



BlackBerry Enterprise Mobility Server Installation Guide

3.8

Contents

What is BEMS?	5
Configuring BlackBerry UEM Cloud email notifications and Cloud Docs service for BlackBerry Dynamics apps	8
Preinstallation and preupgrade requirements for on-premises BEMS	9
Set an environment variable for the Java location.....	10
Setting up a Windows service account for BEMS.....	11
Creating a Microsoft Active Directory account for the BEMS service account.....	12
Change the BEMS service account password.....	12
Configuring connections for the BEMS databases.....	12
Create the BEMS services databases.....	12
BlackBerry Push Notifications database requirements.....	14
Port requirements.....	15
Prerequisites: BlackBerry Push Notifications service.....	20
Grant application impersonation permission to the service account.....	20
Microsoft Exchange Autodiscover.....	21
Docs prerequisites: CMIS Requirements.....	22
Connect prerequisites: Skype for Business.....	22
Preparing the computer that hosts BEMS for use with Skype for Business.....	22
Preparing the Skype for Business topology for BEMS.....	23
SSL certificate requirements for Skype for Business.....	26
Presence prerequisites: Skype for Business.....	32
Presence Prerequisites: Cisco Unified Communications Manager IM and Presence Service.....	32
Create an Application User.....	32
Create a Dummy User.....	32
Configure Cisco Unified Communications Manager and Cisco IM and Presence certificates with the enterprise certificate authority.....	33
Prerequisites: BlackBerry Directory Lookup, BlackBerry Follow-Me, and BlackBerry Certificate Lookup services.....	35
Installing or upgrading the BEMS software	36
Supported installation and upgrade paths.....	36
Best practices: Preparing to upgrade.....	36
BEMS setup application modes.....	36
Install the BEMS software.....	37
Upgrade the BEMS software.....	40
Steps to upgrade BEMS and change to an alternate JRE.....	41
Steps to install BEMS instances into a cluster.....	42
Perform a Silent Install or Upgrade.....	43
Removing the BEMS software	44

Remove the BEMS software.....	44
Remove the BEMS server references from the BlackBerry Dynamics connectivity profile.....	44
Remove the BEMS Connect server references for BlackBerry Connect.....	45

Configuring the BEMS services..... 46

Appendices..... 47

Appendix: AlwaysOn Availability support for SQL Server.....	47
Steps to setup SQL Server for AlwaysOn availability.....	47
Configure the BEMS services databases for AlwaysOn availability.....	47
Enabling AlwaysOn availability group failover to subnets for the BEMS-Core and Mail services.....	48
Enabling AlwaysOn availability group failover to subnets for the Connect service.....	48
Enabling AlwaysOn availability group failover to subnets for the Docs service.....	48
Data flow: BEMS notification flow using the Microsoft Graph API.....	48
Configuring BlackBerry UEM Cloud to communicate with an on-premises BEMS.....	49
Import the certificate to the BEMS Windows keystore.....	50
Import the certificate into the Java keystore on BEMS.....	51
Configure the BlackBerry Dynamics server in BEMS.....	51
Configure BEMS connectivity with BlackBerry Dynamics.....	52
Add an app server hosting the entitlement apps to a BlackBerry Dynamics connectivity profile.....	52
Export the BlackBerry Proxy certificate to the local computer.....	53

Legal notice..... 55

What is BEMS?

To support BlackBerry Dynamics apps, you must install the BlackBerry Enterprise Mobility Server (BEMS) in your BlackBerry UEM environment to provide additional services for BlackBerry Dynamics apps. For more information about the BEMS architecture in a UEM Cloud environment, see the [BlackBerry UEM Architecture in the Overview and Architecture content](#).

The following table describes the available BEMS versions.

Versions	Description
On-premises	<p>Your BEMS instance integrates the following services: BlackBerry Mail, BlackBerry Connect, BlackBerry Presence, and BlackBerry Docs. When these services are integrated, users can communicate with each other using secure instant messaging, view the real-time presence status of users in BlackBerry Dynamics apps, and access, synchronize, and share documents natively with their enterprise file server, Microsoft SharePoint, and so forth. The following table describes the services offered by BEMS.</p> <p>You configure the BEMS server components and services using the BEMS Dashboard after the installation completes. the dashboard is a browser-based administration console. The BEMS Web Console, also browser-based, provides real-time monitoring and logging of device connectivity, traffic load, and throughput in near real-time.</p>
Cloud	<p>Your BlackBerry UEM Cloud instance allows you to enable the BlackBerry Dynamics email notifications and Docs services for your UEM Cloud tenant. When these services are enabled, users can access, synchronize, and share documents using the following storage services: Microsoft SharePoint Online, Microsoft SharePoint, Microsoft OneDrive for Business, and Box. File Share and CMIS-based repository storage providers are not supported.</p> <p>You enable and configure the BlackBerry Push Notifications and the Docs Cloud services using the BlackBerry UEM management console. If your environment requires the BlackBerry Connect service and BlackBerry Presence service, an on-premises BEMS must be installed, and the services configured using the BEMS Dashboard.</p>

Services supported by BEMS

Service	On-premises	Cloud	Description
BlackBerry Mail (BlackBerry Push Notifications)	✓	✓	<p>On-premises: The BlackBerry Mail 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.</p> <p>Cloud: The BlackBerry Dynamics email notifications service accepts push registration requests from devices, such as iOS and Android, and then communicates with the on-premises Microsoft Exchange Server or Microsoft Office 365 server to check the user's mailbox for changes. When changes occur, such as new email, notifications are pushed to devices.</p>
BlackBerry Connect	✓		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.
BlackBerry Presence	✓		This service provides real-time presence status to BlackBerry Work, the BlackBerry Dynamics Launcher, and third-party BlackBerry Dynamics applications, giving them a powerful add-in for mobile collaboration.
BlackBerry Docs	✓	✓	<p>On-premises: The BlackBerry Docs 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.</p> <p>Cloud: The BlackBerry Dynamics Docs service lets your mobile workers access, synchronize, and share documents using the following storage services: Microsoft SharePoint Online, Microsoft SharePoint, Microsoft OneDrive for Business, and Box. File Share and CMIS-based repository storage providers are not supported.</p>

Service	On-premises	Cloud	Description
BlackBerry Directory Lookup	✓	✓	<p>On-premises: This service gives users the ability to look up first name, last name, and picture from your company directory and display it within the BlackBerry Dynamics Launcher and other BlackBerry Dynamics apps such as BlackBerry Connect.</p> <p>Cloud: This service allows users to look up other users by first name, last name, and associated photo or avatar from the company directory.</p>
BlackBerry Follow-Me	✓	✓	This service keeps the BlackBerry Dynamics Launcher synchronized across multiple devices.
BlackBerry Certificate Lookup	✓		The BlackBerry Certificate Lookup service retrieves S/MIME digital certificates from the user's Microsoft Active Directory account and matches the requested key usage. Only the recipient's public certificate is retrieved for matching.

Configuring BlackBerry UEM Cloud email notifications and Cloud Docs service for BlackBerry Dynamics apps

In a BlackBerry UEM Cloud environment, you can configure the BlackBerry Mail (Push Notifications) Service to send notifications to iOS and Android devices when new email is received. You can also configure the BlackBerry Docs service for mobile workers to access, synchronize, and share documents using supported storage services. Optionally, you can configure your UEM Cloud environment to communicate with an on-premises BEMS to use BEMS-Presence, BEMS-Connect, in addition to the BlackBerry Mail (Push Notifications) and BEMS-Docs service for BlackBerry Work. For more information, see the following:

- To configure the BlackBerry Mail (Push Notifications), see [Steps to configure email notifications for BlackBerry Work](#) in the BlackBerry Work administration content.
- To configure the Cloud BlackBerry Docs service, see [Configuring the BlackBerry Docs Service](#) content.
- To configure a hybrid of on-premises BEMS services (For example, on-premises BlackBerry Connect service and cloud email notifications and BEMS-Docs services), see [Configure UEM Cloud to communicate with an on-premises BEMS](#).

Preinstallation and preupgrade requirements for on-premises BEMS

Complete the following tasks, if required, before you install or upgrade the on-premises BEMS.

Hardware requirements

Review and complete the [Capacity Calculator for BlackBerry BEMS](#). The performance calculator provides minimum recommendations based on the values that you enter. If you require additional capacity, redundancy, or room for growth, enter values that reflect these needs to accommodate any near future large app and user deployment projects.

Verify that your environment meets the [hardware requirements](#) for your needs and to determine whether you should install BEMS on a separate server.

Third-party software requirements

Verify that Windows is up-to-date and that you perform any restarts required for the update.

Verify that the server that is hosting BEMS is running [an operating system that supports BEMS](#).

If your organization uses a proxy server for Internet access, verify that you have the proxy server details (for example, the web proxy FQDN). For more information, see [Configure a web proxy server](#) in the BEMS Core configuration content.

Verify the version of Microsoft .NET Framework. For more information, see [Preparing the computer that hosts BEMS for use with Skype for Business](#).

If your environment uses Microsoft Exchange, verify that the Exchange client access server (CAS) version supports TLS 1.2. For more information, see [KB 56869](#). If the TLS version is not updated, Push Notifications fail. BEMS enforces TLS 1.2 for connections to the Microsoft Exchange server.

If your environment uses Microsoft SQL Server, verify that your SQL Server is updated to support TLS 1.2 if database connection encryption is used. If the TLS version is not updated, you receive an error message and can't access the BEMS dashboard. BEMS enforces TLS 1.2 for connections to the SQL Server. For more information, see [KB 56869](#) and [KB 56865](#).

Verify that you have a [database server that supports BEMS](#).

To configure remote TCP/IP connections for Microsoft SQL Server Express, see [BlackBerry Push Notifications database requirements](#).

Verify that you have a [mail server that supports BEMS](#).

Verify that the server's date and time are set correctly.

Verify that the server that is hosting the BEMS instance has been joined to the domain.

Verify that your server that hosts and accesses the on-premises BEMS Dashboard has a [supported browser installed](#).

Third-party software requirements

Set up a [Windows service account for BEMS](#).

Verify that the BEMS service account is a local administrator on the computer that hosts the BEMS instance.

If you plan to install the Docs service and provide users with access to a content storage provider, verify the environment is running a [supported content storage repository](#) (for example, Microsoft SharePoint or Box).

Verify that the SQL Server account or the BEMS Windows service account has db_owner privileges to the database. For more information, see [KB 42661](#).

Verify that you have installed JRE 17 on the servers where you will install BEMS and that you have an environment variable that points to its location. For more information, see [Set an environment variable for the Java location](#). For more information about supported JRE versions, see the [Compatibility matrix](#).

Environment configuration requirements

Verify that you opened the necessary ports on your organization's firewall. For a list of required ports, see [Port requirements](#).

Verify that you have DNS support for the following:

- If your environment uses Microsoft Graph for the BlackBerry Mail service, create a public DNS entry for each BEMS Cluster. The DNS entry must point to the reverse proxy appliance. The public DNS entry is used as the "External Notifications URL" in the BEMS Dashboard.
- If your environment uses Skype for Business using non-trusted application mode, a minimum of one DNS entry for lyncdiscoverinternal exists. For more information, see the Microsoft resource [DNS requirements for Skype for Business Server](#).

Verify that you have configured permissions for the BEMS service account.

During the install or upgrade of the BEMS software, disable any antivirus programs and exclude the BEMS directory from virus scanning.

Set an environment variable for the Java location

BEMS requires you to install a JRE 17 implementation on the servers where you will install BEMS, and that you have an environment variable that points to the Java home location. For more information about supported JRE versions, [see the Compatibility matrix](#).

When you begin the installation, BEMS verifies that it can find Java. If BEMS can't find Java, the setup application will stop on the prerequisites panel, and you must set an environment variable for the Java location. Note that you must close down the installer at this time and restart it only after the environment variable has been created or updated.

Important: It is recommended to disable the auto-updates to the Java Runtime Environment to avoid possible disruption of the BEMS notification function. For instructions on how to upgrade the Java version, visit [KB48312](#).

Before you begin: Verify that you have installed JRE 17 on the server where you will be installing BEMS.

1. Open the **Windows Advanced system settings** dialog box.

2. Click **Environment Variables**.
3. In the **System variables** list, complete one of the following tasks:
 - If **JAVA_HOME** does not exist, create the variable. click **New**. In the **Variable name** field, type `JAVA_HOME`.
 - If the **JAVA_HOME** variable exists, click **Edit**.
4. In the **Variable value** field, type the full path to the Java install folder for the 64-bit JRE. For example,
 - If you installed Oracle's JRE version 17 JDK, type `C:\Program Files\Java\jdk-17`
 - If you install an alternate JRE, for example Zulu, type `C:\Program Files\Zulu\zulu-17`If you use an OpenJDK version and include the direct path to the `java.exe` file, the BEMS installer returns the following error message: **Could not find a valid Java virtual machine to load. You may need to reinstall a supported java virtual machine.**
5. Click **OK**. Click **OK** again.

Setting up a Windows service account for BEMS

A service account is a Windows account that runs the services for BEMS. The BEMS service account must be a member of the local Administrators group on the computer that you install BEMS on, and it must have the Log on as a service permission. The service account must also have permission to access the Microsoft SQL Server unless you are using direct SQL Server authentication.

For the required service account, "BEMSAdmin" is recommended. You can use the same Windows service account to install all of the BEMS service modules. For example, `bemsadmin@example.com`. Make sure the service account has the appropriate administrative privileges for all the BEMS service modules that you plan to install and configure. Permissions for individual service modules may not require the same privilege level as others.

Important: If you're environment runs on-premises Skype for Business and uses the same service account for the Connect and Presence services, you must give the service account the `RTCUniversalReadOnlyAdmins` rights.

Before you begin: Verify that you have [created a Microsoft Active Directory account for the BEMS service account](#).

1. On the taskbar, click **Start > Administrative Tools > Computer Management**.
2. In the left pane, expand **Local Users and Groups**.
3. Navigate to the **Groups** folder.
4. In the right pane, double-click **Administrators**.
5. Click **Add**.
6. In the **Enter the object names to select** field, type the name of the service account (for example, `BESAdmin`).
7. Click **OK**.
8. Click **Apply**.
9. Click **OK**.
10. On the taskbar, click **Start > Administrative Tools > Local Security Policy**.
11. In the left pane, expand **Local policies**.
12. Click **User Rights Assignment**.
13. Configure the **Log on as a service** permission for the service account.

After you finish: Optionally, [Change the BEMS service account password](#).

Creating a Microsoft Active Directory account for the BEMS service account

Note: "Read Only Domain Controllers" are a feature of the Microsoft Active Directory software. Read Only Domain Controllers Microsoft Active Directory servers are not supported for BEMS. BEMS supports only writable domain controllers.

Set the following attributes for the BEMS service account:

- The account for the Connect and Presence services must be in the same Active Directory domain as the BEMS server. For more information, see [KB 63703](#).
- This service account should be a member of local administrator group on the BEMS host machine.
- The account name (UID, distinct from the account password) must be strictly alphanumeric; no special characters are allowed with the exception of underscore (_), hyphen (-), and period (.). For example, BEMSAdmin.
- Account Password (distinct from the account name above) must not contain these characters: semicolon (;), at sign (@), slash mark (/), caret (^), and double quotes (").
- Password Expires option must be set to Never for this account.

Change the BEMS service account password

1. Log in to the server that is hosting the BEMS instance using the updated password.
2. Open the Services window.
3. For the Good Technology Common Services,
 - If the Log On As services is Local System, no action is required.
 - If the Log On As services is service account, update the password and click **Apply**. Restart both services.
4. Log in to the BEMS dashboard.
5. Under **BlackBerry Services Configuration**, click **Mail > Microsoft Exchange**. If the **Use Windows Integrated Authentication** check box is clear, and the same service account is used, update the password, run a test, and then save the configuration
6. If the Good Technology Connect and Good Technology Presence services use the same service account, update that password and save the configuration.

Configuring connections for the BEMS databases

You must create the required database for the BEMS services you plan to install, depending on whether you install all the services on one server or separate servers. BEMS can connect to the database using Windows authentication or Microsoft SQL Server authentication. Verify that your environment is running a supported database server. For more information, see the [BEMS Compatibility Matrix](#).

You can connect to the BEMS core and BEMS services databases using one of the following:

- The service account that you used to complete the installation process
- Microsoft SQL Server account that you specified during the installation process

Create the BEMS services databases

Depending on the configuration of your environment (for example, you plan to install all the BEMS services), you must create one or more Microsoft SQL Server databases.

Verify that the Microsoft SQL Server account or the BEMS Windows service account has db_owner privileges to the databases. For more information, see [KB 42661](#).

The following table is an example of a small deployment that has all of the BEMS services installed on one server. For an example of a large and small deployment that has all of the BEMS services installed on one server, see [Example of a small BEMS deployment](#).

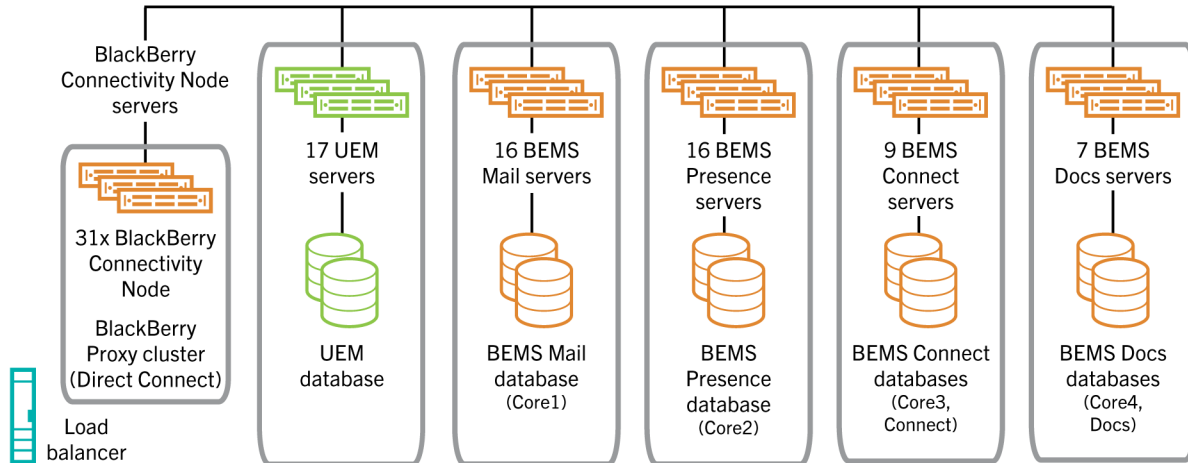
Services	Databases
All BEMS services on the same server	<ul style="list-style-type: none"> • Create a blank SQL database for the BlackBerry Push Notifications service and call it "BEMS_Core". • Create a blank SQL database for the Connect service and call it "BEMS_Connect." • Create a blank database for the Docs service and call it "BEMS_Docs." <p>Note: If this is the first server in the BEMS cluster, create the databases. If this is an additional server for the same BEMS cluster, new databases are not required. Record the existing database names for the BEMS services.</p>

The following table is an example of a large deployment that has the BEMS services installed on separate servers. When you create a separate database for each service, you create a new cluster for that service. The push notifications are included in the Core database. If you create separate databases, select the appropriate database for the service. For an example of a large deployment that has the BEMS services installed on separate servers, see [Example of a large BEMS deployment](#).

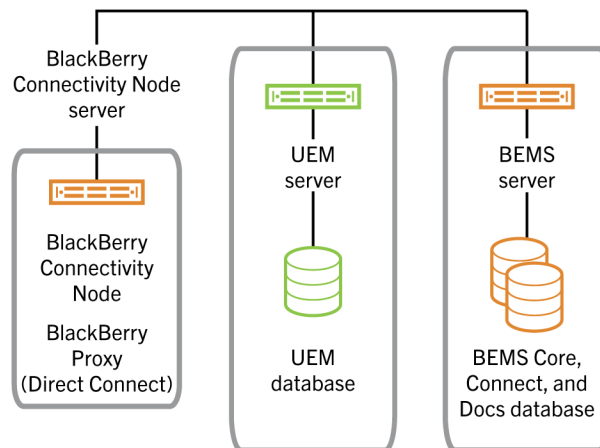
Services	Databases
BlackBerry Push Notifications service (Mail service) on one server	Create a blank database and call it "BEMS_Core1".
Connect service and Presence service on one server	Create two blank databases. Call one "BEMS_Core3" and call one "BEMS_Connect." The Presence service does not require a separate database when it is installed on a server with a service that uses a database.
Connect service only on one server	Create two blank databases. Call one "BEMS_Core3" and call one "BEMS_Connect."
Presence service only on one server*	Create a blank database and call it "BEMS_Core2."
Docs service only on one server	Create two blank databases. Call one "BEMS_Core4" and call one "BEMS_Docs."

Examples of a BEMS deployment

Below is an example of a large deployment of BEMS with all of the services installed on separate servers.



Below is an example of a small deployment of BEMS with all of the services installed on one server.



BlackBerry Push Notifications database requirements

Note: Verify that the Collate property is set to CI (case insensitive). This is the default collation setting when you create a new database. If you are upgrading an existing database, verify the collation setting.

BEMS connects to the Microsoft SQL Server using TCP/IP. If your environment uses Microsoft SQL Server Express, the TCP/IP protocol is not enabled by default. For instructions on how to enable TCP/IP on Microsoft SQL Server Express, see [KB 63994](#).

BEMS supports the use of dynamic ports when connecting to the SQL Server. Dynamic ports is the default setting for SQL Server Express installations and other more complex SQL Server installations. The SQL Server Browser service must be started for BEMS to use SQL Server dynamic ports. BEMS connects to the SQL Server Browser service over port 1434 to obtain the current dynamic port of the SQL Server instance to use. By default, the SQL Server Browser service is disabled in SQL Server Express installations.

Verify the case sensitivity of the BlackBerry Push Notifications database

Run the following SQL query: `SELECT DATABASEPROPERTYEX('dbname', 'Collation')`

Where *dbname* is the name of the BlackBerry Push Notifications database. For example, GEMSDB.

Verify the return value.

- SQL_Latin1_General_CP1_CI_AS, CI indicates that the database is case insensitive.
- SQL_Latin1_General_CP1_CS_AS, CS indicates that the database is case sensitive.

Change the BlackBerry Push Notifications case type to insensitive

To change the case sensitivity, type `alter database [dbname] collate SQL_Latin1_General_CP1_CI_AS`

During installation, you will be prompted to specify the database server and SQL instance. When this information is entered, the BEMS installer will automatically create the schema required by BlackBerry Push Notifications.

Port requirements

Before you install or upgrade BEMS, you should familiarize yourself with how BEMS uses ports.

The BEMS services use various ports to communicate with the BlackBerry Infrastructure, the BlackBerry Dynamics NOC, and internal resources (for example, your organization's messaging software). This section lists the default ports that BEMS uses for outbound, inbound, and internal communications. All ports are TCP, unless otherwise specified. The ports must be open and ready for BEMS to use and not blocked by a firewall.

BEMS must be installed in BlackBerry UEM environments that use BlackBerry Dynamics. BEMS has port requirements for communication with UEM and the BlackBerry Dynamics NOC.

BEMS services TCP ports

Ports	Connection	Service	Purpose
8443	Outbound	Connect, Presence	To connect to the Cisco User Data Service
		Presence	To connect to the Presence Web Service (CIMP server)

Ports	Connection	Service	Purpose
		BlackBerry Mail (Push Notifications Service)	<p>Optionally, if your environment uses Microsoft Graph, 8443 or another configured port to the reverse proxy appliance. For information about how Microsoft Graph communicates with BEMS, see Data flow: BEMS notification flow using the Microsoft Graph API.</p> <p>If your environment uses Microsoft Graph, you can complete the following:</p> <ul style="list-style-type: none"> Restrict the firewall to only accept connections from Microsoft's list of IP addresses. For more information on the available Microsoft Graph Change notifications IP addresses, see the Microsoft resource Other endpoints not included in the Microsoft 365 IP Address and URL Web service. Restrict the reverse proxy server to only proxy the /notificationClient URI (for example, bems_server_name.example.com:443/notificationClient" ;="bems.example.com:8443/notificationClient BEMS_Pool". If the reverse proxy appliance is installed in a DMZ, make sure that port 8443 is open from the reverse proxy to each BEMS node.
	Inbound	Dashboard	The Dashboard binds to this port and allows BEMS administrators and BEMS Docs users to access the Dashboard using a web browser.
		BlackBerry Mail (Push Notifications Service), Presence, and Docs	To connect from the BlackBerry Proxy.
		Docs	To connect from Microsoft Office Web Apps or Office Online Server for Docs.
		Presence	To connect from the BlackBerry Proxy server.
		BlackBerry Mail (Push notifications Service), Presence	To connect from the BlackBerry Proxy server, and optionally for Microsoft Graph (Push Notifications) to the reverse proxy server appliance. For more information about how Microsoft Graph communicates with BEMS, see Data flow: BEMS notification flow using the Microsoft Graph API .

Ports	Connection	Service	Purpose
		BlackBerry Mail (Push Notifications Service), Presence, Docs	To connect from the BlackBerry Proxy server, and from Microsoft Office Web Apps or Office Online Server (Docs).
443	Outbound	BlackBerry Mail (Push Notifications Service)	To connect to <ul style="list-style-type: none"> the BlackBerry Dynamics NOC (includes connections to APNs) (gdweb.good.com) Firebase Cloud Messaging (FCM) for Android Push Notifications Microsoft Exchange Server (Microsoft Exchange Web Services, AutoDiscover), optionally to Microsoft Graph
		Connect	In a Skype for Business on-premises environment that uses non-trusted application mode, to connect to: <ul style="list-style-type: none"> lyncdiscoverInternal.<DomainName>.com FQDN of the internal Skype Front End pool
		BlackBerry Mail (Push Notifications Service)	In an Entra environment, to connect to the following: <ul style="list-style-type: none"> login.microsoftonline.com graph.microsoft.com *.aadrm.com
		Docs	In a SharePoint Online environment, to connect to: <ul style="list-style-type: none"> login.microsoftonline.com *.sharepoint.com
		Docs	In a Box environment, to connect to *.box.com.
17080 or 17433 (SSL)	Outbound	BlackBerry Mail (Push Notifications Service)	To connect to the BlackBerry Proxy server. BEMS requires visibility of all instances of the BlackBerry Proxy server (17080 and 17433), regardless of whether KCD is enabled or not, so that if one BlackBerry Proxy fails, BEMS can communicate with the next BlackBerry Proxy in the cluster for authentication tokens.
1433, 1434	Outbound	BlackBerry Mail (Push notifications Service), Connect, Presence	To connect to the Microsoft SQL Server database (default). To connect to the SQL Browser service when using dynamic ports.

Internal TCP ports for internal BEMS communications

Ports	Purpose
8101	SSH connectivity to BEMS.
8443	Used by the BlackBerry Mail (Push notifications Service) and Presence service.
8099	Used by the .NET Component Manager.
8060	Used by the Lync Presence Provider (LPP).
6379	Used by LPP in a Skype for Business environment and BEMS-Core in a Cisco Unified Communications Manager IM and Presence environments to read and write to the Redis service database.
1001	Used by BEMS for internal process communications when Active Directory Rights Management Services (AD RMS) and Entra-IP RMS are used in the environment.

BlackBerry Push Notifications (Mail) service TCP ports

Important: Devices must be able to connect to the Apple Push Notification Service (APNS) and cloud messaging servers to receive push notifications from BEMS. If your Wi-Fi network restricts outbound access, verify that the proper outbound ports are open for your devices.

Ports	Connection	Purpose
61616 or 61617 (SSL)	Bidirectional	<p>Connection to and from servers that host BEMS in the same cluster.</p> <p>To support clustering, BEMS employs ActiveMQ's enterprise features. By design, network port 61616 and 61617 (SSL) are used for inter-BEMS communication. Any firewall between BEMS nodes in the same cluster should have rules allowing bi-directional communication between BEMS nodes over port 61616 and/or 61617 (SSL).</p>
80	Outbound	To connect to Microsoft Exchange Server (AutoDiscover).
389 or 636 (SSL)	Outbound	To connect to Active Directory using LDAP.
3268 or 3269 (SSL)	Outbound	To connect to the Global catalog.
Google Authentication Server URLs	Outbound	<p>To connect to the following URLs:</p> <ul style="list-style-type: none"> • https://accounts.google.com/o/oauth2/auth • https://oauth2.googleapis.com/token • https://www.googleapis.com/oauth2/v1/certs

BlackBerry Connect and BlackBerry Presence service TCP and UDP ports

If you install Connect for Skype for Business, if the Skype for Business database server is using a static port, then you must open that port. The range of ports is necessary only when the Skype for Business database server is using dynamic ports.

Ports	Connection	Purpose
8080 or 8082 (SSL)	Inbound	Connection from the BlackBerry Proxy server and is used by the BlackBerry Connect service. By default, SSL communication is enabled with a new BEMS 2.12.5.6 or later installation and is bound to port 8082. If you upgraded from BEMS 2.10 or earlier and SSL communication with the BlackBerry Connect app is not enabled, use port 8080. For more information, see Configure BlackBerry Connect app settings in BlackBerry UEM in the BlackBerry Connect administration content .
49555	Inbound	Connection from the on-premises Skype for Business server (for BlackBerry Connect) when the Connect service is trusted by Skype for Business.
49777	Inbound	Connection from the on-premises Skype for Business for BlackBerry Presence.
5061	Outbound	To connect from the BlackBerry Connect service to the on-premises Skype for Business server configured as trusted mode.
1434	Outbound	UDP port to connect to the on-premises Skype for Business database. This is used for the initial setup only.
49152 to 57500	Outbound	A random port in this range to the Skype for Business database. This is used for the initial setup only.
5222	Outbound	To connect to the Cisco Jabber XMPP Service. To connect to the Presence Web Service (CIMP server).
8083	Outbound	To connect to the Cisco IM and Presence Service.

BlackBerry Docs service TCP ports

Ports	Connection	Purpose
80 or 443	Outbound	To connect to your Microsoft SharePoint server.
443	Outbound	To connect to Microsoft Office Web Apps or Office Online Server.
445 or 139	Outbound	To connect to the CIFS share.
389 or 636	Outbound	To connect to Active Directory using LDAP.

Ports	Connection	Purpose
137, 138	Outbound	UDP port to connect to the CIFs share.

Prerequisites: BlackBerry Push Notifications service

The BlackBerry Push Notifications service requires that you set up a Windows service account for BEMS in support of your Microsoft Exchange environment.

Microsoft Exchange Web Services (EWS) push notifications are sent (or pushed) by the server to a client-side web service. Push notifications are ideally suited for tightly coupled clients like BlackBerry Work and other BEMS supported apps to which the server has reliable access. When the BlackBerry Push Notifications service is configured, Microsoft Exchange Web Services events are sent.

If you deploy BEMS in a mixed environment, where BEMS and Microsoft Exchange are not co-located, there are additional requirements and prerequisites which may apply. Consider the following scenarios:

Scenario	Tasks
Cloud-based BEMS with on-premises Microsoft Exchange	<ol style="list-style-type: none"> 1. You must expose Microsoft Exchange Web Services and Autodiscover from your on-premises Microsoft Exchange to the Internet on port 443. 2. Both Basic Authentication and Windows authentication are supported for Microsoft Exchange Web Services and Autodiscover.
On-Premises BEMS with Cloud-based Exchange	<ol style="list-style-type: none"> 1. You must expose Microsoft Exchange Web Services and autodiscover from cloud-based Microsoft Exchange to on-premises BEMS on port 443. 2. BEMS supports Modern Authentication and Microsoft Graph.
On-premises BEMS with on-premises and cloud-based Microsoft Exchange	<ol style="list-style-type: none"> 1. You must expose Microsoft Exchange Web Services and autodiscover from cloud-based Microsoft Exchange to on-premises BEMS on port 443. 2. BEMS supports the following: <ul style="list-style-type: none"> • On-premises Microsoft Exchange: Both Basic Authentication and Windows authentication are supported for Microsoft Exchange Web Services and Autodiscover. • Cloud-based Microsoft Exchange: Modern Authentication and Microsoft Graph. 3. The BEMSAdmin account must have impersonation rights on both the on-premises and Microsoft 365 Microsoft Exchange systems. For more information, see Grant application impersonation permission to the service account.

For more information on configuring Microsoft Exchange Web Services and Autodiscover for external access, see the following articles:

- Microsoft Technet:[Configure the Autodiscover Service for Internet Access](#)
- Microsoft Technet:[Configuring EWS for External Access](#)

Grant application impersonation permission to the service account

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

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

Grant application impersonation permissions	Steps
Microsoft 365 using the Exchange Administration Center console	<ul style="list-style-type: none"> a. Sign in to https://admin.exchange.microsoft.com/. b. Click Roles > Admin roles. c. Click Add role group. d. Type a name for the role. e. In the Write scope drop-down list, click Default. f. Click Next. g. In the Search field, search for the ApplicationImpersonation role. Click the checkbox next to the role. h. Click Next. i. In the text field, type the member name or the service account that will process the notifications. j. Click Next. k. Click Add role group. l. Click Done.
On-premises Microsoft Exchange using the Exchange Administration Center	<ul style="list-style-type: none"> a. In a browser window, type <code>https://<url_to_on-premises_client_access_server>/ecp</code> and sign in with a valid account. b. Click permissions. c. Click +. d. Type a name and description for the role group. e. In the Roles section, click +. Click ApplicationImpersonation > add > OK. f. In the Members section, click +. Click an account to add and then click add > OK.
Using Microsoft Exchange Management Shell	<ul style="list-style-type: none"> a. Open Microsoft Exchange Management Shell. b. Type <code>New-ManagementRoleAssignment -Name:<ImpersonationAssignmentName> -Role:ApplicationImpersonation -User:<ServiceAccount></code>. For example, <code>New-ManagementRoleAssignment -Name:BlackBerryAppImpersonation -Role:ApplicationImpersonation -User:BEMSAAdmin</code>. <p>For more information on how to restrict Application Impersonation rights to specific users, organizational units, or security groups, visit the MSDN Library to see How to: Configure impersonation.</p>

Microsoft Exchange Autodiscover

Ensure that your Microsoft Exchange Autodiscover is setup correctly.

The Autodiscover feature in Microsoft Exchange provides the mail client with configuration options and shares only the user's email address and password. This is useful for remote users and smartphone users who do not want to enter advanced settings like server names and domains. It is also required for the correct functioning of features such as out of office and the offline address book in Microsoft Outlook.

Use EWSEditor to test if there are any doubts. For more information, see [KB 40351](#).

Docs prerequisites: CMIS Requirements

Content Management Interoperability Services (CMIS) is an open standard that allows different content management systems to inter-operate over the Internet. The Docs service supports content management systems that support CMIS.

Consult your vendor documentation to determine whether your system is supported by CMIS and whether that support comes via AtomPub or Web Services. If both are supported, Atom Pub is recommended. You must have the binding URL for this support.

Only Microsoft Active Directory users are supported for CMIS. That is, the content management system must be connected to Microsoft Active Directory for user authentication for Docs service to support it.

Connect prerequisites: Skype for Business

The prerequisites discussed here do not apply to Cisco Unified Communications Manager for IM and Presence environments, when Jabber is selected during the BEMS server installation for use with the Connect service.

If your environment uses multiple Skype for Business on-premises servers using trusted application mode or non-trusted application mode, have the Skype for Business servers load balanced with a load balance server. For more information, visit Microsoft resource [Load balancing requirements for Skype for Business](#).

If you configure Connect for Skype for Business with the Connect service trusted by Skype for Business, complete the following pre-requisites:

1. [Create the required BlackBerry Connect service database\(s\)](#).
2. [Prepare the computer that hosts BEMS for use with Skype for Business](#).
3. [Prepare the Skype for Business Topology for Connect](#).
4. [SSL certificate requirements for Skype for Business](#).

If you configure Connect for Skype for Business with the Connect service configured as non-trusted by Skype for Business, complete the following pre-requisites:

1. [Prepare the computer that hosts BEMS for use with Skype for Business](#).
2. [Create the required BlackBerry Connect service database\(s\)](#).

Preparing the computer that hosts BEMS for use with Skype for Business

If you plan to install BEMS for use with Skype for Business, you must verify that the computer that you install BEMS on meets specific requirements.

All instant messaging server platforms require the Connect service to be installed on a computer that runs a supported version of Windows Server. For more information, see [the BEMS Compatibility Matrix](#).

Before you install BEMS, you must perform the following actions in the order listed. Complete these tasks on each computer that hosts the Connect service.

1. Install and enable a command-line shell and scripting tool. On a computer that is running Windows Server 2016, Windows Server 2019, or Windows Server 2022, Windows PowerShell is enabled by default. Open Windows PowerShell and run the following script:

```
Set-ExecutionPolicy -Scope CurrentUser RemoteSigned
```

2. Verify that Microsoft .NET Framework 4.6 or later is installed and enabled. For more information, see [.NET Framework system requirements](#).
3. If needed, install **Media Foundation**. When the installation prompts you to restart the computer, click **Yes**.
4. Download and install the Microsoft Unified Communications Managed API.

If you use Skype for Business 2015 or Skype for Business 2019, download Microsoft Unified Communications Managed API 5.0 Runtime (UcmaRuntimeSetup.exe). To download the file, visit www.microsoft.com/download and search for ID=47344. UCMA 6.0 is not supported.

5. Run **OCSCore.msi**. This file is included with the Microsoft Unified Communications Managed API and located in a hidden folder at `<drive>:\ProgramData\Microsoft\<instant messaging server type>\Deployment\cache\<version>\Setup\`
6. If you enable persistent chat in a Skype for Business 2015 environment, download and install Microsoft Visual C++ 2012 x64 Minimum Runtime. To download the file, click [here](#).

Persistent chat is not supported in a Skype for Business 2019 environment. For more information, see [What's deprecated from Skype for Business Server 2019](#).

7. Install the latest service pack and critical Windows updates on your computer.

Preparing the Skype for Business topology for BEMS

The Connect service and Lync Presence Provider (LPP) are Microsoft Lync trusted-UCMA applications. You must be a member of the RTCUniversalServerAdmins and Domain Admins security groups to provision and publish new applications in the Skype for Business Topology. If you have a designated Skype for Business administrator within your organization, that person should perform all subsequent preparation steps for this procedure.

To provision the computer hosting the Connect and Presence services as a trust application server with Skype for Business, you must use the Skype for Business Management Shell to complete the following tasks:

1. Create a trusted application pool as a virtual container for one or more computers hosting the BEMS-Connect service and the BEMS-Presence service.
2. Designate trusted applications for the use of the BEMS computer.
3. Create a trusted-computer entry for every BEMS in the environment.
4. Create one or more virtual trusted application endpoints for the Presence service.
5. Publish the changes to the Skype for Business topology.

A trusted application pool is a virtual pool or container of one or more trusted application servers, (for example, the Connect service and the Presence service). The trusted application cmdlets define parameters for the services available in the trusted application servers that are associated with the trusted application pool, (for example, the application identifier for Connect service and the Presence service and the listening ports used by these services). The trusted application pool doesn't provide load balancing services for the Connect and Presence services. It only provides configuration and registration information to the Skype for Business to allow the messaging servers to route incoming chat requests or presence status updates to the mobile users being managed by each Connect and Presence service. A BlackBerry Connect app user cannot be represented by more than one BEMS-Connect service at any time. Any type of load balancing or user endpoint distribution is managed by the Connect service directly. For more information about sizing requirements, see the [BEMS Performance Calculator](#).

A trusted application endpoint represents a virtual user to allow the Presence service to subscribe to SIP-enabled users to receive presence availability updates and make this information available to mobile users (for example, BlackBerry Work users). One or more trusted application endpoints must be created for each Presence service on the Skype for Business to process subscriptions. "Trusted application endpoint" only refers to the virtual user used by the Presence service to make the subscription requests. The endpoint remains on the computer hosting the BEMS-Presence service. The Presence service only communicates with the Front End Pool using port 5061. When a subscription is made to a SIP-enabled user to receive availability updates, the Skype for Business Front End Pool sends the user's updated presence status on port 49777 to the Presence service. The number of subscriptions handled by each Presence service and each trusted application endpoint used by the Presence service is managed by the Presence service. For more information about creating trusted application endpoints, see ["Manually configure the Presence service for multiple application endpoints" in the Presence Configuration content](#).

You must complete the application provisioning process described in the following instructions:

- Preparing the initial computer hosting BEMS
- Preparing additional computers hosting BEMS. If you installed the BEMS services on separate computers, you must complete this step for each computer.

After updating the topology, the administrator must delegate RTCUniversalReadOnlyAdmins permission to the BEMS service account for the BEMS Dashboard to access the provisioning information during the BEMS configuration process.

Prepare the initial computer hosting BEMS

When you create a trusted application pool for the installation of BEMS, you also create the trusted-computer entry. Subsequent installations of BEMS machines do not require a new trusted application pool or designated trusted applications because they are added to the existing trusted application pool.

Before you begin: Verify that the account that you use to complete this task is a member of the RTCUniversalServerAdmins group.

1. Log in to the computer that hosts the Skype for Business.
2. Open the **Management Shell**.
3. On the computer that hosts Skype for Business, create the trusted application pool.
 - a) To obtain the SiteID of your Skype for Business, run the following command. Record the SiteID.

```
Get-CsSite
```

- b) To display the Registrar service value for a selected site, run the following command. Record the Registrar service value.

```
Get-CsSite <SiteID> | Select-Object -ExpandProperty Services
```

- c) To configure the trusted application entry for the newly created trusted application pool for BEMS, run the following command:

```
New-CsTrustedApplicationPool -Force -Identity <YourPoolFQDN> -Registrar  
<registrar> -RequiresReplication $false -Site <SiteID> -ComputerFQDN  
<BEMSFQDN>
```

- Where *<YourPoolFQDN>* is the desired FQDN of the virtual Application pool of the BEMS instances.
- Where *<SiteID>* is the SiteID that was recorded in step 3a.
- Where *<registrar>* is the value recorded in step 3b.
- Where *<BEMSFQDN>* is the FQDN of computer hosting BEMS.

For example, `New-CsTrustedApplicationPool -Force -Identity BEMSAppPool.mycompany.com -Registrar registrar.mycompany.com -RequiresReplication $false -Site 1 -ComputerFQDN BEMSHost.mycompany.com`

Prepare additional computers hosting BEMS

Before you begin:

- Verify that a BEMS server is installed in your environment, and a trusted application pool and trusted computer entry is created according to the instructions in [Prepare the initial computer hosting BEMS](#).
- Verify that the account that you use to complete this task is a member of the RTCUniversalServerAdmins group.

1. Log in to the computer that hosts the Skype for Business using an account with RTCUniversalServerAdmins group permissions.
2. Open the **Management Shell**.
3. On the computer that hosts Skype for Business, create the trusted computer for the BEMS trusted application pool.
 - a) To add the trusted computer for the BEMS trusted application pool, run the following command:

```
New-CsTrustedApplicationComputer -Identity <BEMSFQDN> -Pool <YourPoolFQDN>
```

- Where <BEMSFQDN> is the FQDN of computer hosting BEMS.
- Where <name of BEMS pool previously created> is the name of the BEMS pool in step 3c of [Prepare the initial computer hosting BEMS](#).

For example: `New-CsTrustedApplicationComputer -Identity BEMSHost2.mycompany.com -Pool BEMSAppPool.mycompany.com`

4. If the computer hosting BEMS runs the BEMS Presence service, create an application endpoint. Run the following command:

```
New-CsTrustedApplicationEndpoint -ApplicationId <appid_presence> -TrustedApplicationPoolFqdn <YourPoolFQDN> -SipAddress "sip:presence_<BEMSFQDN>@"
```

Where <appid_presence> is the desired application ID of the BEMS Presence service.

For example: `New-CsTrustedApplicationEndpoint -ApplicationId appid_presence -TrustedApplicationPoolFqdn BEMSAppPool.mycompany.com -SipAddress "sip:presence_BEMSHost2.mycompany.com@mycompany.com"`

5. To publish the change to Skype for Business environment, run the following command:

```
Enable-CsTopology
```

Creating an additional trusted application pool

One BlackBerry Connect instance can be associated with only one Trusted Application Pool. In a high availability or disaster recovery scenario, it is recommended that you create an additional trusted application pool in your Front-End high availability and disaster recovery pool for your Connect high availability and disaster recovery instances.

The steps for creating an additional trusted application pool are the same as creating your first trusted application pool for Connect with the exception that trusted application pool names must be unique. Therefore, if you named your first trusted application pool "pool1_bems.example.com", then your second trusted application pool name must be different. For example, "pool2_bems.example.com".

Remove provisioning of the BEMS as a trusted application and trusted application pool

You can use Windows PowerShell to remove the provisioning of the BEMS as a trusted application software and trusted application pool before you remove the Connect service and Presence service from the BEMS instances in your organization's network.

When you remove provisioning of BEMS as a trusted application, the provisioning record is removed from Microsoft Active Directory. When the provisioning record is removed from Microsoft Active Directory, BEMS remains running, but the communication to the Microsoft Lync Server stops.

If your environment is running Skype for Business, you must remove provisioning of the BEMS as a trusted application and trusted application pool using the Microsoft Lync Server Management Shell that you used to create it.

1. Log in to the computer that hosts Skype for Business using an account with RTCUniversalServerAdmins group rights.
2. Open a Management Shell window and complete the following steps:
 - a) To display the Trusted Application Pool that the computer is a part of, run the following command. Record the Pool name.

```
Get-CsTrustedApplicationComputer -Identity <FQDN_of_the_bems_host>
```

- b) To display all the computers in the Pool name recorded in step 2a, run the following command. Record if more than one FQDN entry is listed.

```
Get-CsTrustedApplicationPool -pool <FQDN_of_the_pool_from_step_a>
```

- c) To display additional information about the above Trusted Application Pool, run the following command:

```
Get-CsTrustedApplicationPool -PoolFqdn <FQDN_of_the_pool_from_step_a>
```

- d) To remove one BEMS instance from the trusted application pool when you have more than one BEMS instance in your organization's environment, run the following command:

```
Remove-CsTrustedApplicationComputer -Identity <FQDN_of_the_bems_host>
```

- e) To remove all BEMS instances from the Trusted Application Pool and remove the pool itself, run the following command:

```
Remove-CsTrustedApplicationPool -Identity <FQDN_of_the_pool_from_step_2a>
```

- f) To publish the change to the Skype for Business environment, run the following command:

```
Enable-CsTopology
```

- g) To verify that the trusted application pool is removed, run the following command:

```
Get-CsTrustedApplicationComputer -Identity <FQDN_of_the_bems_host>
```

SSL certificate requirements for Skype for Business

If your enterprise doesn't already have one, or one designated for use by BEMS, you must obtain and install a digital certificate.

Your enterprise can sign its own digital certificates, acting as its own certificate authority (CA), or you can submit a certificate request to a well-known, third-party CA. Although you can preinstall the root authority for your own CA on each user's device, it makes sense to get an independent CA-validated certificate.

In the following sections, references to SSL, CA-signed, and personal certificates refer to the digital certificate.

Mutual TLS (MTLS) certificates

Connect and Lync Presence Provider (LPP) connections to Skype for Business rely on mutual TLS (MTLS) for mutual authentication. On an MTLS connection, the server originating a message and the server receiving it exchange certificates from a mutually trusted CA. The certificates prove the identity of each server to the other.

In Skype for Business deployments, certificates issued by the enterprise CA that are valid and not revoked by the issuing CA are automatically considered valid by all internal clients and servers because all members of a Microsoft Active Directory domain trust the Enterprise CA in that domain. In federated scenarios, the issuing CA must be trusted by both federated partners. Each partner can use a different CA, if desired, so long as that CA is

also trusted by the other partner. This trust is most easily accomplished by the Edge Servers having the partner's root CA certificate in their trusted root CAs, or by use of a third-party CA that is trusted by both parties.

Hence, BEMS must form a mutual trust relationship for MTLS communications supporting its network server environment. Mutual trust requires a valid SSL certificate that meets the following criteria:

- The following certificates must be stored on the computer that hosts BEMS in the Windows Certificate store. You can access the certificates using the Microsoft Management Console (MMC).
 - The private certificate issued for BEMS by a trusted CA and that is accessible using the Microsoft Management Console (MMC) in the Console Root\Certificates <local_host_name>\Personal\Certificate folder.
 - The BEMS computer's private certificate and the Skype for Business internal computer certificate must both be trusted by root certificates and accessible using the Microsoft Management Console (MMC) in the Console Root\Certificate <local_host_name>\Trusted Root Certification Authorities\Certificates folder.
 - Intermediate certificates for both the BEMS private certificate and the Skype for Business internal computer certificate and accessible using the Microsoft Management Console (MMC) in the Console Root\Certificates <local_host_name>\Intermediate Certification Authorities\Certificates folder.
- The Subject Name certificate property must contain the Common Name (CN) of a valid FQDN such as a trusted application pool name (for example, CN=bemsappool.example.com). For more information about the trusted application pool name, see [Prepare the initial computer hosting BEMS](#).
- The Subject Alternative Name (SAN) certificate property must include the FQDN for the trusted application pool and the FQDN of each BEMS instance that the certificate will be used for (for example, bemsappool.example.com, bemsserver01.example.com, bemsserver02.example.com, bemserver03.example.com, and so forth).
- The certificate must be signed by a CA that is mutually trusted by both Skype for Business and BEMS.

The account used to run BEMS must have read access to the certificate store and the private key. You can assign read rights to the private key by right-clicking on the certificate.

For more information about generating SSL certificates with subject alternative names, see the Microsoft resource [How to generate a certificate with subject alternative names \(SAN\)](#).

Steps to create a CA-signed certificate for the local computer account using a CSR for BEMS

When you create a CA-signed certificate for the local computer account for BEMS that can be used on all computers hosting BEMS, you perform the following actions.

Step	Action
1	Create a CSR for the local computer account for BEMS
2	Obtain a CA-signed certificate from the CA server
3	Import the CA-signed certificate on the CSR requesting BEMS
4	Export the CA-signed certificate and private key from the Microsoft Management Console

Step	Action
5	Import the CA-signed certificate and private key to additional BEMS instances

Steps to create a CA-signed for the local computer account using automatic enrollment for BEMS

When you create a Personal Certificate for the local computer account for BEMS that can be used on all computers hosting BEMS, you perform the following actions.

Step	Action
1	Create a Personal Certificate for the local computer account for BEMS
2	Export the CA-signed certificate and private key from the Microsoft Management Console
3	Import the CA-signed certificate and private key to additional BEMS instances

Create a CSR for the local computer account for BEMS

If you want to use an enterprise CA to generate the SSL certificate, you must create a custom request on a computer that hosts BEMS.

1. On the computer that hosts BEMS, open the Microsoft Management Console.
2. Click **Console Root**.
3. Click **File > Add/Remove Snap-in**.
4. In the **Available snap-ins** column, click **Certificates**. Click **Add**.
5. In the **Certificates snap-in** wizard, select **Computer account**. Click **Next**.
6. On the **Select Computer** screen, select **Local computer**.
7. Click **Finish**. Click **OK**.
8. In the Microsoft Management Console, expand **Certificates (Local Computer)**.
9. Right-click **Personal**, then click **All Tasks > Advanced Operations > Create Custom Request**.
10. In the **Certificate Enrollment wizard**, click **Next**.
11. Click **Proceed without enrollment policy**. Click **Next**.
12. On the **Custom request** screen, click **Next**.
13. On the **Certificate Information** screen, click the **Details > Properties**.
14. On the **Subject** tab, in the **Subject name** section, complete the following actions:
 - a) In the **Type** drop-down list, click **Common Name**.
 - b) In the **Value** field, type a valid FQDN such as a trusted application pool name (for example, CN=bemsappool.example.com) that was recorded in step 3c of [Prepare the initial computer hosting BEMS](#).
 - c) Click **Add**.
15. In the **Alternative name** section, add the following values:
 - a) In the **Type** drop-down list, click **DNS**.

- b) In the **Value** field, type the FQDN of the trusted application pool (for example, bemsappool.example.com).
- c) Click **Add**.
- d) In the **Value** field, type the FQDN of a BEMS instance that the certificate will be used for (for example, bemsserver01.example.com).
- e) Click **Add**.
- f) Repeat steps d and e for each BEMS instance that the certificate will be used for (for example, bemsserver02.example.com, bemserver03.example.com, and so forth).

16. Optionally, on the **General** tab, specify a friendly name for the certificate. The name of the template is often the only way to distinguish its purpose and must be unique. This is important when deploying the final name of the issued certificate, which should always match the designated service name. For more information about using friendly names for certificates in Connect and Presence, see ["Using friendly names for certificates in BlackBerry Connect" in the Connect configuration content](#) and ["Using friendly names for certificates in BlackBerry Presence" in the Presence configuration content](#).

17. On the **Private Key** tab, in the **Key options**, verify that **Make private key exportable** is selected.

18. Click **Apply**.

19. Click **OK**.

20. Click **Next**.

21. Save the certificate information to your desktop with a file format of Base 60.

22. Click **Finish**.

After you finish: [Obtain a CA-signed certificate from the CA server](#)

Obtain a CA-signed certificate from the CA server

Before you begin: Verify that you have access to the CSR file that was created in [Create a CSR for the local computer account for BEMS](#).

1. Open the CSR certificate information and copy the certificate information, including the Begin and End Certificate request lines.
2. Access the CA server and obtain the CA-signed certificate.

After you finish: [Import the CA-signed certificate on the CSR requesting BEMS](#).

Import the CA-signed certificate on the CSR requesting BEMS

You must import the CA-signed certificate on the BEMS instance that requested the CSR to pair the public and private keys.

Before you begin: Verify that you have access to the CA-signed certificate that you obtained.

1. On the computer that hosts BEMS, in the **Microsoft Management Console**, expand **Personal**.
2. Right-click **Certificates**, then click **All Tasks > Import**.
3. Click **Next**.
4. Navigate to the signed CA-certificate that you obtained. Click **Next**.
5. Click **Next** again.
6. Click **Finish**.

After you finish: [Export the CA-signed certificate and private key from the Microsoft Management Console](#)

Create a Personal Certificate for the local computer account for BEMS

Complete this task on each computer that hosts the Presence and/or Connect service. You can create one certificate to be used for all BEMS instances.

1. On the computer that hosts BEMS, open the Microsoft Management Console.
2. Click **Console Root**.
3. Click **File > Add/Remove Snap-in**.
4. In the **Available snap-ins** column, click **Certificates**. Click **Add**.
5. In the **Certificates snap-in** wizard, select **Computer account**. Click **Next**.
6. On the **Select Computer** screen, select **Local computer**.
7. Click **Finish**. Click **OK**.
8. In the Microsoft Management Console, expand **Certificates (Local Computer)**.
9. Right-click **Personal**, then click **All Tasks > Request New Certificate**.
10. In the **Certificate Enrollment wizard**, click **Next**. Click **Next** again.
11. Select an appropriate web server template from the available templates.
 - a) Click **Details** to verify that the Server Authentication is displayed in the Application Policies section.
 - b) In the **Application policies** section, verify that **Server Authentication** is listed. If Server Authentication is not listed, select a different web server template. Contact your CA administrator for more information about templates.
12. Click **More information is required to enroll for this certificate. Click here to configure settings**.
13. On the **Subject** tab, in the **Subject name** section, complete the following actions:
 - a) Click the **Type** drop-down list. Select **Common Name**.
 - b) In the **Value** field, type a valid FQDN such as a trusted application pool name (for example, CN=bemsappool.example.com) that was recorded in step 3c of [Prepare the initial computer hosting BEMS](#).
 - c) Click **Add**.
14. In the **Alternative name** section, add two values by completing the following actions:
 - a) Click the **Type** drop-down list. Select **DNS**.
 - b) In the **Value** field, type the FQDN of the trusted application pool (for example, bemsappool.example.com).
 - c) Click **Add**.
 - d) In the **Value** field, type the FQDN of a BEMS instance that the certificate will be used for (for example, bemsserver01.example.com).
 - e) Click **Add**.
 - f) Repeat steps d and e for each BEMS instance that the certificate will be used for (for example, bemsserver02.example.com, bemserver03.example.com, and so forth).
15. Optionally, on the **General** tab, specify a friendly name for the certificate. The name of the template is often the only way to distinguish its purpose and must be unique. This is important when deploying the final name of the issued certificate, which should always match the designated service name. For more information about using friendly names for certificates in Connect and Presence, see ["Using friendly names for certificates in BlackBerry Connect" in the Connect configuration content](#) and ["Using friendly names for certificates in BlackBerry Presence" in the Presence configuration content](#).
16. On the **Private Key** tab, in the **Key options**, verify that **Make private key exportable** is selected.
 - a) Click the **Private Key** tab.
 - b) Click the **Key options** drop-down list. Select the **Make private key exportable** check box.
17. Click **Apply**.
18. Click **OK**.
19. Click **Enroll**.
20. Click **Finish**.

After you finish:

- Grant the service account read access to the certificate. Right-click the certificate and click **All Tasks > Manage Private Keys**. On the **Security** tab, add the service account.
- Export the certificate and the private key, then import the certificate to each of the other computers that host a BEMS instance. For instructions, see [Export the CA-signed certificate and private key from the Microsoft Management Console](#) and [Import the CA-signed certificate and private key to additional BEMS instances](#) respectively.

Export the CA-signed certificate and private key from the Microsoft Management Console

Export the certificate from the Microsoft Management Console (MMC). Include the private key and save it as a .pfx file. For more information, see the Microsoft resource [Export a Certificate with the Private Key](#).

Before you begin: Verify that you created a CA-signed certificate for the local computer account to use on multiple BEMS instances running the Connect and/or Presence services. For instructions on creating a CA-signed certificate using automatic enrollment, see [Create a Personal Certificate for the local computer account for BEMS](#). For instructions on creating a CA-signed certificate using a CSR, see [Create a CSR for the local computer account for BEMS](#).

1. On the computer that hosts BEMS, open the Microsoft Management Console.
2. Expand **Personal**.
3. Click **Certificates**.
4. Right-click the personal certificate that you created and click **All Tasks > Export**.
5. In the **Certificate Export Wizard**, select **Yes, export the private key**.
6. Click **Next**.
7. Verify that the **Include all certificates in the certification path if possible** check box is selected. Clear the other check boxes.
8. Select the appropriate security method and enter the required security information. Click **Next**.
If you select Groups and users, make sure that you log on to the BEMS instance where the certificate will be imported as the user or member of that group.
9. Click **Browse** to specify a name for the certificate and save it to your desktop.
10. Click **Next**.
11. Click **Finish**.
12. Click **OK**.

After you finish: [Import the CA-signed certificate and private key to additional BEMS instances](#).

Import the CA-signed certificate and private key to additional BEMS instances

Complete this task on each computer that hosts the Presence and/or Connect service and is configured to use Skype for Business. You can use one signed certificate for multiple BEMS instances. For more information, see the Microsoft resource [Import a Certificate](#).

Before you begin:

- Verify that you have the access to the exported signed certificate. Instructions, see [Export the CA-signed certificate and private key from the Microsoft Management Console](#).
 - If the certificate was exported and a security principal was specified, you must log in as a member of that specified group or user.
 - Make sure that you have the password that is assigned to the exported certificate.
1. On the computer that hosts BEMS, open the Microsoft Management Console.
 2. Expand **Personal**.
 3. Right-click **Certificates**, then click **> All Tasks > Import**.

4. Click **Next**.
5. Navigate to the certificate that you want to import. Click **Next**.
6. Enter the password for the private key. Click **Next**.
7. Click **Finish**.

Presence prerequisites: Skype for Business

For Skype for Business, the Presence service has the same predeployment requirements as the Connect service.

Presence for Skype for Business on-premises using non-trusted application mode doesn't use the Good Technology Presence service. Therefore, there is no requirement to start the service, and no requirement to make sure that an MTLS certificate is issued for the Presence service to use. Presence status is provided by Good Technology Common Services service.

Presence Prerequisites: Cisco Unified Communications Manager IM and Presence Service

Turn off antivirus software for computers running BEMS with Connect-Presence.

Create an Application User

This application user is a logical entity that represents a third-party application that can log into Cisco Unified CM IM and Presence.

1. Log in to the Cisco Unified Communications Manager Administration console.
2. Click **User Management > Application User**.
3. Click **Add New**.
4. Type a User ID and password and confirm the password.
5. In the **Permissions Information** section, click **Add to Access Control Group**.
6. In the **Find and List Access Control Groups** window, select the **Admin-3rd Party API** checkbox.
7. Click **Add Selected**.
8. Click **Close** and save.

Create a Dummy User

Use this dummy UDS user to log in to Cisco Unified CM IM and Presence Administration as an end user and get presences of other LDAP end users.

If the customer has configured single sign-on, the dummy user must be synchronized from LDAP directory to the CUCM.

1. Log into Cisco Unified Communications Manager Administration console.
2. Click **User Management > End User**.
3. Click **Add New**.
4. Type a User ID, password, and confirm password for the dummy user account.
5. Select the **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile) checklist** to enable the user for presence.
6. Click **Save**.

Configure Cisco Unified Communications Manager and Cisco IM and Presence certificates with the enterprise certificate authority

Cisco Unified Communications Manager (CUCM) and Cisco IM and Presence (CIMP) provide the ability to use multi-server certificates with Subject Alternative Names for tomcat, cup-xmpp, and cup-xmpp-ECDSA services. This topic describes certificate configuration using these recent feature enhancements. Multi-server certificates need only be configured on the CUCM and CIMP Publishers. Regardless of CIMP version, the cup service certificate is not multi-server and must be configured on each CIMP server in the cluster.

If your environment is not using multi-server certificates, you must use the Cisco Operating System Administration user interface on all of the CUCM and CIMP nodes to configure the Tomcat certificates. You must use the Cisco Operating System Administration interface on all of the CIMP nodes to configure the cup, cup-xmpp, and cup-xmpp-ECDSA certificates. The Cisco Tomcat service runs on both CUCM and CIMP servers. The cup, cup-xmpp, and cup-xmpp-ECDSA services only run on the CIMP servers.

When you configure the Presence service to communicate with CUCM and CIMP, you can configure the Cisco certificates to be signed by the enterprise certificate authority. You require the following certificates and certificate signing requests (CSR) when you want to configure the Presence service to communicate with the Cisco Unified Communications Manager and Cisco IM and Presence:

Service	Certificates or CSRs
Configure the Connect service only ¹	<ul style="list-style-type: none"> Enterprise Root CA certificate Tomcat Certificate Signing Request (from CUCM) Tomcat - CA signed certificate Tomcat - ECDSA CA signed certificate Cup-xmpp Certificate Signing Request (from CIMP) Cup-xmpp CA signed certificate Cup-ECDSA CA signed certificate (from CIMP) Cup-xmpp-ECDSA CA signed certificate (from CIMP)
Configure the Presence service only ¹	<ul style="list-style-type: none"> Enterprise Root CA certificate Tomcat Certificate Signing Request (from CUCM) Tomcat - CA signed certificate Tomcat - ECDSA CA signed certificate Cup Certificate Signing Request (from CIMP) Cup - CA signed certificate Cup-ECDSA CA signed certificate (from CIMP) Cup-xmpp-ECDSA CA signed certificate (from CIMP)

¹ If you configure both the Connect and Presence services, make sure that all of the required certificates or CSRs uploaded.

Note: You must upload the root CA certificate as a trust certificate for the corresponding services or you will receive the error message **CA certificate is not available in the trust-store**. For example, if you want to use a CA-signed tomcat certificate, you must first upload the root CA certificate as a tomcat-trust certificate, if you want to use a CA-signed cup certificate, you must first upload the root CA certificate as a cup-trust certificate, and if you want to use a CA-signed cup-xmpp certificate, you must first upload the root CA certificate as a cup-xmpp-trust certificate.

1. Complete steps 2 to 10 for all of the certificate pairs. For example, tomcat/tomcat-trust, cup/cup-trust, cup-xmpp/cup-xmpp-trust, and cup-xmpp-ECDSA/cup-xmpp-trust.

2. Log in to the **Cisco Unified OS Administration** using your administrator credentials. Complete the following tasks on the CUCM Publisher and the IM and Presence Publisher. For the cup service certificate, complete the following tasks on all servers in the cluster.
3. Click **Security > Certificate Management**.
4. Upload the root enterprise CA certificate.
The uploaded certificate is distributed to all of the servers in the cluster for the given service (for example, tomcat, cup, cup-xmpp, and cup-xmpp-ECDSA).
 - a) Click **Upload Certificate/Certificate chain**.
 - b) In the **Certificate Purpose** drop-down list, select the trust store (For example, tomcat-trust, cup-trust, or cup-xmpp-trust).
 - c) Click **Browse**. Navigate to the enterprise root certificate downloaded earlier.
 - d) Click **Open**.
 - e) Click **Upload**.
 - f) If the certificate upload is successful, click **Close**.
5. Request a CSR.
 - a) Click **Generate CSR**. The new CSR will overwrite the existing CSR for that certificate.
 - b) In the **Certificate Purpose** drop-down list, click the service you want to generate the CSR for. For example, tomcat, cup, or cup-xmpp.
 - c) In the **Distribution** drop-down list, select **Multi-server (SAN)**.
Note: Make sure that the list of auto-populated domains in the Subject Alternate Names section contain the FQDNs of the CUCM and CIMP servers that will be configured in BEMS.
 - d) Click **Close**. A second copy of the *<service>* certificate appears in the certificate list as a CSR Only type.
 - e) Click the CSR Only type version of the *<service>* certificate link.
 - f) In the **CSR Details for <Publisher_Hostname-ms.domain>, <service> certificate** dialog box, click **Download CSR**.
 - g) Save the *<service>.csr* file. Open the file in a text editor.
 - h) Copy the certificate information, including the Begin and End Certificate request lines.
6. Paste the new CSR certificate information to the Microsoft Active Directory Certificate Services server.
 - a) On the **Microsoft Active Directory Certificate Services** server, click **Request a certificate**.
 - b) Click **Advanced certificate request**.
 - c) On the **Submit a Certificate Request or Renewal request** window, in the **Saved Request** field, paste the certificate information that you copied in step 5h.
 - d) In the **Certificate Template** drop-down list, click **Web Server**.
 - e) Click **Submit**.
 - f) On the **Certificate Issued** window, select **DER encoded**. Click **Download certificate**.
 - g) Click **OK**. By default, the certificate is saved to the Downloads folder.
7. Upload the CA-signed certificate to Cisco Unified Operating System Administration web page to replace the CSR Only version of the appropriate service certificate with the CA-signed version.
 - a) On the **Cisco Unified Operating System Administration** web page, click **Upload Certificate/Certificate chain**.
 - b) Click **OK**.
 - c) Click **Close**. The CSR version of the *<service>* certificate changes to CA-signed.
8. Restart Cisco Services on all IM and Presence nodes.
 - a) Log in to the **Cisco Unified IM and Presence Serviceability** server.
 - b) Click **Tools > Control Center - Network Services**.
 - c) In the **Server** drop-down list, select the IM and Presence server. Click **Go**.
 - d) Under **IM and Presence Services**, select **Cisco XCP Router**.

- e) Click **Restart**. Click **OK**.
 - f) Click **Tools > Control Center - Feature Service**.
 - g) In the **Server** drop-down list, select the IM and Presence server. Click **Go**.
 - h) Under **IM and Presence Services**, select **Cisco SIP Proxy**.
 - i) Click **Restart**. Click **OK**.
 - j) Repeat steps h and i for **Cisco Presence Engine**.
9. Restart the **Cisco Tomcat Service** using SSH on all CUCM and CIMP nodes.
In a command prompt, type `utils service restart Cisco Tomcat`.

Prerequisites: BlackBerry Directory Lookup, BlackBerry Follow-Me, and BlackBerry Certificate Lookup services

The BlackBerry Directory Lookup, BlackBerry Follow-Me, and BlackBerry Certificate Lookup services are installed with the BlackBerry Push Notifications (Core and Mail) service and share the same prerequisites.

Installing or upgrading the BEMS software

You can download and install BEMS from the Software Downloads page in the [BlackBerry myAccount portal](#). To allow users in your environment to use the latest features available with BEMS, it is recommended that you upgrade your BEMS instances and BlackBerry Dynamics apps on user devices to the latest software versions. BEMS installations are supported only on English implementations of the OS.

Supported installation and upgrade paths

You can use the setup application to install the BEMS software or to upgrade from up to two previous versions of BEMS. For more information about supported upgrade paths, see [KB 53472](#).

If you are upgrading from a previous version of BEMS, verify that your servers meet the requirements for the BEMS configuration you are upgrading to.

If you have multiple instances of BEMS in your environment, you must complete this task on each computer that hosts an instance of BEMS.

Best practices: Preparing to upgrade

When you upgrade from an earlier version of BEMS, consider the following guidelines:

- Administrators must provide their Microsoft Active Directory user credentials to log in to the BEMS Dashboard during the upgrade.
- If you are upgrading multiple instances in a cluster, you must upgrade each computer that hosts an instance of BEMS.
- If multiple BEMS instances point to a shared (common) database, new features are not available until all instances are upgraded. Running in a mixed-version environment for an extended period is not recommended.
- Special characters, for example semicolon (;), at sign (@), and slash mark (/), are not supported for the BEMS service account.

BEMS setup application modes

When you have installed a BEMS instance in your environment and you run the setup application, the following three options are available: Modify, Repair, and Uninstall.

- **Modify:** Select this option to make changes to your environment such as add or remove BEMS services (for example, BEMS-Presence or BEMS-Connect). For more information on how to use the Modify option to remove one or more BEMS services, see [KB 82381](#).
- **Repair:** Select this option to make changes to the BEMS instance such as move the BEMS database to a new Microsoft SQL Server, change service account credentials and log file locations, and rebuild the BEMS jetty keystore if it is missing. This option does not resolve issues that might be encountered such as resetting configuration files. For more information on how to use the Repair option, see the appropriate content below:
 - To move the BEMS databases to a new SQL Server instance, see [KB 45396](#).
 - To change the BEMS service account and account password, see [KB 58463](#).
 - To change the log file location, see [KB 42316](#).
 - To rebuild the jetty keystore, see [KB 57959](#).
- **Uninstall:** Select this option to remove the BEMS software from the computer that hosts the BEMS instance.

Install the BEMS software

BEMS installations are supported only on English implementations of the operating system.

Before you begin:

- [Verify that you completed the preinstallation and prerequisite requirements.](#)
- If your organization uses AlwaysOn support for SQL Server, complete the steps in [Appendix: AlwaysOn Availability support for SQL Server](#) and verify that you have the FQDN of the AlwaysOn Listener and name of the database that is added to the AlwaysOn Availability Group available before you install the BEMS software. For information about supported SQL Server versions, see the [BEMS Compatibility Matrix](#). When you install the BEMS services on separate computers, all steps will not apply. Complete this task on each computer that you install one or more services on.
- By default, encrypt=false is prepopulated in the Additional properties, so data between BEMS and the SQL Server is not encrypted. If your environment requires data to be encrypted, and requires verification of the TLS certificate, you must change the encrypt option in the Additional properties to true and add trustServerCertificate=false separated by a semicolon (no space before or after the semicolon) during the installation or after in the Dashboard. Make sure that you first import the CA certificate that is signing your SQL Server certificate into the Java certificate store before you change the properties, or BEMS will be unable to connect to the SQL Server database. For more information, see [Import the CA certificate into the Java certificate store](#).
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. Log in to the computer that you want to install BEMS on using the BEMS service account.
2. Copy the installation files to the computer.
3. Extract the content to a folder on the computer.
4. In the **GoodEnterpriseMobilityServer** installation folder, double-click **InstallBEMS.bat**. If you double-click **GoodEnterpriseMobilityServer.<version number>.exe**, the installer fails, and the following error message appears: "Could not find a valid Java machine to load."
If a Windows message appears and requests permission for **GoodEnterpriseMobilityServer.<version number>.exe** to make changes to the computer, click **Yes**. If a supported version of Java isn't installed on the computer or the JAVA_HOME system variable isn't specified correctly, an error message indicates that a supported version of Java is required. For more information, see [Set an environment variable for the Java location](#).
5. Click **Next**.
6. Accept the license agreement and click **Next**.
7. In the **Services** dialog box, select the services you want to install. Click **Next**.
8. In the **Prerequisite** dialog box, click **Next**.
If the Prerequisite dialog box displays a warning that a prerequisite is not met, you must cancel the installation and complete the prerequisites before you can start the installation again.
9. In the **Host information** dialog box, verify the BEMS hostname and Domain name. If necessary, select **Modify these values** and type the new hostname and domain name.
10. Click **Next**.
11. In the **Choose Install Folder** dialog box, click **Next** to accept the default installation folder location.
12. In the **Choose Logs Folder** dialog box, click **Next** to accept the default log file folder location.
13. In the **Administration Information** dialog box, select **This Account (domain\user)** and type the login credentials for the BEMS service account you created in [Set an environment variable for the Java location](#). Click **Next**.

14. In the **Database Information** dialog box, perform the following actions:

- a) Specify the Microsoft SQL Server connection information for the BEMS-Core service database. This content prepopulates the BEMS-Core database screen (BEMS System Settings > Database) in the Dashboard. For more information, see [BEMS-Core database](#).

Field	Description
Host	Type the FQDN and, if applicable, the SQL instance name of your SQL Server. For example, SQL Express or SQL Server using a SQL Instance name: <i><server name>\<database instance name></i> SQL Express or SQL Server using a SQL Instance name: <i><server name>\<database instance name></i> . If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener.
Database name	Type the name for the BEMS-Core database. For information on database names based on the configuration of your environment, see Create the BEMS services databases . If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group
Port	Type the port number that connects to the SQL Server. If the SQL Server instance is using dynamic ports, leave this field blank. By default, this port is 1433 if a static TCP/IP port is used. To use SQL Server dynamic TCP/IP ports, make sure that the SQL Server Browser service is running
Authentication Type	Specify the SQL Server connection information for the BEMS-Connect service database and enter the BEMS service account login credentials under which the BEMS-Connect Windows service run.
Additional Properties	Optional. Specify any connection properties (for example, name1=value1; name2=value2, and so on). For more information, visit docs.microsoft.com to see Setting the connection properties . If your environment uses AlwaysOn with multisubnet deployment, type <code>MultiSubnetFailover=true</code> .

- b) Enter the BEMS service account login credentials under which the BEMS-Connect Windows service will run.
- c) Specify the SQL Server connection information for the BEMS-Connect service database.

Field	Description
Host	Type the FQDN and, if applicable, the SQL instance name of your SQL Server. For example, SQL Express or SQL Server using a SQL Instance name: <i><server name>\<database instance name></i> SQL Express or SQL Server using a SQL Instance name: <i><server name>\<database instance name></i> . If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener.
Database name	Type the name for the BEMS-Connect database. For information on database names based on the configuration of your environment, see Create the BEMS services databases . If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group

Field	Description
Port	Type the port number that connects to the SQL Server. If the SQL Server instance is using dynamic ports, leave this field blank. By default, this port is 1433 if a static TCP/IP port is used.
Authentication Type	Specify the SQL Server connection information for the BEMS-Connect service database and enter the BEMS service account login credentials under which the BEMS-Connect Windows service run.
Additional Properties	Optional. Specify any connection properties (for example, name1=value1; name2=value2, and so on). For more information, visit docs.microsoft.com to see Setting the connection properties . If your environment uses AlwaysOn with multisubnet deployment, type <code>MultiSubnetFailover=true</code> .

- d) Enter the BEMS service account login credentials under which the BEMS-Presence Windows service run. Note that a database is not required for the Presence service if all of the BEMS services are installed on one computer. For more information, see [Create the BEMS services databases](#).
- e) Specify the SQL Server connection information for the BEMS-Docs service database.

Field	Description
Host	Type the FQDN and, if applicable, the SQL instance name of your SQL Server. For example, SQL Express or SQL Server using a SQL Instance name: <code><server name>\<database instance name>SQL Express or SQL Server using a SQL Instance name: <server name>\<database instance name></code> . If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener.
Database name	Type the name for the BEMS-Docs database. For information on database names based on the configuration of your environment, see Create the BEMS services databases . If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group
Port	Type the port number that connects to the SQL Server. If the SQL Server instance is using dynamic ports, leave this field blank. By default, this port is 1433 if a static TCP/IP port is used.
Authentication Type	Specify the SQL Server connection information for the BEMS-Docs service database and enter the BEMS service account login credentials under which the BEMS-Connect Windows service run.
Additional Properties	Optional. Specify any connection properties (for example, name1=value1; name2=value2, and so on). For more information, visit docs.microsoft.com to see Setting the connection properties . If your environment uses AlwaysOn with multisubnet deployment, type <code>MultiSubnetFailover=true</code> .

15. In the **Pre-installation Summary** dialog box, click **Install**.

16. In the **Installing** dialog box, click **Next** when the installation of a BEMS service is complete.

17. In the **Install Complete** dialog box, click **Done**.

18. In a browser, open the BEMS Dashboard at <https://localhost:8443/dashboard>.

After you finish: Complete the component configuration in the Dashboard. For information, see [Configuring the BEMS services](#).

Upgrade the BEMS software

When you perform an in-place upgrade of the BEMS instance, you upgrade the existing services only. During the upgrade process you cannot add, change, or remove services. During the upgrade process, notifications are suspended. The BEMS log files, Windows event logs, and the database record the upgrade as BEMS being in maintenance mode. After the upgrade is complete, the log files, event logs, and database show BEMS as being in upgraded mode. A restart of the computer might be required. For more information, see [Standard InstallAnywhere Variables](#).

If you installed the BEMS services on separate computers, complete this task on each computer that you installed a service on. Depending on the services that you install on the computer, some steps might not apply.

Note: When you upgrade to JRE 17, it is a best practice to uninstall JRE 8 after the upgrade is complete, to allow for potential rollback if necessary.

Before you begin: The BEMS instance must be fully functional, and the Good Technology Common Services service must be running to perform an in-place upgrade of the BEMS software.

- Make sure you log in with the BEMS service account you created to install BEMS.
- [Verify that you completed the prerequisites and preinstallation and tasks](#).
- Verify that the BEMS debug logging level is not set to Debug or Trace, or the upgrade or repair of the BEMS instance fails. For more information, visit [KB 42408](#).
- Verify that you have the password for the BEMS service account.
- If you upgrade BEMS in a cluster environment, back up the BEMS cluster database.
- By default, `encrypt=false` is prepopulated in the Additional properties, so data between 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, you must change the `encrypt` option in the Additional properties to `true` and add `trustServerCertificate=false` separated by a semicolon (no space before or after the semicolon) during the installation or after in the Dashboard. Make sure that you first import the CA certificate that is signing your SQL Server certificate into the Java certificate store before you change the properties, or BEMS will be unable to connect to the SQL Server database. For more information, see [Import the CA certificate into the Java certificate store](#).

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. Log in to the computer that hosts BEMS using your BEMS service account.
2. Copy the installation files to the computer.
3. Extract the contents to a folder on the computer.
4. In the **GoodEnterpriseMobilityServer** installation folder, double-click **InstallBEMS.bat**. If you double-click `GoodEnterpriseMobilityServer.<version number>.exe`, the installer fails, and the following error message appears: "Could not find a valid Java machine to load."

If a Windows message appears and requests permission for **GoodEnterpriseMobilityServer.<version number>.exe** to make changes to the computer, click **Yes**. If a supported version of Java isn't installed on the computer or the `JAVA_HOME` system variable isn't specified correctly, an error message indicates that a supported version of Java is required. For more information, see [Set an environment variable for the Java location](#).

5. In the **BlackBerry Enterprise Mobility Server v<version number> setup** screen, in the **Introduction** dialog box, select **Upgrade**. Click **Next**.
6. Accept the license agreement and click **Next**.
7. Click **Next**.
8. In the **Services** dialog box, click **Next**
9. In the **Prerequisite** dialog box, click **Next**.
If the Prerequisite dialog box displays a warning that a prerequisite is not met, you must cancel the upgrade and complete the prerequisites before you can continue with the upgrade
10. In the **Host information** dialog box, complete one of the following actions:
 - Select **Use previously installed certificate** to accept the default values and keep the existing certificate.
 - Select **Accept these values for Hostname and Domain**, to create the certificate for BEMS.
 - Select **Modify these values** and enter the new hostname and domain name.
11. Click **Next**.
12. In the **Choose Install Folder** dialog box, click **Next** to accept the default installation folder location.
13. In the **Choose Logs Folder** dialog box, click **Next** to accept the default log file folder location.
14. In the **Administration Information** dialog box, type the password for the BEMS service account. Click **Next**.
15. In the **AD User Credentials** dialog box, enter the existing BEMS service account login credentials to access the BEMS Dashboard. Click **Next**.
16. In the **Database Information** dialog box, verify the BEMS-Core service database information to connect to the Microsoft SQL Server and enter the BEMS service account password. Click **Next**.
17. In the **Connect Administrator Information** dialog box, enter the BEMS-Connect service account password. Click **Next**.
18. In the **Connect Database Information** dialog box, verify the BEMS-Connect database information to connect to the Microsoft SQL Server and enter the BEMS service account password. Click **Next**.
19. In the **Presence Administrator Information** dialog box, enter the BEMS-Presence service account password. Click **Next**.
20. In the **Docs Database Information** dialog box, verify the BEMS-Docs database information to connect to the Microsoft SQL Server and enter the BEMS service account password. Click **Next**.
If your environment uses AlwaysOn with multi-subnet deployment, in the **Additional Properties** field, type `MultiSubnetFailover=true`.
21. In the **Pre-installation Summary** dialog box, click **Install** to install BEMS.
22. In the **Upgrade Complete** dialog box, click **Next** when the upgrade of the BEMS service is complete.
23. In the **Upgrade Complete** dialog box, complete the following steps:
 - a) Verify that the **Start BEMS services** checkbox is selected. If you clear the **Start BEMS services** checkbox, the BEMS installer stops the Good Technology Common Services.
 - b) If you are prompted to restart the computer. Select **Yes, restart my system** or **No, I will restart my system myself**.
24. Click **Done**.

Steps to upgrade BEMS and change to an alternate JRE

Perform the following steps to upgrade BEMS and change from Oracle JRE to an alternate JRE (for example, Azul Systems or Zulu). For more information, see [57053](#).

Consider the following before you upgrade the BEMS instance:

- The BEMS instance must be fully functional, and the Good Technology Common Services service must be running to perform an in-place upgrade of the BEMS software.
- Before you upgrade, verify that the BEMS debug logging level is not set to DEBUG or TRACE, or the upgrade or repair of the BEMS instance fails. For more information, see [42408](#).

Note: When you upgrade to JRE 17, it is a best practice to uninstall JRE 8 after the upgrade is complete, to allow for potential rollback if necessary.

If you have multiple BEMS instances in your environment, repeat these steps on each instance.

Step	Action
1	Download and install a supported OpenJDK.
2	Set the environment variable for the Java location to use the OpenJDK.
3	Import any custom certificates into the new lib\security\cacerts keystore. For instructions, see "Importing CA certificates for BEMS" in the Configuring BEMS-Core content .
4	Upgrade the BEMS software.
5	Optionally, uninstall JRE 8.

Steps to install BEMS instances into a cluster

When you add multiple BEMS instances to an existing BEMS instance, you create a cluster of BEMS instances. When you install additional BEMS instances, verify that you enter the existing database servers and database names in the appropriate database screens.

Step	Action
1	A BEMS instance is installed and configured in the environment.
2	Verify and complete the prerequisites and preupgrade tasks. Complete the preinstallation tasks on each additional BEMS instance.
3	Install the BEMS software.

Perform a Silent Install or Upgrade

You can perform a silent new installation, upgrade, or repair using the `silentInstall.bat` file or a command prompt. By default, BEMS is installed at the following location: `C:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server`.

A template response file `GoodServerSetup.properties` is provided, along with a `silentInstall.bat` file and the BEMS installer, in the installer zip file. The `GoodServerSetup.properties` file contains the variables and values of the inputs for each screen in the installer for fresh installation, along with instructions on how to edit the variables. The `silentInstall.bat` file is provided as a convenience to run the silent install command. If you install the BEMS services on separate computers or a custom location (for example, the E drive), modify the `GoodServerSetup.properties` file accordingly.

If you install, perform an upgrade, or repair a BEMS instance that is not installed in the default location, you must update the `USER_INSTALL_DIR1=<BEMS path>` property in the `GoodServerSetup.properties` file before you run the `silentInstall.bat` file. For example, to install BEMS on an E drive using the same folder path, you must complete the following steps:

1. In a text editor, open the `GoodServerSetup.properties` file.
2. Locate the existing entry "`USER_INSTALL_DIR1=C:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server`".
3. Update `USER_INSTALL_DIR1`: parameter with the custom path (for example, `USER_INSTALL_DIR1=E:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server`)
4. Save the file.

Double-click **silentInstall.bat file** or in a command prompt, type `<BEMS Installer> LAX_VM "%JAVA_HOME%\bin\java.exe" -i silent -f <response file>`

You can enter Admin-user details, machine details, SQL Server details, and other configuration specifics in this property file and then install the BEMS server in an unattended mode.

Installation results are logged in the install log file folder (for example, `<drive>:\Users\<alias>\AppData\Local\good`). Where `<alias>` is the name of the admin user account.

This silent install feature also can be used to upgrade or repair/modify the server. A password can be specified as part of the command file.

Removing the BEMS software

When you stop a BEMS instance, it will not be used by your high availability implementation, and all users that are serviced by the discontinued instance are reallocated to other servers automatically as soon as the discontinued instance goes down. This also applies to BlackBerry Connect server instances. If you installed the BEMS services on separate computers, complete these tasks on each computer that hosts the BEMS services.

After the BEMS software is removed, other BEMS instances check the BEMS databases (for example, BEMS-Core and BEMS-Connect) for instances that have not checked in within the default number of days. Inactive server references are removed from the databases automatically.


- For BEMS instances that were installed with the BEMS-Core, Mail, Docs, or Presence services, the default inactive time period is 30 days.
 - For BEMS instances that were installed with the Connect service, the default inactive time period is three days.
1. [Remove the BEMS software.](#)
 2. [Remove the BEMS server references from the BlackBerry Dynamics connectivity profile.](#)
 3. [Remove the BEMS Connect server references for BlackBerry Connect.](#)

Remove the BEMS software

Complete one of the following tasks on the computer that hosts BEMS:

Remove method	Steps
Installer	<ol style="list-style-type: none">a. Navigate to the GoodEnterpriseMobilityServer installation folder. By default, it is located at <code><BEMS_install_location>\GoodEnterpriseMobilityServerSetup<version></code>.b. Double-click InstallBEMS.bat.c. Select Uninstall and follow the instructions on the screen.
Control Panel	<ol style="list-style-type: none">a. Open the Control Panel.b. Click Uninstall a program.c. Click BlackBerry Enterprise Mobility Server > Uninstall/Change.d. Click Uninstall and follow the instructions on the screen.

Remove the BEMS server references from the BlackBerry Dynamics connectivity profile

1. In the BlackBerry UEM management console, on the menu bar, click **Policies and profiles**.
2. Click **Networks and connections > BlackBerry Dynamics connectivity profile**.
3. Click the BlackBerry Dynamics connectivity profile that you want to remove the BEMS instance from.
4. Click .
5. If specified, in the **Additional servers** section, remove the BEMS instances.
6. If specified, in the **IP address ranges** section, remove the BEMS instances.
7. In the **App servers** section, if listed locate the BlackBerry Work app entitlement.
8. Click **X** beside the instance that has been decommissioned.

9. Repeat steps 7 and 8 for the following entitlements that might be listed:
 - Good Enterprise Services (com.good.gdserviceentitlement.enterprise)
 - BlackBerry Connect (com.good.goodconnect)
 - Feature-Docs Service Entitlement (com.good.feature.share)
 - BlackBerry Core and Mail Services (com.blackberry.gdserviceentitlement.coreandmail)
 - BlackBerry Presence Service (com.blackberry.gdservice.entitlement.presence)
 - BlackBerry Tasks (com.blackberry.gd.tasks)
 - BlackBerry Notes (com.blackberry.gd.notes)
10. Click **Remove** beside any additional entitlements that do not have a BEMS instance associated with them.
11. Click **Save**.

Remove the BEMS Connect server references for BlackBerry Connect

1. In the BlackBerry UEM management console, on the menu, click **Apps**.
2. Search for and click the BlackBerry Connect app.
3. On the **Settings > BlackBerry Dynamics** tab, in the **App configuration** section, click the App Configuration you want to remove the BEMS instance from.
4. On the **Server Configuration** tab, remove the BEMS instance from the Connect Server Hosts table. For more information, see ["Configure BlackBerry Connect app settings in BlackBerry UEM" in the BlackBerry Connect administration content](#).
5. Click **Save**.

Configuring the BEMS services

After you have installed the BEMS instance, see to the following configuration content to configure the necessary services for your environment:

Task	Description
Configure the Core services.	Configure the shared settings for all of the on-premises BEMS services (for example, certificates, dashboard administrators, and web proxy server).
Configure the BlackBerry Mail (BlackBerry Push Notifications) service.	If you have installed the BlackBerry Mail (BlackBerry Push Notifications), configure the email notifications for iOS and Android in the environment.
Configure the BlackBerry Docs service	If you have installed the BlackBerry Docs service, configure the service to allow mobile workers access, synchronize, and share documents.
Configure the BlackBerry Presence service	If you have installed the BlackBerry Presence service, configure the service to provide real-time presence status to BlackBerry Work app users, the BlackBerry Dynamics Launcher, and third-party BlackBerry Dynamics apps.
Configure the BlackBerry Connect service	If you have installed the BlackBerry Connect service, configure the service to allow users to communicate and collaborate with secure instant messaging.
Configuring an on-premises BEMS in a BlackBerry UEM Cloud environment	BlackBerry UEM Cloud environments configured for email notifications and BEMS-Docs service for BlackBerry Work can configure an on-premises BEMS instance configured to allow iOS and Android users to use the on-premises BEMS-Connect, BEMS-Presence, BEMS-Docs services.

Appendices

Appendix: AlwaysOn Availability support for SQL Server

The AlwaysOn Availability Groups feature is a high-availability and disaster-recovery solution that provide an enterprise-level alternative to database mirroring. Introduced in SQL Server 2012, AlwaysOn Availability Groups maximize the availability of a set of user databases for an enterprise that is running SQL Server 2014, 2016, or 2017. An availability group supports a failover environment for a discrete set of user databases, known as availability databases, that fail over together. A read-scale availability group is a group of databases that perform read-only work and are copied from other SQL Server instances.

An availability group supports a set of read-write primary databases and one to eight sets of corresponding secondary databases. Optionally, secondary databases can be made available for read-only access and some backup operations.

For more information about AlwaysOn availability, visit docs.microsoft.com to read [Overview of Always On Availability Groups](#).

Steps to setup SQL Server for AlwaysOn availability

When you setup SQL Server for AlwaysOn availability, you perform the following actions:

Step	Action
1	Create an AlwaysOn availability group.
2	Configure SQL Server for AlwaysOn availability.
3	Install the BEMS software.
4	Configure the BEMS services databases for AlwaysOn availability.
5	Configure AlwaysOn availability group failover for single and multi-subnets for the following services: <ul style="list-style-type: none">• Core and Mail• Connect• Docs

Configure the BEMS services databases for AlwaysOn availability

Complete this task if you installed BEMS in your environment without specifying the server and database for AlwaysOn during the installation. Complete these steps on each BEMS instance in your environment.

If you manually specify the AlwaysOn Listener and database name in the BEMS dashboard, you must specify the updated server and database information when you perform future upgrades. For instructions on upgrading BEMS, see [Upgrade BEMS](#).

Before you begin:

- To install BEMS services connected to a database in AlwaysOn, the instance name must be set to the Listener in the AlwaysOn group, not the cluster name and not the host name of the host server in the cluster.
 - The databases created for BEMS services need to be added into the AlwaysOn group.
1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Mail**.
 2. Click **Database**.
 3. In the **Server** field, enter the FQDN of the AlwaysOn Listener.
 4. In the **Database** field, enter the name of the database that is added to the AlwaysOn Availability Group.
 5. Click **Test** to test the connection.
 6. Click **Save**.
 7. Repeat the previous steps for the Connect and Docs services.

Enabling AlwaysOn availability group failover to subnets for the BEMS-Core and Mail services

You can enable availability group failovers to different subnets by setting MultiSubnetFailover to true for the BEMS-Core and Mail services. You can set this option if you have single and multi-subnet connections. For more information about subnet failovers, visit docs.microsoft.com to read [Listeners, clients and failover](#).

For instructions on enabling AlwaysOn availability group failover to subnets for the BEMS-Core and Mail services when installing a new BEMS or upgrading a BEMS instance, see the following:

- During a new installation, see [Install the BEMS software](#).
- During an upgrade, see [Upgrade the BEMS software](#).

Enabling AlwaysOn availability group failover to subnets for the Connect service

You can enable availability group failovers to different subnets during BEMS installation, upgrade, and repair processes. You can set this option if you have single and multi-subnet connections. For more information about subnet failovers, see the Microsoft Documentation to read [Listeners, clients and failover](#).

For instructions on enabling AlwaysOn availability group failover to subnets for the Connect service when installing a new BEMS or upgrading a BEMS instance, see the following:

- During a new installation, see [Install the BEMS software](#).
- During an upgrade, see [Upgrade the BEMS software](#).

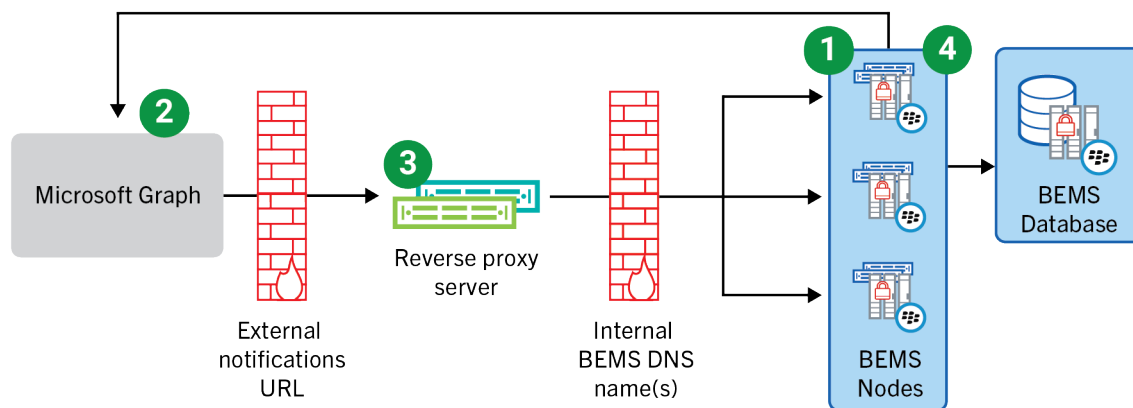
Enabling AlwaysOn availability group failover to subnets for the Docs service

You can enable AlwaysOn availability group failover to subnets for the Docs service during the BEMS installation, upgrade, and repair processes. For instructions on enabling AlwaysOn availability group failover to subnets for the Docs service when installing a new BEMS or upgrading a BEMS instance, see the following:

- During a new installation, see [Install the BEMS software](#).
- During an upgrade, see [Upgrade the BEMS software](#).

Data flow: BEMS notification flow using the Microsoft Graph API

This diagram shows how BEMS uses Microsoft Graph to send notifications to devices when a reverse proxy is used. BlackBerry recommends using a reverse proxy.



Component name	Description
BEMS	BEMS consolidates several BEMS services used to send work data to and from BlackBerry Dynamics apps, including BlackBerry Push Notifications (BlackBerry Mail), BlackBerry Connect, BlackBerry Presence, and BlackBerry Docs. BEMS listens for notification URI sent by the Microsoft Graph API.
Reverse proxy server	The reverse proxy server receives the Microsoft Graph connection and proxies the connection to the private BEMS URI.
Microsoft Graph	Microsoft Graph is a RESTful web API that allows you to communicate with Microsoft Cloud service resources.

1. BEMS sends a request to Microsoft Graph to subscribe to mailbox changes (for example, new email). The External Notification URL is included in the request.
2. Microsoft Graph initiates a connection to your organization's reverse proxy using the External Notification URL and sends a request that includes notification details.
3. The reverse proxy server intercepts the Microsoft Graph connection request and translates/routes the request to your BEMS cluster or instance.
4. BEMS receives the request from the reverse proxy and sends the new notification (for example, new email) to BlackBerry Work based on the notification rules and the user's device settings.

Configuring BlackBerry UEM Cloud to communicate with an on-premises BEMS

You can configure an on-premises BEMS to communicate with the BlackBerry Proxy to authenticate GDAuth tokens in a BlackBerry UEM Cloud environment. When you configure your environment with an on-premises BEMS, you allow iOS and Android users to use the BEMS-Connect, BEMS-Presence, and BEMS-Docs services, in addition to the email notifications and BEMS-Docs service for BlackBerry Work.

If your environment requires users to access File Shares or CMIS-based repositories, configure BEMS-Docs in an on-premises BEMS. Enabling BEMS-Docs in BlackBerry UEM Cloud and in an on-premises BEMS in a BlackBerry UEM Cloud environment is not supported. You can configure BEMS with only one on-premises BlackBerry UEM or BlackBerry UEM Cloud environment at a time.

When you configure BlackBerry UEM Cloud to communicate with on-premises BEMS, you perform the following actions. Note that some of the actions might have already been completed when you configured BlackBerry UEM Cloud.

Step	Action
1	Configure BlackBerry UEM Cloud in your environment.
2	In the UEM management console, verify that you have installed and activated the BlackBerry Connectivity Node .
3	If you are using Connect, install and configure the following on-premises BEMS services. <ul style="list-style-type: none"> • BEMS-Connect • BEMS-Presence • BEMS-Docs
4	In the BEMS Dashboard, Configure the BlackBerry Dynamics server in BEMS . Optionally, configure SSL communication between the BlackBerry Connectivity Node and the on-premises BEMS on port 17433. <ol style="list-style-type: none"> 1. Export the BlackBerry Proxy certificate to the local computer 2. Import the certificate to the BEMS Windows keystore 3. Import the certificate into the Java keystore on BEMS
5	In the BEMS Dashboard, Configure BEMS connectivity with BlackBerry Dynamics .
6	In the UEM management console, assign the BlackBerry Connect and BlackBerry Presence Service apps to users. You can assign the apps using one of the following methods. For instructions, see Managing apps in the BlackBerry UEM Managing apps content. <ul style="list-style-type: none"> • Assign an app to a user group • Assign an app group to a user group • Assign an app to a user account • Assign an app group to a user account
7	In the UEM management console, create a BlackBerry Dynamics Connectivity profile and add the app server that hosts the BlackBerry Connect and BlackBerry Presence Service, and Feature - Docs Service Entitlement apps .

Import the certificate to the BEMS Windows keystore

For the Connect service to trust the BlackBerry Proxy server's certificate, you must import the BlackBerry Proxy certificate to the Connect service Windows keystore. Repeat this task on each BEMS instance.

Before you begin: Save a copy of the ca.cer certificate you exported to a convenient location on the computer that hosts BEMS. For instructions, see [Export the BlackBerry Proxy certificate to the local computer](#).

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 certificate that you exported (for example `<drive>:\bemscert\ca.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 BEMS connectivity with BlackBerry Dynamics](#).

Import the certificate into the Java keystore on BEMS

For the Presence and Docs service to trust the BlackBerry Proxy server's certificate, you must import BlackBerry Connectivity Node certificate. Use the DBmanager to import the certificate into the BEMS Java keystore. By default, DBmanager is located in the installation folder at `<drive>:\GoodEnterpriseMobilityServer<version>\GoodEnterpriseMobilityServer\DBManager`.

Before you begin: Save a copy of the ca.cer certificate you exported to a convenient location on the computer that hosts BEMS. For instructions, see [Export the BlackBerry Proxy certificate to the local computer](#).

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**.

For more information about setting the Path system variable, see [Set an environment variable for the Java location](#).
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 root BlackBerry Proxy certificate.
 - a) Open a command prompt and navigate to the DBManager folder. For example, if the installation files are saved to your Downloads folder, type `C:\Users\besadmin\Downloads\GoodEnterpriseMobilityServer<version>\GoodEnterpriseMobilityServer\DBManager`
 - b) Import the certificate. Type `java -jar dbmanager-<version>-jar-with-dependencies.jar -moduleName pushnotify -dbType sqlserver -dbName <SQL_server_DB_name> -dbHost <Name of the computer hosting the SQL DB> -dbPort 1433 -userName gems_sa -password <BEMS_service_account_password> -action addcertificate -pemFile "C:\<path to the pemfile location>\<certificate name>.cer" -alias gdcert`
4. 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](#).

Configure the BlackBerry Dynamics server in BEMS

Your BEMS environment must be configured to trust the Root CA for the BlackBerry Proxy HTTPS configuration. For instructions, see ["Importing and configuring certificates" in the BEMS-Core configuration content](#).

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

3. If a BlackBerry Proxy server is not defined, do the following:
 - a) Click **Add BlackBerry Proxy**.
 - b) In the **Host Name** field, type the BlackBerry Proxy server 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. This is secure. You must [Export the BlackBerry Proxy certificate to the local computer](#) and then [Import the certificate into the Java keystore on BEMS](#).
 - If you select HTTP, the **Port** field prepopulates to 17080.
 - d) Click **Test** to test the connection.
 - e) Repeat the previous steps to add additional BlackBerry Proxy servers for redundancy continuity.
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.
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 Proxy server. If you don't configure SSL communication between the BlackBerry Connectivity Node and the on-premises BEMS on port 17433, verify that this check box has been cleared.
6. Click **Save**.

Configure BEMS connectivity with BlackBerry Dynamics

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Connect**.
2. Click **Service Account**.
3. Enter the service account username and password.
4. Click **Save**.
5. Click **BlackBerry Dynamics**.
6. In the **Hostname** field, type the BlackBerry Proxy server hostname.
7. In the **Port** field, the port number is prepopulated based on the communication type that you select.
 - If you select HTTP, the Port field prepopulates to 17080.
 - If you select HTTPS, the Port field prepopulates to 17433. This is secure.
8. Click **Test** to verify the connection to the BlackBerry Proxy server.
9. Click **Save**.

After you finish: If you selected HTTPS, you must complete the following:

- Configure the BlackBerry Connect app to use SSL communications. For instructions, see "Configuring BlackBerry Connect app settings" for your environment in the [BlackBerry Connect Administration content](#).
- [Export the BlackBerry Proxy certificate to the local computer](#) and then [Import the certificate to the BEMS Windows keystore](#).

Add an app server hosting the entitlement apps to a BlackBerry Dynamics connectivity profile

1. In the UEM management console, click **Policies and profiles**.
2. Click **Networks and Connections > BlackBerry Dynamics connectivity**.
3. Click **+** to create a new connectivity profile or select the BlackBerry Dynamics connectivity profile that you want to add an app server to and click **✎**.
4. Under **App servers**, click **Add**.
5. Select the **Feature - Docs Service Entitlement** app that you want to add an app server for.
6. Click **Save**.

7. In the table for the app, click **+**.
8. In the **Server** field, specify the FQDN of the on-premises BEMS server.
9. In the **Port** field, specify the port of the BlackBerry Proxy cluster that is used to access the server. By default, the port is 8443.
10. In the **Priority** drop-down list, specify the priority of this or these servers as primary.
11. In the **Primary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the primary cluster.
12. In the **Secondary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
13. Click **Save**.
14. Repeat steps 5 to 14 for the following apps:
 - BlackBerry Connect
 - BlackBerry Presence Service

Export the BlackBerry Proxy certificate to the local computer

If you must configure SSL communication to allow communication between the BlackBerry Connectivity Node and on-premises BEMS services (for example, the Connect, Docs, and Mail services), export the BlackBerry Proxy root and intermediate certificate chains and import them into the Java keystore on BEMS and the Windows keystore.

The following task is not browser-specific. For specific instructions, see the documentation for the browser you are using.

Before you begin: Verify that the BlackBerry Connectivity Node is installed with a status of Running.

1. On the computer that hosts the BlackBerry Connectivity Node, export the BlackBerry Proxy certificate to your computer. In a browser, type `https://localhost:17433`. A certificate error message is displayed because the certificate was signed by a CA that is not recognized as a well-known CA.
2. To open the Certificate dialog, click the certificate icon in the URL field.
3. Click **Certificate**.
4. Click **Certificate 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. Click **Browse**.
13. Enter a name for the certificate (for example, `ca.cer`) and export it to the local computer.
14. Click **Save**.
15. Click **Finish**.
16. Click **OK**.

After you finish:

- If you configure the Connect service, copy the exported BlackBerry Proxy certificate to the computer that hosts BEMS and [Import the certificate to the BEMS Windows keystore](#).

- If you configure the Presence service and Docs service, copy the exported BlackBerry Proxy certificate to the computer that hosts BEMS and [Import the certificate into the Java keystore on BEMS](#).

Legal notice

©2024 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Patents, as applicable, identified at: www.blackberry.com/patents.

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

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

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

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

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

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

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

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

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

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

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

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

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

Published in Canada