you begin: Ensure that you have recorded the SSL certificate private key password. For more information, see Create a new keystore, generate a CSR request, and obtain a signed certificate from a CA or Import a previously issued certificate using a .pfx file.

1. Update the certificate password in BEMS. Perform the following actions:
   a) In a command prompt, navigate to the jetty util file. By default, the file is located at `<drive>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<version>\system\org\eclipse\jetty\jetty-util\9.<version>`.
   b) Type `java -cp jetty-util-9.<version>.jar org.eclipse.jetty.util.security.Password "<passwordToObfuscate>"`.
      For example, if the certificate private key password is dr*W0prr3!b, type `java -cp jetty-util-9.4.48.v20220622.jar org.eclipse.jetty.util.security.Password "dr*W0prr3!b"`
   c) Copy the **OBF** value for later reference. This is the obfuscated password.
2. Backup the jetty.xml file. By default the jetty.xml file is located at `<drive>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<version>\etc`.
3. Update the **keyStorePassword**, **trustStorePassword**, and **keyManagerPassword** in the jetty.xml file with the obfuscated password with the obfuscated password. For examples, see Jetty.xml file reference. Perform the following actions:
   a) In a text editor, open the jetty.xml file.
   b) Locate the <New class="org.eclipse.jetty.util.ssl.SslContextFactory" id="sslContextFactory"> section.
   c) Locate the following elements and update them with the obfuscated password from the jetty util file text output OBF value in step 1c above.
      - <Set name=”KeyStorePassword”>
      - <Set name=”TrustStorePassword”>
      - <Set name=”KeyManagerPassword”>
4. Start the Good Technology Common Services service from the Windows Service Manager.
5. Test the new certificate by accessing the BEMS Dashboard in a browser. Its certificate information now reflects the newly imported certificated.

Jetty.xml file reference

The keystore file is referenced in jetty.xml. Its default location of the jetty.xml file is on the computer hosting BEMS at `<BEMS Machine Path>\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<version>\etc\`. You can access this folder using the service account you used to install the BEMS software or the local system account.

The relevant snippet from jetty.xml referencing the location of the keystore file and its associated password would look like the following. If you import the certificate for one node, the CertAlias displays "serverkey". If you update the certificate and select the "Use the uploaded Server SSL Certificate for all nodes in a cluster" in the BEMS Dashboard, the CertAlias displays "server_cert".

```
<New id="sslContextFactory" class="org.eclipse.jetty.util.ssl.SslContextFactory
$Server">
  <Set name="KeyStorePath">
    <SystemProperty name="jetty.home" default="."/>
    /etc/keystores/bems.pfx
```

```
    </Set>
  <Set name="TrustStorePath">
    <SystemProperty name="jetty.home" default="."/>
    /etc/keystores/bems.pfx
  </Set>
  <Set name="KeyStorePassword">OBF:1mik1w8d1ugi1x841....1x8q1uh81w9d1mma</Set>
  <Set name="KeyManagerPassword">OBF:1mik1w8d1ugi1x841....1x8q1uh81w9d1mma</Set>
  <Set name="TrustStorePassword">OBF:1mik1w8d1ugi1x841....1x8q1uh81w9d1mma</Set>
  <Set name="KeyStoreType">PKCS12</Set>
  <Set name="TrustStoreType">PKCS12</Set>
  <Set name="wantClientAuth">true</Set>
  <Set name="CertAlias">server_cert</Set>
```

The passwords are obfuscated. The KeyStorePassword and the TrustStorePassword are typically identical and represent the keystore password. The KeyManagerPassword is the challenge password for the certificate.

Certificate format

Any certificate used should include the following:

- Be PKCS #12
- The private key must contain a challenge password
- Has the appropriate key chain (for example, the root and intermediate certificate)
- The Subject or Subject Alternative Names properties includes the FQDN of the BEMS node. This is required for BEMS to be trusted by web browsers and BlackBerry Dynamics apps.

Configuring HTTPS for BEMS to the BlackBerry Proxy server

Optionally, you can configure HTTPS for BEMS to the BlackBerry Proxy server. By default, the CA root certificate of the BlackBerry Proxy server is not located in the Java keystore that hosts BEMS or in the BEMS database. The BlackBerry Proxy server uses a certificate that is signed by BlackBerry UEM. This means that BEMS cannot verify the BlackBerry Proxy server's SSL certificate; and, therefore, any HTTPS connection made from BEMS to the BlackBerry Proxy server fails.

Export the BlackBerry Proxy CA certificate chain to your desktop

If your environment enforces the use of SSL certificate validation when BEMS communicates with BlackBerry Dynamics, you must export the root and intermediate BlackBerry UEM certificate chains used by the BlackBerry Proxy and import them into the BEMS Java keystore or upload them into the BEMS database using the BEMS Dashboard.

Note: The following task is not browser-specific. For specific instructions, see the documentation for the browser you are using in Mozilla Firefox, Windows Internet Explorer, Microsoft Edge, or Google Chrome. If you encounter issues when exporting the certificate, see KB 64803.

1. In a browser, enter the FQDN of the BlackBerry Proxy server and port 17433 (for example, https://<*Proxy_server_FQDN*>:17433). You may see a certificate error message because the certificate might be signed by the BlackBerry UEM or Control CA or another internal CA, but the browser does not recognize it as a well-known CA.
2. To open the Certificate dialog, click the certificate icon in the URL field.
3. Click **Certificate (Invalid)**.
4. Click **Certification Path**.
5. Click the root certificate. The root certificate is the first item in the Certificate hierarchy.

6. Click **View Certificate**.
7. Click the **Details** tab.
8. Click **Copy to File**.
9. Click **Next**.
10. Select **Base-64 encoded X.509 (.CER)**.
11. Click **Next**.
12. Enter a name for the certificate and export it to your desktop.
13. Click **Save**.
14. Click **Finish**.
15. Click **OK**.

After you finish: Create a trusted connection with Microsoft Exchange and other servers that BEMS must communicate with

Import the BlackBerry Proxy CA certificate into the Java keystore on BEMS

Before you begin: Save a copy of the certificate that you exported to a convenient location on the computer that hosts BEMS (for example, C:\bemscert). For instructions, see Export the BlackBerry Proxy CA certificate chain to your desktop.

1. On the computer that hosts BEMS, verify the Java directory is specified in the JAVA_HOME system environment variable. In a command prompt, change to the %JAVA_HOME% folder. Type `cd %JAVA_HOME%`. For more information, see Set an environment variable for the Java location in the installation content.
2. Make a backup of the Java keystore file. The Java keystore file is located at `%JAVA_HOME%\lib\security\cacerts`, where JAVA_HOME is confirmed in Step 1.
3. Import the exported BlackBerry Control or BlackBerry Proxyroot certificate. In a command prompt, type `bin\keytool.exe -importcert -trustcacerts -file"<drive>:\bemscert\bproot.cer" -keystore lib\security\cacerts -alias gda -storepass changeit`

   The -alias value must be unique in the destination keystore. If it is duplicated, you might experience import errors. You can output the cacerts keystore to a text file to manually confirm the existing certificates using a text editor. Type **bin\keytool.exe -list -v -keystore lib\security\cacerts > c:\bemscert\cacertsoutput.txt**

   For more information about keystore commands, see Keystore commands.

   Important: If you do not specify the -keystore parameter correctly or omit it, the keytool creates a new keystore. BEMS services do not use the new keystore."
4. If you did not import the BlackBerry Control root certificate into the Windows keystore, import it now. For instructions, see Import the BlackBerry Proxy CA certificate to the BEMS Windows keystore.
5. Restart the Good Technology Common Services service in the Windows Service Manager.

After you finish: Configure the Core BEMS service for communicating to BlackBerry Dynamics. For instructions, see Configure the BlackBerry Dynamics server in BEMS.

Import the BlackBerry Proxy CA certificate to the BEMS Windows keystore

For the Connect service to trust the BlackBerry Proxy server's certificate, you must import the BlackBerry Proxy root CA certificate to the Connect service Windows keystore.

1. Open the Microsoft Management Console.
2. Click **Console Root**.
3. Click **File > Add/Remove Snap-in**.
4. Click **Certificates**.

5. Select **Computer Account > Local computer > OK**.
6. Expand **Certificates (Local Computer) > Trusted Root Certification Authorities**.
7. Right-click **Certificates**, and click **All Tasks > Import**.
8. Click **Next**.
9. Browse to where you saved the BlackBerry Proxy CA certificate that you exported (for example <*drive*>: \bemscert\bproot.cer). Click **Open**.
10. Click **Next**.
11. Click **Finish**. Click **OK**.

After you finish: Configure the Core BEMS service for communicating to BlackBerry Dynamics. For instructions, see Configure the BlackBerry Dynamics server in BEMS.

Assign the BEMS SSL certificate to users

By default, BEMS uses a self-signed certificate that is generated by the BEMS installer. If the BEMS SSL certificate is CA signed, export the CA root and intermediates as described in Replacing the autogenerated SSL certificate.

1. If the BEMS SSL certificate has not been replaced, export the SSL certificate to a file.
   a) In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **SSL Certificate**.
   b) Click **Download SSL Certificate**. By default, the BemsCert.cer file is saved to the Downloads folder.
2. Create a CA certificate profile for the BEMS Self-Signed certificate, or create individual CA certificate profiles for the CA Root certificate and any CA Intermediate certificates. Assign the profiles to users or user groups. For instructions on creating a CA certificate profile and assigning it to users or user groups, see the BlackBerry UEM Managing Secure Connections content.

Keystore commands

The following table lists the keystore commands that are available at the command line. For more information, see the Oracle resource, visit keytool.

Action	Command
Check which certificates are currently in the keystore	`keytool -list -v -keystore lib\security\cacerts`
Export a list of the certificates that are currently in the keystore	`keytool.exe -list -v -keystore lib\security\cacerts > c:\bemscert\cacertsoutput.txt`
Export a certificate from the keystore	`keytool -exportcert -alias <alias_name> -file <file_name>.crt -keystore lib\security\cacerts`
Check a standalone certificate	`keytool -printcert -v -file <filename>.crt`
Delete a certificate from the keystore	`keytool -delete -alias <alias_name> -keystore lib \security\cacerts`
Import a signed primary certificate to an existing BEMS Java keystore	`keytool -importcert -trustcacerts -alias <alias_name> -file <file_name>.crt -keystore lib\security\cacerts`

Add dashboard administrators

You add groups using Microsoft Active Directory groups to the Dashboard Administrators setting and give members of the group dashboard login and configuration permissions. You can add one or more groups, but the group must be a part of the security groups. Users who are members of the Local Administrators group can also log in to BEMS.

You can also configure BEMS to require users to log in to the BEMS Dashboard using certificate-based authentication. When you enable certificate-based authentication, BEMS contacts the LDAP server and verifies the following information for the BEMS administrator:

- The user account is enabled.
- The user belongs to a security group that can log in to the BEMS Dashboard.

Before you begin: If you choose to enable certificate-based authentication, verify the following:

- You have access to the root and intermediate certificates from the certificate authority (CA). You can upload a base64-encoded or binary-encoded format certificate file that includes one or more trusted certificates to the BEMS Dashboard. When you upload one or more certificate files, the certificates are displayed in the dashboard. BEMS supports the following file extensions: .cer, .der, .pem, and .crt. For more information see KB 57259.
- Do not save the certificate file with a .pfx extension. PFX file extensions are not supported.
- Have BEMS administrators import the user credential certificates in the Personal Windows certificate store on the computer that is used to login to the BEMS Dashboard.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **BEMS Configuration**.
2. Click **Dashboard Administrators**.
3. Click **Add Group**.
4. In the **Active Directory Security Group** field, type the name of the Microsoft Active Directory security group.
5. Click **Save**.
6. Repeat steps 3 to 5 to add additional security groups.
7. Optionally, complete the following steps to require users to use certificate-based authentication to login to the BEMS Dashboard.
   a) Select the **Enable Client Certificate Authentication** checkbox.
   b) Click **Choose File**. Navigate to and select the client certificate file.
   c) Click **Open**.
   d) Enter the LDAP server information details.
      - In the **LDAP Server Name** field, type the name of the LDAP server. For example, ldap.<*DNS_domain_name*>.
      - In the **LDAP Server port** field, type the port number of the LDAP server. By default, the port number is 389. 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.
      - Enter the LDAP username and password. In a Microsoft Active Directory environment, enter the username in the format **domain\username**.
   e) Click **Save**.
   f) Restart each instance of BEMS.

After you finish: If you configured your environment for BEMS administrators to use certificate-based authentication, verify that users are prompted to select a certificate when they log in to the BEMS Dashboard. If BEMS Administrators experience an issue logging in to the dashboard using certificate authentication, they can log in with their user credentials.

Replace or delete the user credential certificates for certificate-based authentication

When you replace the user credential certificates (for example, when the certificate expires) that BEMS administrators use to authenticate to the Dashboard, you replace the existing certificates (root or intermediate certificate chain) in the BEMS database. You can upload a base64-encoded or binary-encoded file that includes one or more certificates. When you upload a single file that includes multiple certificates, the certificates are listed in the management console and can be deleted and replaced individually as required.

Before you begin: You have access to updated root and intermediate certificates from the certificate authority (CA) in a base64-encoded or binary-encoded format and they are stored in a network location that you can access from the management console.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **BEMS Configuration**.
2. Click **Dashboard Administrators**.
3. In the **Certificate Information** section, select the **Delete** checkbox beside each certificate that you want to delete. Click **Delete**.
4. Add the new certificate files as required. For instructions, see Add dashboard administrators.

BEMS-Core database

You can access the BEMS-Core database screen in the BEMS Dashboard (BEMS System Settings > BEMS Configuration > Database). It is prepopulated with the information that you entered during the BEMS software installation and requires a Microsoft SQL Server database that is available for BEMS. The information includes the SQL Server and database name, the authentication type used for BEMS to authenticate with the database, and any additional SQL properties that are required in your environment. By default, no changes are required on the Database Configuration screen. However, if you choose to make changes to it, consider the following:

- You must restart the Good Technology Common Services service for BEMS to update any changes.
- 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.

  1. 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 in the Installation content.
  2. Change the encrypt property to true and add trustServerCertificate=false separated by a semicolon (no space before or after the semicolon).
- You can use the information to verify the database settings by clicking the Test button after you install the BEMS software.

Configure the BlackBerry Dynamics server in BEMS

Your BEMS environment must be configured to trust the Root CA for the BlackBerry Proxy HTTPS configuration or implement the Karaf workaround. For instructions, see Configuring HTTPS for BEMS to the BlackBerry Proxy server.

The BlackBerry Dynamics server information in the following instructions refers to the FQDN of the server that hosts the BlackBerry Proxy service. The BlackBerry Proxy service is installed on on-premises BlackBerry UEM servers that have the BlackBerry Connectivity Node. The BlackBerry Connectivity Node is required for some BlackBerry UEM Cloud deployments when they link a company directory to the BlackBerry UEM Cloud tenant, and to offer on-premises connectivity to BlackBerry Dynamics users activated using the BlackBerry UEM Cloud. For more information about the BlackBerry Connectivity Node, see the BlackBerry UEM Installation and upgrade content.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **BEMS Configuration**.
2. Click **BlackBerry Dynamics**.
3. Complete one of the following actions:

Task	Steps
If a BlackBerry Proxy server is not defined	**a.** Click **Add BlackBerry Proxy**. **b.** In the **Host Name** field, type the FQDN of the server that hosts the BlackBerry Proxy service host name. **c.** In the **Protocol** drop-down list, select the protocol used to communicate with the BlackBerry Proxy server. • If you select HTTPS, the **Port** field prepopulates to 17433. • If you select HTTP, the **Port** field prepopulates to 17080. **d.** Click **Test** to test the connection. **e.** Repeat steps 1 to 4 to add additional BlackBerry Proxy servers for redundancy continuity.
If one or more BlackBerry Proxy servers are defined	No action is required. Previously defined BlackBerry Proxy servers are listed.

4. Select the **Apply to other nodes in the BEMS cluster** check box to communicate the BlackBerry Proxy server information to all of the BEMS nodes in the cluster. If this option is not selected, repeat steps 1 to 3 on each BEMS instance in your environment.
5. Optionally, select the **Enforce the SLL Certificate validation when communicating with BlackBerry Dynamics** check box when you use the https protocol to communicate with the BlackBerry Dynamics or BlackBerry Proxy server. It is best practice to enable this option when your environment is configured to use HTTPS SSL connections from BEMS to the BlackBerry Proxy server.
6. Click **Save**.

Configure a web proxy server

Apple Push notifications for iOS devices are sent by the BlackBerry Dynamics NOC to the Apple Push Notification Service (APNs). Push notifications for Android devices are sent directly to Firebase Cloud Messaging (FCM). Because the APNS and FCM reside outside of your enterprise network, a proxy server might be required.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings** click **BEMS Configuration**.
2. Click **Web Proxy**.
3. Select the **Use Web Proxy** checkbox.
4. In the **Proxy Address** field, enter the FQDN of the web proxy server.
5. In the **Proxy Port** field, type the port number.
6. Optionally, depending on your environment configuration you can specify URLs or domains that you want to pass through the web proxy server or bypass the web proxy server. If you enter multiple URLs or domains, separate them with a comma (,). You can use wildcards (*) when listing the URLs or domains. The URLs or domains that you list are not case-sensitive.
7. In the **Proxy Server Authentication Type** drop-down list, select an authentication type. By default, the authentication is set to **None**.

   If you choose Basic or NTLM authentication, enter the credentials and, optionally, the Domain.
8. Select the **Use the Web Proxy settings to connect to Exchange Server** checkbox, if you want to use the web proxy to communicate with Microsoft Exchange Server or Microsoft 365.
9. Select the **Apply to other nodes in the BEMS cluster** check box to communicate the BlackBerry Proxy server information to all of the BEMS nodes in the cluster.
10. Click **Test** to verify the connection to the proxy server.
11. Click **Save**.

Enabling log file compression

You can compress the log files that are generated and saved in the default log folder or folder you specified during the installation of BEMS. Currently, log files are generated and rotated once a day at midnight, when the server is restarted, or at the specified size you set. By default, the logs rotate at 100 MB. For more information on how to change the size when log files rotate, see KB 59146. When a log file exceeds the default or set size, it is compressed immediately and saved to the appropriate log file folder. If you require the logs to be compressed at a later time, you can specify a delay to a maximum of 1440 minutes (24 hours). By default, log file compression is disabled.

Consider the following scenario: You enable log compression with a delayed compression time of 360 minutes (six hours).

- At midnight, log file A rotates, but is not compressed. The delayed compression timer initiates. Log file A is scheduled to compress at 6 am. A new log file B starts to generate.
- You restart the BEMS service at 9 am. Log file B is rotated and the delay compression timer initiates. A new log file C starts to generate. BEMS verifies if the previous log file A has a last modified time of six hours. Since log file A is already compressed, no action from BEMS. is required.

Enable log file compression

If you installed the BEMS services on multiple computers and want to compress log files, and optionally delay compression of the log file, you must complete this task on one BEMS instance in the same database.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings** click **BEMS Configuration**.
2. Click log **Log Settings**.
3. Select the **Enable Log Compression**.
4. Optionally, specify a delayed time for the rotated log files to compress. If you enable delayed compression, you must specify a time in minutes. If a time is not specified, the delayed time defaults to zero minutes and the log files are compressed immediately after they rotate.
   a) Select the **Enable Delayed Compression** check box.
   b) In the **Delay for Compression** field, enter a time in minutes up to 1440 minutes.
5. Click **Save**.

Firebase Push Notifications

Configure FCM to send notifications to Android devices when the BlackBerry Work app and BlackBerry Connect app are in the background.

Note: Make sure that you complete the following steps before the end of June 2024 or email notifications will not be received on Android devices. For information on the HTTP v1 API, visit Migrate legacy FCM APIs to HTTP v1.

Before you begin: Generate the private key in your FCM project. For instructions, visit Migrate from legacy FCM APIs to HTTP v1

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings** click **BEMS Configuration**.
2. Click **Firebase Push Notification**.
3. In the **FCM Sender ID** field, type the **Sender ID** value of the project you created in Firebase. For more information, see KB 44617.
4. In the **Google Application Credentials** section, upload the private key of the project that you created in Firebase. The private key will be stored as a JSON file.
5. Click **Test** to verify that the JSON file is valid and can obtain a token from Google.
6. Click **Save**.
7. Instruct your users to restart the BlackBerry Work and BlackBerry Connect app.

Enabling FIPS Mode in BEMS

BEMS-Core, BEMS-Mail, BEMS-Docs, BEMS-Connect, and BEMS-Presence services can be configured to use FIPS 140-2 (U.S. Federal Information Processing Standards) compliant algorithms for cryptographic operations. When FIPS-compliance mode is enabled on one BEMS instance in a cluster, all instances in the cluster are enabled. To enable this feature in the cluster, all BEMS nodes must be running the same version of BEMS (for example, BEMS 2.12 or later). By default, FIPS 140-2 compliant mode is disabled. BEMS doesn't verify if the OS that hosts the BEMS-Docs service is running in FIPS 140-2 compliant mode.

Enable FIPS-compliance mode

Before you begin: Confirm that all BEMS nodes in the cluster are running the same version of BEMS. When you enable FIPS 140-2 compliance mode on one node in the cluster, all the nodes in the cluster are enabled.

1. In the BlackBerry Enterprise Mobility Server Dashboard, under **BEMS System Settings**, click **BEMS Configuration**.
2. Click **FIPS Mode**.
3. Select the **Enable FIPS Mode for Cluster** check box.
4. Click **Save**.
5. To enable FIPS-compliance mode for BEMS-Connect, complete the following steps on each computer that hosts an instance of the BEMS-Connect service:
   a) In a text editor, open the **GoodConnectServer.exe.config** file. By default, the file is located in <*drive*>`:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Connect\`.
   b) In the **<appSettings>** section, add the following key and value to the file: type `<add key="MESSAGE_ENCODING_TYPE” value="NON-SHIFT" />`.
   c) Save the file.
   d) In the Windows Manager, restart the Good Technology Connect service.

Verify that FIPS-compliance is enabled

When FIPS-compliance mode is enabled, the BEMS log file logs the action. The log files also log when an administrator accesses the FIPS mode configuration screen and saves the settings without making a change and when the feature is disabled. The following log lines are logged:

Logging	Description
`Changed FIPS mode to true`	FIPS-compliance mode is enabled.
`Changed FIPS mode to false`	FIPS-compliance mode is disabled.
`No change for FIPS mode`	FIPS-compliance mode settings were saved without changes.

Configuring BlackBerry Dynamics Launcher

The BlackBerry Dynamics Launcher is a UI component that is accessed in BlackBerry Dynamics apps (for example, BlackBerry Work) with the BlackBerry Dynamics Launcher button. The BlackBerry Dynamics Launcher creates a placeholder location for app settings. The BlackBerry Dynamics Launcher is a library module with numerous functions, currently comprising of the following:

- The user's name, photo, presence, and status
- A list of BlackBerry Dynamics-powered apps and modules installed on the device.
- Quick create options to easily compose an email, create a note, schedule a calendar event, or add a contact, regardless of which app is currently open.

To provide this rich user experience, the BlackBerry Dynamics Launcher library requires BEMS server-side services to:

- Synchronize policy-based sections (modules) between applications. For example, when Docs is enabled in BlackBerry Work, the Docs icon is enabled in the BlackBerry Dynamics Launcher, even when it is opened outside of BlackBerry Work in apps like BlackBerry Access or BlackBerry Connect.
- Fetch company directory information about the user to display the correct name and picture.
- Fetch presence information for the user and display the appropriate status (available, busy, away, do not disturb) and the user's presence message.

The required server-side services for the BlackBerry Dynamics Launcher comprise of the following:

- Presence (service id = com.good.gdservice.enterprise.presence)
- BlackBerry Directory Lookup (service id = com.good.gdservice.enterprise.directory)
- BlackBerry Follow-Me Store (service id = com.good.gdservice.enterprise.followme)

The client entitlement app to use these services is Good Enterprise Services (AppID = com.good.gdserviceentitlement.enterprise). For information on entitlement apps that are required when the services are installed on separate computers, see Server-side services.

BlackBerry Dynamics clients, like the BlackBerry Work app, check the server list for available BEMS instances hosting these services. This means the list must be populated with at least one computer that hosts BEMS to enable Good Enterprise Services. In addition, the Good Enterprise Services entitlement app must be added to at least one App Group in BlackBerry UEM like "All users".

Configuring Good Enterprise Services in BlackBerry UEM

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

1. Verify the Good Enterprise Services app is available in BlackBerry UEM.
2. Add BEMS to the Good Enterprise Services entitlement app.
3. Add the Good Enterprise Services entitlement app to users. You can use one or more of the following options. For instructions, see the Managing BlackBerry UEM administrators, users, and groups content.
   - To apply the app directly, assign the entitlement app to a user group or user account.
   - To assign the entitlement app to an app group, assign the app group to a user group or user account.

Verify that Good Enterprise Services are available in BlackBerry UEM

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

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

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

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

Task	Steps
Route all traffic	Select the **Route all traffic** checkbox to specify whether all BlackBerry Dynamics app data is routed through the BlackBerry Proxy. For more information about the BlackBerry Dynamics connectivity profile and routing behavior, see "Setting up network connections for BlackBerry Dynamics apps" in the BlackBerry UEM Managing apps content.
Add the BEMS instance to the Additional servers	**a.** In the **Additional servers** section, click +. **b.** In the **Server** field, specify the FQDN of the BlackBerry Enterprise Mobility Server. **c.** In the **Port** field, specify the port for the BlackBerry Enterprise Mobility Server. By default, the port number is 8443. **d.** In the **Primary BlackBerry Proxy cluster** drop-down list, select the name of the BlackBerry Proxy cluster that you want to set as the primary cluster. **e.** If necessary, in the **Secondary BlackBerry Proxy cluster** drop-down list, select the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.

5. Add the BEMS instance to the Good Enterprise Services entitlement app.
   a) In the **App servers** section, click **Add**.
   b) Search for and select **Good Enterprise Services**.
   c) Click **Save**.
   d) In the **App servers** for **Good Enterprise Services**, click +.
   e) In the **Server** field, specify the FQDN of the BlackBerry Enterprise Mobility Server.
   f) In the **Port** field, specify the listening port that is used by BEMS. By default, this is port 8443.
   g) In the **Priority** drop-down list, select the priority of the BlackBerry Proxy cluster that must be used to reach the domain.
   h) If necessary, in the **Secondary BlackBerry Proxy cluster** drop-down list, select the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
   i) Click **Save**.
6. Add the BEMS instance to the BlackBerry Work entitlement app.
   a) In the **App servers** section, click **Add**.
   b) Search for and select **BlackBerry Work**.
   c) Click **Save**.

d) In the **App servers** for **BlackBerry Work**, click +.
e) In the **Server** field, specify the FQDN of the BlackBerry Enterprise Mobility Server.
f) In the **Port** field, specify the listening port that is used by BEMS. By default, this is port 8443.
g) In the **Priority** drop-down list, select the priority of the BlackBerry Proxy cluster that must be used to reach the domain.
h) If necessary, in the **Secondary BlackBerry Proxy cluster** drop-down list, select the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
i) Click **Save**.

7. To save the updates to the existing profile, click **Save**.
8. To save the settings and add the new profile, click **Add**.

After you finish: Assign the entitlements to user accounts and groups or assign the entitlement app to an app group. You can use one or more of the following options. For instructions, see the BlackBerry UEM Administration content.

Verify Good Enterprise Services in Good Control

Presuming Good Control is installed, and now that you've installed BEMS on, for example, BEMS-Host1 and BEMS-Host2, the BlackBerry Presence, BlackBerry Directory Lookup, and Good Follow-Me services are now published in Good Control. Even so, it is wise to confirm that these services are available.

1. In Good Control, under **Apps**, click **Manage Services**.
2. Verify that the three BlackBerry Dynamics Launcher required services are listed.

After you finish: If the three services are not listed, verify your prerequisites for installing BEMS.

Setting a customized icon for the BlackBerry Dynamics Launcher

You can specify a default customized icon for the BlackBerry Dynamics Launcher on users' devices. When you specify a customized icon, the icon replaces the BlackBerry Dynamics icon for all users managed by the BEMS instance. For more information and tips on creating custom icons, see KB 44753.

When you specify a customized icon, make sure that the file meets the following requirements:

- Less than 500kb. Icons larger than 500kb are not added to the custom icons list.
- Named using the following format: <*file name*>_<*device_type*>_<*resolution*>.png. For example, Icon_iOS_2x.png.

  Where *resolution* is the supported resolution for the device. For example:

  - Android devices: ldpi, mdpi, hdpi, xhdpi, xxhdpi, and xxxhdpi
  - iOS devices: 1x, 2x, 3x, and so on
- Saved as a .png format

Specify a customized icon for the BlackBerry Dynamics Launcher

BEMS allows you to specify a custom icon for users in your environment. When you add custom icons, BEMS verifies the validity of the uploaded images. For more information about customized icon requirements, see Setting a customized icon for the BlackBerry Dynamics Launcher.

Before you begin: In a BlackBerry UEM Cloud environment, verify the following:

- The Email notifications for BlackBerry Work are configured.
- You have access to a supported customized icon for the BlackBerry Dynamics Launcher. For more information about the file requirements, see Setting a customized icon for the BlackBerry Dynamics Launcher.

1. Complete one of the following:

Environment	Steps
On-premises BEMS	**a.** In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry System Settings**, click **Launcher Branding**. **b.** Select the **Show customized icon in launcher** checkbox. **c.** Click the device drop-down list and select the device that you want to specify the launcher icon for. By default, Android is selected. **d.** Under **Icon**, click **Choose File**. **e.** Navigate to the icon file location. Click the file and then click **Open**. **f.** Click **Save**.
BlackBerry UEM Cloud	**a.** In the BlackBerry UEM management console, on the menu bar, click **Settings > BlackBerry Dynamics > Launcher Branding**. **b.** Select the **Show customized icon in launcher** check box. **c.** Click the tab for the device for which you want to specify the launcher icon. By default, Android is selected. **d.** Click +. **e.** Navigate to the icon file location. Click the file and then click **Open**. **f.** Click **Submit**. **g.** Click **Save**.

2. Repeat the steps for a customized Android device icon file resolution.
3. Complete the steps for a customized iOS device icon file resolution.

After you finish: If you remove all of the customized icon files, the default Launcher icon is used on the client devices for the Launcher app. To delete the customized icon, select the device for which you want to remove the customized Launcher icon and click **Delete** or **X**.

Remove a customized icon for the BlackBerry Dynamics Launcher

You can choose to remove a customized icon you specified for the BlackBerry Dynamics Launcher. If you remove all of the customized icon files, the default Launcher icon is used on the client devices for the Launcher app.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry System Settings**, click **Launcher Branding**.
2. Click the **Device** drop-down list and select the device for which you want to remove the customized Launcher icon.
3. Click **Delete** beside the icon you want to remove.
4. Click **Save**.

Next steps

After you complete the tasks to configure the BEMS Core tasks, see to the following configuration content to configure the necessary services for your environment:

- BlackBerry Mail (BlackBerry Push Notifications) service: This service accepts push registration requests from devices, such as iOS and Android, and then communicates with Microsoft Exchange Server using its Microsoft Exchange Web Services protocol to monitor the user's enterprise mailbox for changes.
- BlackBerry Docs service: This service lets your mobile workers access, synchronize, and share documents natively using their enterprise file server, SharePoint, Box, and content management systems supporting CMIS, without the need for VPN software, firewall reconfiguration, or duplicate data stores.
- BlackBerry Presence service: This service provides real-time presence status to BlackBerry Work, BlackBerry Dynamics Launcher, and third-party BlackBerry Dynamics applications.
- BlackBerry Connect service: This service boosts user communication and collaboration with secure instant messaging, corporate directory lookup, and user presence from an easy-to-use interface on IT-provisioned devices.

Appendix: Java Memory Settings

The Java settings for BEMS are located in the GoodServerDistribution-wrapper.conf file. By default, this file is located in the following location:

- In a new BEMS installation: `C:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<version>\etc\GoodServerDistribution-wrapper.conf`
- In an environment upgraded from GEMS to BEMS: `C:\Program Files\Good Technology\Good Enterprise Mobility Server\Good Server Distribution\gems-quickstart-version>\etc\GoodServerDistribution-wrapper.conf`

You can review or modify the default Java settings used by BEMS. However, in general, you won't need to make changes to the following initial memory allocation settings:

- # Initial Java Heap Size (in MB)

  ```
  wrapper.java.initmemory=2048
  ```

- # Maximum Java Heap Size (in MB)

  ```
  wrapper.java.maxmemory=4096
  ```

Appendix: Server-side services

The following table lists the server-side services when all of the BEMS services are installed on one computer or the services are installed on separate computers. Depending on the configuration for your BlackBerry Work app in your environment, you require different services. Consider the following scenarios:

- BlackBerry Work app is configured to use heritage settings: You can assign the Good Enterprise Services entitlement in the BlackBerry Dynamics Connectivity profile.
- BlackBerry Work isn't configured to use heritage settings: You must add the necessary entitlements individually.

For more information on configuring the BlackBerry Work app, see the BlackBerry Work administration content.

Installations	Required app and service IDs	Included server-side services
All of the BEMS services are installed on one computer.	• Good Enterprise Services (com.good.gdserviceentitlement.enterprise) • BlackBerry Connect (com.good.goodconnect)	• Directory Service 1.0.0.0 (com.good.gdservice.enterprise.directory) • Email Service 1.0.0.0 (com.good.gdservice.enterprise.email) • FollowMe Store Service 1.0.0.0 (com.good.gdservice.enterprise.followme) • Launcher customization service 1.0.0.0 (com.blackberry.gdservice.launcher-customization) • Presence Service 1.0.0.0 (com.good.gdservice.enterprise.presence) • Docs Service 1.0.0.0 (com.good.gdservice.enterprise.docs)
Only the Mail service is installed on one computer	BlackBerry Core and Mail Services (com.blackberry.gdservice-entitlement.coreandmail)	• Directory Service 1.0.0.0 (com.good.gdservice.enterprise.directory) • Email Service 1.0.0.0 (com.good.gdservice.enterprise.email) • FollowMe Store Service 1.0.0.0 (com.good.gdservice.enterprise.followme) • Launcher customization service 1.0.0.0 (com.blackberry.gdservice.launcher-customization)
Only the Connect service is installed on a computer	BlackBerry Connect (com.good.goodconnect)	Send Message Service 1.0.0.0 (com.good.gdservice.send-message)
Only the Presence service is installed on a computer	BlackBerry Presence Service (com.blackberry.gd-service.entitlement.presence)	Presence Service 1.0.0.0 (com.good.gdservice.enterprise.presence)

Installations	Required app and service IDs	Included server-side services
Only the Docs service is installed on a computer.	Feature-Docs Service Entitlement (com.good.feature.share)	Docs Service 1.0.0.0 (com.good.gdservice.enterprise.docs)
The Mail and Presence services are installed on one computer	• BlackBerry Core and Mail Services (com.blackberry.gdservice-entitlement.coreandmail) • BlackBerry Presence Service (com.blackberry.gd-service.entitlement.presence)	The Mail services and Presence services listed above.
The Connect and Presence services installed on a computer.	• BlackBerry Connect (com.good.goodconnect) • BlackBerry Presence Service (com.blackberry.gd-service.entitlement.presence)	The Connect and Presence services listed above.

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