BEMS in a BlackBerry UEM environment

Installation Guide

2.12
About this guide

This guide describes how to install BEMS in your BlackBerry UEM environment.

**Note:** For ease of following the instructions in this guide, you should use the suggested database names.

This guide is intended for senior and junior IT professionals who are responsible for installing BEMS.

Before using this guide, make sure that you read the following guides:

- For information about planning your BEMS installation in a BlackBerry UEM environment, see the BlackBerry UEM Planning content.
- For information about the BEMS architecture in a BlackBerry UEM environment, see the BlackBerry UEM architecture and data flows content.
- For information about configuring your environment for disaster recovery, see the Disaster recovery content.
- For information about getting started with BlackBerry Dynamics in a BlackBerry UEM environment, see the BlackBerry Dynamics Administration content.
What is BEMS?

BEMS provides additional services for BlackBerry Dynamics apps. BEMS 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 real-time presence status of users in BlackBerry Dynamics apps, and access, synchronize, and share work file server and Microsoft SharePoint. The following table describes the services offered by BEMS.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlackBerry Mail (BlackBerry Push Notifications)</td>
<td>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.</td>
</tr>
<tr>
<td>BlackBerry Connect</td>
<td>The BlackBerry Connect 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.</td>
</tr>
<tr>
<td>BlackBerry Presence</td>
<td>The BlackBerry Presence service provides real-time presence status to BlackBerry Work, BlackBerry Dynamics Launcher, and third-party BlackBerry Dynamics applications—giving them a powerful add-in for mobile collaboration.</td>
</tr>
<tr>
<td>BlackBerry Docs</td>
<td>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.</td>
</tr>
<tr>
<td>BlackBerry Directory Lookup</td>
<td>The BlackBerry Directory Lookup service provides 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.</td>
</tr>
<tr>
<td>BlackBerry Follow-Me</td>
<td>The BlackBerry Follow-Me service keeps the BlackBerry Dynamics Launcher synchronized across multiple devices.</td>
</tr>
<tr>
<td>BlackBerry Certificate Lookup</td>
<td>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.</td>
</tr>
</tbody>
</table>

The BEMS Dashboard is a browser-based administration console which you use to configure the server components and services after the installation completes. The BEMS Web Console, also browser-based, provides real-time monitoring and logging of device connectivity, traffic load, and throughput in near real-time.

Services, in the context of BlackBerry Dynamics, refers to concrete business-level functionality that can be consumed by a plurality of BlackBerry Dynamics applications. For example, “Look up this contact in the directory,” “Subscribe to Presence for these contacts,” and “Save this file to SharePoint.” The BlackBerry Dynamics Services Framework allows client applications on an authenticated device to discover and utilize services by providing...
API publication, as well as life cycle and visibility management of services using the BlackBerry Developers For Enterprise Apps.
Preinstallation checklists

Verify that the requirements for the following BEMS services are met before you install BEMS.

- BlackBerry Push Notifications (BlackBerry Mail)
- BlackBerry Connect and BlackBerry Presence
- BlackBerry Docs

You can download the BEMS software from the BlackBerry Enterprise Mobility Suite & BlackBerry Application Support. 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.

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

When you verify requirements in this document, see the BEMS Compatibility Matrix.

**Note:** For ease of following the instructions in this guide, we recommend you use the suggested database names.

### BlackBerry Push Notifications

The following requirements apply when you need to configure servers to support BEMS with the BlackBerry Push Notifications (BlackBerry Mail) service in your organization.

<table>
<thead>
<tr>
<th>Complete</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registration</strong></td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td>Request the BlackBerry Work app from the Marketplace for Enterprise Software portal.</td>
</tr>
<tr>
<td>☐</td>
<td>Log in to <a href="https://account.blackberry.com/a/organization//entitlements">https://account.blackberry.com/a/organization//entitlements</a> and confirm that you have the BlackBerry Work app (com.good.gcs.g3) listed</td>
</tr>
<tr>
<td>Complete</td>
<td>Requirement</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Verify that the following ports are open for BEMS:</td>
</tr>
<tr>
<td></td>
<td>Inbound TCP ports</td>
</tr>
<tr>
<td></td>
<td>• 61616 or 61617 (SSL) to and from servers that host BEMS in the same cluster (bidirectional)</td>
</tr>
<tr>
<td></td>
<td>• 8443 from the BlackBerry Proxy server (required for Presence and Push Notifications)</td>
</tr>
<tr>
<td></td>
<td>Outbound TCP ports</td>
</tr>
<tr>
<td></td>
<td>• 80 to Microsoft Exchange Server (AutoDiscover)</td>
</tr>
<tr>
<td></td>
<td>• 389 and 3268 to Active Directory</td>
</tr>
<tr>
<td></td>
<td>• 443 to BlackBerry Dynamics NOC (includes connections to APNS)</td>
</tr>
<tr>
<td></td>
<td>• 443 to Firebase Cloud Messaging (FCM)</td>
</tr>
<tr>
<td></td>
<td>• 443 to Microsoft Exchange Server (Microsoft Exchange Web Services, AutoDiscover)</td>
</tr>
<tr>
<td></td>
<td>• 17080 to the BlackBerry Proxy server (17433 for SSL)</td>
</tr>
<tr>
<td></td>
<td>• 61616 or 61617 (SSL) to and from servers that host BEMS in the same cluster (bidirectional)</td>
</tr>
</tbody>
</table>

**Microsoft Active Directory, Microsoft Exchange, and Microsoft Office 365**

<table>
<thead>
<tr>
<th>Complete</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify that you have a mail server that supports BEMS.</td>
</tr>
<tr>
<td></td>
<td>Create a Microsoft Active Directory account for the BEMS service account. For example, BEMSAdmin</td>
</tr>
<tr>
<td></td>
<td>For password considerations, see Creating a Microsoft Active Directory account for the BEMS service account.</td>
</tr>
<tr>
<td></td>
<td>Create a mailbox for the BEMSAdmin account.</td>
</tr>
<tr>
<td></td>
<td>Grant Application Impersonation Permissions to the BEMSAdmin account in Microsoft Exchange. For instructions, see Grant application impersonation permission to the BEMS service account</td>
</tr>
<tr>
<td></td>
<td>Make sure that your Microsoft Exchange Autodiscover is set up correctly.</td>
</tr>
<tr>
<td></td>
<td>For more information on how to use third-party tools to test autodiscover, visit support.blackberry.com/community to read article 40351.</td>
</tr>
<tr>
<td></td>
<td>Make sure that Microsoft Exchange Web Services (EWS) is enabled on port 443, and that connections are permitted from the BEMS server.</td>
</tr>
<tr>
<td></td>
<td>Make sure that your Microsoft Exchange ActiveSync environment is updated to support TLS 1.2. For more information, visit support.blackberry.com/community to read article 56869. If the TLS version is not updated, Push Notifications fail.</td>
</tr>
</tbody>
</table>

**Microsoft .NET Framework**
<table>
<thead>
<tr>
<th>Complete</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify the version of Microsoft .NET Framework. For more information, see Preparing the computer that hosts BEMS for use with Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business.</td>
</tr>
</tbody>
</table>

**BEMS**

|          | Verify that your environment is running a version of BlackBerry UEM that supports BEMS. For instructions on installing or upgrading BlackBerry UEM, see the BlackBerry UEM Installation and Upgrade content. |
|          | Verify that your server is running an operating system that supports BEMS. For information about the supported operating systems, see the BEMS Compatibility Matrix. |
|          | Verify that you have the required hardware to host BEMS. For more information about hardware requirements, see BlackBerry UEM Planning content. If you configure your environment for disaster recovery, see the Disaster recovery content. |
|          | Make sure that the BEMS service account is a local administrator on the server. |
|          | Make sure that the BEMS service account has "Log on as a service" permission. |
|          | Verify that the servers that host and access the BEMS Dashboard have a supported browser installed. |
|          | Make sure that the server's date and time are set correctly. |
|          | Make sure that the server has been joined to the domain. |
|          | Make sure that the Windows Firewall is disabled. |
|          | Disable antivirus programs before you install or upgrade the BEMS software. |
|          | Verify that you have installed JRE 8 on the servers where you will install BEMS and that you have an environment variable that points to its location. For instructions, see Configure the Java Runtime Environment. For information about supported JRE versions, see the BEMS Compatibility Matrix. |
|          | Make sure you have connectivity to SQL Server. Typically this is through TCP port 1433. You can use the SQL Server browser to verify. |
|          | Ensure connectivity to Microsoft Exchange Web Services (EWS). For more information on how to use third-party tools to test connectivity, visit support.blackberry.com/community to read article 40351. |

**Database**
### Complete Requirement

- **Verify that your environment has a database server that supports BEMS.**
  
  To configure remote TCP/IP connections for Microsoft SQL Server Express, see BlackBerry Push Notifications database requirements.

- **Make sure that your Microsoft SQL Server environment 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. For more information, visit support.blackberry.com/community to read article 56869 and 56865.

- **Create a SQL Server database for the BlackBerry Push Notifications service and call it “BEMS-Core”**.
  
  **Note:** If this is the first server in the BEMS cluster, create the database. If this is an additional server for the same BEMS cluster, then a new database is not required. Record the existing database name for the BEMS-Core and Mail cluster.

- **Make sure that the Microsoft SQL Server account or the BEMS Windows service account has db_owner privileges to the database.** For more information, visit support.blackberry.com/community to read article 42661.

### BlackBerry Connect and BlackBerry Presence

The following requirements apply when you need to configure servers to support BEMS with the BlackBerry Connect and BlackBerry Presence services.

<table>
<thead>
<tr>
<th>Complete</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registration</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Request the BlackBerry Connect app from the Marketplace for Enterprise Software portal.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Log in to <a href="https://account.blackberry.com/a/organization//entitlements">https://account.blackberry.com/a/organization//entitlements</a> and confirm that you have the BlackBerry Connect app (com.good.goodoconnect) listed for the Connect service and the BlackBerry Work app (com.good.gcs.g3) listed for connections to the Presence service.</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Network - Microsoft Lync Server, Skype for Business, Skype for Business Online
<table>
<thead>
<tr>
<th>Complete</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>Verify that the following ports are open for BEMS:</td>
</tr>
<tr>
<td></td>
<td>Inbound TCP Ports</td>
</tr>
<tr>
<td></td>
<td>• 8080 or 8082 from the BlackBerry Proxy server (for BlackBerry Connect)</td>
</tr>
<tr>
<td></td>
<td>• 8443 from the BlackBerry Proxy server (for BlackBerry Presence)</td>
</tr>
<tr>
<td></td>
<td>• 49555 from the Microsoft Lync Server (for BlackBerry Connect)</td>
</tr>
<tr>
<td></td>
<td>• 49555 from the on-premises Skype for Business server (for BlackBerry Connect) when the Connect service is trusted by Skype for Business</td>
</tr>
<tr>
<td></td>
<td>• 49777 from the on-premises Microsoft Lync Server or Skype for Business (for BlackBerry Presence)</td>
</tr>
<tr>
<td></td>
<td>Outbound TCP Ports</td>
</tr>
<tr>
<td></td>
<td>• 443 to the BlackBerry Dynamics NOC</td>
</tr>
<tr>
<td></td>
<td>• In a Skype for Business Online environment, 443 to the following:</td>
</tr>
<tr>
<td></td>
<td>• login.microsoftonline.com</td>
</tr>
<tr>
<td></td>
<td>• lyncdiscover.EMAIL-DOMAIN</td>
</tr>
<tr>
<td></td>
<td>• *.online.lync.com</td>
</tr>
<tr>
<td></td>
<td>• 206.124.114.0/24</td>
</tr>
<tr>
<td></td>
<td>• 206.124.121.0/24</td>
</tr>
<tr>
<td></td>
<td>• 206.124.122.0/24</td>
</tr>
<tr>
<td></td>
<td>• 5061 (for BlackBerry Connect) to the Microsoft Lync Server or on-premises Skype for Business server configured as trusted mode</td>
</tr>
<tr>
<td></td>
<td>• 17080 or 17433 to the BlackBerry Proxy server</td>
</tr>
<tr>
<td></td>
<td>• 1433 to the Microsoft SQL Server (default)</td>
</tr>
<tr>
<td></td>
<td>• 1434 UDP to the on-premises Microsoft Lync or Skype for Business database (for initial setup only)</td>
</tr>
<tr>
<td></td>
<td>• 49152 – 57500 TCP: Random port in this range to the Microsoft Lync or Skype for Business database (for initial setup only)</td>
</tr>
<tr>
<td>☐</td>
<td>If BEMS requires a proxy server for external access, record it here:</td>
</tr>
<tr>
<td></td>
<td>• Proxy server make and model: __________________________</td>
</tr>
<tr>
<td></td>
<td>• Method: __________________________</td>
</tr>
</tbody>
</table>

Network - Cisco Unified Communications Manager and Cisco IM and Presence
<table>
<thead>
<tr>
<th>Complete</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>Verify that the following ports are open for BEMS:</td>
</tr>
<tr>
<td></td>
<td>Inbound TCP Ports</td>
</tr>
<tr>
<td></td>
<td>• 8080 or 8082 from the BlackBerry Proxy server (for BlackBerry Connect)</td>
</tr>
<tr>
<td></td>
<td>Outbound TCP Ports</td>
</tr>
<tr>
<td></td>
<td>• 443 to the BlackBerry Dynamics NOC</td>
</tr>
<tr>
<td></td>
<td>• 206.124.114.0/24</td>
</tr>
<tr>
<td></td>
<td>• 206.124.121.0/24</td>
</tr>
<tr>
<td></td>
<td>• 206.124.122.0/24</td>
</tr>
<tr>
<td></td>
<td>• 8443 to the Cisco User Data Service</td>
</tr>
<tr>
<td></td>
<td>• 5222 to the Cisco Jabber XMPP Service</td>
</tr>
<tr>
<td></td>
<td>• 8083 to the Cisco IM and Presence Service</td>
</tr>
<tr>
<td></td>
<td>• 17080 or 17433 to the BlackBerry Proxy server</td>
</tr>
<tr>
<td></td>
<td>• 1433 to the Microsoft SQL Server server (default)</td>
</tr>
<tr>
<td>☐</td>
<td>If BEMS requires a proxy server for external access, record it here:</td>
</tr>
<tr>
<td></td>
<td>• Proxy server make and model: __________________________</td>
</tr>
<tr>
<td></td>
<td>• Method: _____________________________</td>
</tr>
</tbody>
</table>

**Microsoft Active Directory: Microsoft Lync Server, Skype for Business, and Skype for Business Online**

| ☐       | Create a Microsoft Active Directory service account for the BEMS software (Can be the same account used for BlackBerry Push Notifications. For example, BEMSAdmin. |
| ☐       | Verify that the BEMS service account has RTCUniversalReadOnlyAdmins permission during the BEMS installation. This permission is granted in the Microsoft Active Directory. |
| ☐       | 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 about load balancing requirements, visit [https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/load-balancing](https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/load-balancing). |

**Microsoft Active Directory: Cisco Unified Communications Manager and Cisco IM and Presence**

| ☐       | Create a Microsoft Active Directory service account for the BEMS software. |

**BEMS: Microsoft Lync Server, Skype for Business, and Skype for Business Online**

<p>| ☐       | Verify that your environment is running a version of BlackBerry UEM that supports BEMS. For instructions on installing or upgrading BlackBerry UEM, see the BlackBerry UEM Installation and Upgrade content. |
| ☐       | Verify that you have a supported instant messaging server. |</p>
<table>
<thead>
<tr>
<th>Complete</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If your environment runs Skype for Business Online, record the tenant name.</td>
</tr>
<tr>
<td></td>
<td>Make sure that the BEMS service account is a local administrator on the server.</td>
</tr>
<tr>
<td></td>
<td>Make sure that the BEMS service account has &quot;Log on as a service&quot; permission.</td>
</tr>
<tr>
<td></td>
<td>Verify that the servers that host and access the BEMS Dashboard have a supported browser installed.</td>
</tr>
<tr>
<td></td>
<td>Make sure that the server’s date and time are set correctly.</td>
</tr>
<tr>
<td></td>
<td>Make sure that the server is joined to the domain.</td>
</tr>
<tr>
<td></td>
<td>Verify that the servers are running an operating system that supports the Connect service before you install or upgrade.</td>
</tr>
</tbody>
</table>
|           | If your environment runs one of the following instant messaging services, make sure that Windows PowerShell (x86) is installed:  
|           | • Microsoft Lync Server 2010  
|           | • Microsoft Lync Server 2013  
|           | • Skype for Business on-premises for Presence and plan to configure the Connect service as trusted by Skype for Business  
|           | Open "Windows PowerShell (x86)" and run the following command to enable execution of remote signed scripts: `Set-ExecutionPolicy -Scope CurrentUser RemoteSigned` |
|           | If your environment includes the following instant messaging servers, create a Trusted Application Pool, trusted application, and trusted application endpoint for BEMS in the Microsoft Lync Shell Console:  
|           | • Microsoft Lync Server  
|           | • Skype for Business on-premises and plan to configure the Connect service as trusted by Skype for Business  
|           | Note: The user creating the Trusted Application Pool must have RTCUniversalServerAdmins and Domain Admins permissions.  
|           | For more information about preparing the first server hosting BEMS, see Prepare the initial computer hosting BEMS. |
|           | If your environment includes the following instant messaging servers, verify the version of Microsoft .NET Framework:  
|           | • Skype for Business Online For more information, see Preparing the computer that hosts BEMS for use with Skype for Business Online.  
<p>|           | • Skype for Business on-premises and plan to configure the Connect service as non-trusted by Skype for Business. For more information, see Preparing the computer that hosts BEMS for use with Skype for Business using non-trusted application mode |</p>
<table>
<thead>
<tr>
<th>Complete</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| ☐        | If your environment runs one of the following instant messaging servers, make sure that the required Microsoft Unified Communications Managed API is installed:  
  • Microsoft Lync Server 2010  
  • Microsoft Lync Server 2013  
  • Skype for Business on-premises for Presence and plan to configure the Connect service as trusted by Skype for Business  
  For more information, see Preparing the computer that hosts BEMS for use with Microsoft Lync Server 2010, Microsoft Lync Server 2013, Skype for Business, or Skype for Business Online. |
| ☐        | If your environment runs one of the following instant messaging servers, request and install an SSL certificate on BEMS.  
  • Microsoft Lync Server 2010  
  • Microsoft Lync Server 2013  
  • Skype for Business on-premises for Presence and plan to configure the Connect service as trusted by Skype for Business  
  For more information, see SSL certificate requirements for Microsoft Lync Server, Skype for Business, and Presence. |
| ☐        | Disable all antivirus programs and backup software before you install or upgrade the BEMS software. |
| ☐        | Verify that you have installed JRE 8 on the servers where you will install BEMS and that you have an environment variable that points to its location. For instructions, see Configure the Java Runtime Environment. For information about the supported JRE versions, see the BEMS Compatibility Matrix. |

**BEMS - Cisco Unified Communications Manager and Cisco IM and Presence**

| ☐        | Verify that your environment is running a version of BlackBerry UEM that supports BEMS. For instructions on installing or upgrading BlackBerry UEM, see the BlackBerry UEM Installation and Upgrade content. |
| ☐        | Make sure that the BEMS service account is a local administrator on the server. |
| ☐        | Make sure that the BEMS service account has Logon As a Service permission. |
| ☐        | Make sure that the server's date and time are correctly set. |
| ☐        | Make sure that the server is joined to the domain. |
| ☐        | Disable all antivirus programs and backup software before you install or upgrade the BEMS software. |
**Complete** | **Requirement**
--- | ---
☐ | Verify that you have installed JRE 8 on the servers where you will install BEMS and that you have an environment variable that points to its location. For instructions, see Configure the Java Runtime Environment. For information about the supported JRE versions, see the BEMS Compatibility Matrix.

**Database**

☐ | Verify your environment is running a supported database server.

☐ | Create a SQL Server database for the BlackBerry Connect service and call it "BEMS-Connect". **Note:** If this is the first server in the BEMS cluster, Create the database. If this is an additional server for the same BEMS cluster, then a new database is not required. Record the existing database name for the BEMS-Connect cluster.

☐ | Make sure that the BEMS service account has db_owner permission to the database. For more information, visit support.blackberry.com/community to read article 42661.

**BlackBerry Docs**

The following requirements apply when you need to configure servers to support BEMS with the BlackBerry Docs service in your organization.

<table>
<thead>
<tr>
<th>Complete</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registration</strong></td>
<td></td>
</tr>
</tbody>
</table>

☐ | Request the BlackBerry Work app from the Marketplace for Enterprise Software portal.

☐ | Log in to https://account.blackberry.com/a/organization//entitlements and confirm that you have the BlackBerry Work app (com.good.gcs.g3) listed for connections to the Docs service, and the Feature - Docs Service Entitlement app listed.

**Network**
<table>
<thead>
<tr>
<th>Complete</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify that the following ports are open for BEMS:</td>
</tr>
<tr>
<td></td>
<td>Inbound TCP ports</td>
</tr>
<tr>
<td></td>
<td>• 8443 from the BlackBerry Proxy server</td>
</tr>
<tr>
<td></td>
<td>Outbound TCP ports</td>
</tr>
<tr>
<td></td>
<td>• 80 or 443 to Microsoft SharePoint server</td>
</tr>
<tr>
<td></td>
<td>• 80 or 443 to Microsoft Office Web Apps server</td>
</tr>
<tr>
<td></td>
<td>• 17080 or 17433 to the BlackBerry Proxy server</td>
</tr>
<tr>
<td></td>
<td>• 1433 to the SQL Server (default)</td>
</tr>
<tr>
<td></td>
<td>• 445, 139 to CIFS share</td>
</tr>
<tr>
<td></td>
<td>• 389 or 636 to LDAP</td>
</tr>
<tr>
<td></td>
<td>• In a SharePoint Online environment, 443 to the following:</td>
</tr>
<tr>
<td></td>
<td>• login.microsoftonline.com</td>
</tr>
<tr>
<td></td>
<td>• *.sharepoin.com</td>
</tr>
<tr>
<td></td>
<td>• In an Azure Information Protection environment, 443 to the following:</td>
</tr>
<tr>
<td></td>
<td>• login.microsoftonline.com</td>
</tr>
<tr>
<td></td>
<td>• graph.microsoft.com</td>
</tr>
<tr>
<td></td>
<td>• *.aadrm.com</td>
</tr>
<tr>
<td></td>
<td>• In a Box environment, 443 to *.box.com</td>
</tr>
<tr>
<td></td>
<td>Outbound UDP ports</td>
</tr>
<tr>
<td></td>
<td>• 137–138 to CIFS share</td>
</tr>
<tr>
<td></td>
<td>If BEMS requires a proxy server for external access, record the following information:</td>
</tr>
<tr>
<td></td>
<td>• Proxy server make and model: _______________________________</td>
</tr>
<tr>
<td></td>
<td>• Authentication method: _______________________________</td>
</tr>
<tr>
<td></td>
<td>If your environment is configured for a specific version of SMB or CIFS protocol to access a File Share, make sure that BEMS is installed on a compatible Microsoft Windows operating system. Refer to your Microsoft documentation for more information on compatibility.</td>
</tr>
<tr>
<td></td>
<td><strong>Microsoft Active Directory</strong></td>
</tr>
<tr>
<td></td>
<td>Create a Microsoft Active Directory service account for the BEMS software.</td>
</tr>
<tr>
<td></td>
<td><strong>Microsoft .NET Framework</strong></td>
</tr>
<tr>
<td></td>
<td>Verify the version of Microsoft .NET Framework.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Preparing the computer that hosts BEMS for use with Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business.</td>
</tr>
<tr>
<td></td>
<td><strong>BEMS</strong></td>
</tr>
<tr>
<td>Complete</td>
<td>Requirement</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>☐</td>
<td>Verify that your environment is running a version of BlackBerry UEM that supports BEMS. For instructions on installing or upgrading BlackBerry UEM, see the BlackBerry UEM Installation and Upgrade content.</td>
</tr>
<tr>
<td>☐</td>
<td>Verify that the server hosting BEMS is running an operating system that supports BEMS. For information about the supported operating systems, see the BEMS Compatibility Matrix.</td>
</tr>
<tr>
<td>☐</td>
<td>Verify that you have the required hardware to host BEMS. For more information about hardware requirements, see BlackBerry UEM Planning content. If you configure your environment for disaster recovery, see the Disaster recovery content.</td>
</tr>
<tr>
<td>☐</td>
<td>Verify that the servers that host and access the BEMS Dashboard have a supported browser installed.</td>
</tr>
<tr>
<td>☐</td>
<td>Make sure that the server's time and date are set correctly.</td>
</tr>
<tr>
<td>☐</td>
<td>Make sure that the server is joined to the domain.</td>
</tr>
<tr>
<td>☐</td>
<td>Verify Microsoft SharePoint and Box support. Microsoft SharePoint 2007, Microsoft SharePoint 2010, Microsoft SharePoint 2013, Microsoft SharePoint 2016, Microsoft SharePoint Online, and Box are supported.</td>
</tr>
<tr>
<td>☐</td>
<td>If you are using resource based Kerberos constrained delegation or Kerberos constrained delegation (KCD), make sure that the BEMS service account is a local administrator on the server.</td>
</tr>
<tr>
<td>☐</td>
<td>Make sure that the BEMS service account has &quot;Log on as a service&quot; permission.</td>
</tr>
<tr>
<td>☐</td>
<td>Make sure that the Windows Firewall is disabled.</td>
</tr>
<tr>
<td>☐</td>
<td>Disable all antivirus programs and backup software before you install or upgrade the BEMS software.</td>
</tr>
<tr>
<td>☐</td>
<td>Verify that you have installed JRE 8 on the servers where you will install BEMS and that you have an environment variable that points to its location. For instructions, see Configure the Java Runtime Environment. For information about the supported JRE versions, see the BEMS Compatibility Matrix.</td>
</tr>
<tr>
<td>Database</td>
<td>Verify your environment is running a supported database server.</td>
</tr>
<tr>
<td>Complete</td>
<td>Requirement</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td><strong>Create a SQL Server database for the Docs service and call it &quot;BEMS-Docs&quot;.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If this is the first server in the BEMS cluster, create the database. If this is an additional server for the same BEMS cluster, then a new database is not required. Record the existing database name for the BEMS-Docs cluster.</td>
</tr>
<tr>
<td></td>
<td><strong>Make sure the BEMS service account has db_owner permissions to the database. For more information, visit <a href="http://support.blackberry.com/community">support.blackberry.com/community</a> to read article 42661.</strong></td>
</tr>
</tbody>
</table>
Installation and upgrade

Steps to install BEMS

For a new installation of BEMS, perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verify the prerequisites.</td>
</tr>
<tr>
<td>2</td>
<td>Complete the preinstallation tasks.</td>
</tr>
<tr>
<td>3</td>
<td>Install the BEMS software.</td>
</tr>
</tbody>
</table>

Supported installation and upgrade paths

To upgrade to BEMS 2.12, you can use the following installation and upgrade paths.

**Note:** When you upgrade from an earlier version of BEMS, you must complete the upgrade precheck.

- You can upgrade BEMS 2.9 (2.9.13.15) and later to BEMS 2.12 using the setup application on the computer that hosts the previous version of BEMS.
- If you change the instant messaging server (for example, from Microsoft Lync Server 2013 to Skype for Business) that your BEMS instance connects to, you must remove the existing BlackBerry Connect and BlackBerry Presence instances. You must verify the Skype for Business prerequisites and can then install BEMS 2.8.x or later.

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.
Steps to upgrade BEMS

Before you upgrade BEMS, make sure that the BEMS debug logging level is not set to ALL. If the logging level is set to ALL, the upgrade or repair of the BEMS instance fails. For more information, visit http://support.blackberry.com/community to read article 42408.

When you upgrade BEMS to the latest version, you perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Review the best practices for preparing to upgrade BEMS.</td>
</tr>
<tr>
<td>2</td>
<td>Verify the prerequisites.</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade the BEMS software.</td>
</tr>
</tbody>
</table>

Steps to upgrade BEMS and change to an alternate JRE

When you upgrade BEMS and change from Oracle JRE8 to an alternate JRE (for example, Azure Systems or Zulu), you perform the following actions. For more information about switching to an alternate JRE, visit http://support.blackberry.com/community to read article 57053.

Before you upgrade BEMS, make sure that the BEMS debug logging level is not set to ALL. If the logging level is set to ALL, the upgrade or repair of the BEMS instance fails. For more information, visit http://support.blackberry.com/community to read article 42408.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download and install a supported OpenJDK.</td>
</tr>
<tr>
<td>2</td>
<td>Configure the Java Runtime Environment to use the OpenJDK.</td>
</tr>
</tbody>
</table>
| 3    | On the computer hosting the BEMS instance, stop the following BEMS services. For example,  
|      | • Good Technology Connect  
|      | • Good Technology Presence  
|      | • Good Technology Common Services  
<p>|      | • Good Technology .NET Services Manager |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Optionally, uninstall the Oracle JRE8. Optionally, verify the JAVA version using the command prompt. In the command prompt, type <code>java -version</code>. Press Enter.</td>
</tr>
<tr>
<td>5</td>
<td>Import any custom certificates into the new <code>lib\security\cacerts</code> keystore.</td>
</tr>
<tr>
<td>6</td>
<td>Start the Good Technology Common Services.</td>
</tr>
<tr>
<td>7</td>
<td>Upgrade the BEMS instance to 2.12 or later.</td>
</tr>
</tbody>
</table>

**Steps to upgrade BEMS and change the instant messaging service**

Before you upgrade BEMS, make sure that the BEMS debug logging level is not set to ALL. If the logging level is set to ALL, the upgrade or repair of the BEMS instance fails. For more information, visit [http://support.blackberry.com/community](http://support.blackberry.com/community) to read article 42408.

When you upgrade BEMS and change the instant messaging service from Microsoft Lync Server to Skype for Business, you perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade the BEMS software.</td>
</tr>
<tr>
<td>2</td>
<td>Stop the Good Technology Connect service and Good Technology Presence service.</td>
</tr>
<tr>
<td>3</td>
<td>Remove the Connect and Presence services.</td>
</tr>
<tr>
<td>4</td>
<td>Uninstall the current Microsoft Unified Communications Managed API and install Microsoft Unified Communications Managed API 5.0.</td>
</tr>
<tr>
<td>5</td>
<td>Add the Connect and Presence services.</td>
</tr>
<tr>
<td>6</td>
<td>Remove BEMS from the trusted server entry records and trusted application pool.</td>
</tr>
<tr>
<td>7</td>
<td>Create a trusted pool application for BEMS on the computer that hosts Skype for Business.</td>
</tr>
</tbody>
</table>
### Steps to upgrade BEMS and change the instant messaging service to Skype for Business Online

Before you upgrade BEMS, make sure that the BEMS debug logging level is not set to ALL. If the logging level is set to ALL, the upgrade or repair of the BEMS instance fails. For more information, visit [http://support.blackberry.com/community](http://support.blackberry.com/community) to read article 42408.

When you upgrade BEMS and change the instant messaging service from Microsoft Lync Server or Skype for Business to Skype for Business Online only, you perform the following actions.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Upgrade the BEMS software.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Stop the Good Technology Connect service and Good Technology Presence service.</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Remove the Connect and Presence services.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>If required, uninstall the current Microsoft Unified Communications Managed API and install Microsoft Unified Communications Managed API 5.0.</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Add the Connect service.</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>Remove BEMS from the trusted server entry records and trusted application pool.</td>
</tr>
</tbody>
</table>
| **7** | Configure the services.  
• Connect service  
• Presence service |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Start the Good Technology Connect service and Good Technology Presence service.</td>
</tr>
</tbody>
</table>
Prerequisites: Installing and configuring BEMS

Successful installation of BEMS requires that a supporting infrastructure of necessary hardware and software is installed. These prerequisites include:

- Core requirements
- BlackBerry Push Notifications service (PNS) requirements
- BlackBerry Connect requirements
- BlackBerry Presence requirements
- BlackBerry Docs requirements
- BlackBerry Directory Lookup requirements
- BlackBerry Follow-Me requirements
- BlackBerry Certificate Lookup requirements

Core requirements

When you configure Core, you complete the following actions:

- Verify the system and network requirements
- Verify the BlackBerry UEM requirements
- Configure the Java Runtime Environment (JRE)
- Set up a Windows service account for BEMS
- Verify the database requirements

System and network requirements

Verify that your environment and the servers that host BEMS meet the following system and network requirements.

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>Verify that you have installed JRE 8 on the servers where you will install BEMS and that you have an environment variable that points to its location.</td>
</tr>
<tr>
<td>Operating system</td>
<td>Verify that your server is running an operating system that supports BEMS. For information about the supported operating systems, see the BEMS Compatibility Matrix.</td>
</tr>
<tr>
<td>Supported browsers</td>
<td>Verify that the servers that host and access the BEMS Dashboard have a supported browser installed.</td>
</tr>
<tr>
<td>Administration rights</td>
<td>Requirement</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>• The user that performs the installation must have local administrative privileges on the host machine. The user that performs the installation must also have <code>db_owner</code> permissions to all the BEMS databases. For more information, visit support.blackberry.com/community to read article 42661.</td>
<td></td>
</tr>
<tr>
<td>• The BEMS service account must have &quot;Log on as a service&quot; right.</td>
<td></td>
</tr>
<tr>
<td>• Disable antivirus software before you install or upgrade the BEMS software.</td>
<td></td>
</tr>
<tr>
<td>• Exclude the BEMS directory from virus scanning.</td>
<td></td>
</tr>
<tr>
<td>• The local Windows firewall must be disabled.</td>
<td></td>
</tr>
<tr>
<td><strong>Important:</strong> A Group Firewall Policy will cause the installer to fail its prerequisite checks, even if the local firewall is disabled.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inbound TCP Ports</th>
<th>The following ports must be open and ready for BEMS and not blocked by any firewall:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 8080 from the BlackBerry Proxy server or 8082 if SSL is required for inbound BlackBerry Proxy communications</td>
<td></td>
</tr>
<tr>
<td>• 8443 from the BlackBerry Proxy server for Push Notifications, Presence, and Docs and from Microsoft Office Web Apps server for Docs</td>
<td></td>
</tr>
<tr>
<td>• 49555 from Microsoft Lync Server for the Connect service</td>
<td></td>
</tr>
<tr>
<td>• 49555 from the on-premises Skype for Business server (for BlackBerry Connect) when the Connect service is trusted by Skype for Business</td>
<td></td>
</tr>
<tr>
<td>• 49777 from the Microsoft Lync Server or Skype for Business for the Presence service</td>
<td></td>
</tr>
<tr>
<td>• 61616 TCP port to and from BEMS servers in the same cluster (bidirectional)</td>
<td></td>
</tr>
<tr>
<td>• 61617 TCP (SSL) to and from BEMS servers in the same cluster (bidirectional)</td>
<td></td>
</tr>
<tr>
<td><strong>Important:</strong> 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).</td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>Requirement</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Outbound TCP Ports</td>
<td>Verify that the following ports are open and ready for BEMS and not blocked by any firewall:</td>
</tr>
<tr>
<td></td>
<td>• 443 to BlackBerry Dynamics NOC (gdweb.good.com)</td>
</tr>
<tr>
<td></td>
<td>• 443 to Microsoft Exchange</td>
</tr>
<tr>
<td></td>
<td>• 443 to Firebase Cloud Messaging (FCM) for Android Push Notification</td>
</tr>
<tr>
<td></td>
<td>• 443 or 80 to Microsoft SharePoint</td>
</tr>
<tr>
<td></td>
<td>• 443 to Microsoft Office Web Apps Server (OWAS)</td>
</tr>
<tr>
<td></td>
<td>• In a Skype for Business Online environment, 443 to the following:</td>
</tr>
<tr>
<td></td>
<td>• login.microsoftonline.com</td>
</tr>
<tr>
<td></td>
<td>• lyncdiscover.EMAIL-DOMAIN</td>
</tr>
<tr>
<td></td>
<td>• *.online.lync.com</td>
</tr>
<tr>
<td></td>
<td>• 5061 (for BlackBerry Connect) to the Microsoft Lync Server or on-premises Skype for Business server configured as trusted mode</td>
</tr>
<tr>
<td></td>
<td>• 17080 to the BlackBerry Proxy server</td>
</tr>
<tr>
<td></td>
<td>• 17433 to the BlackBerry Proxy server</td>
</tr>
<tr>
<td></td>
<td>• 1433 to the Microsoft SQL Server (default)</td>
</tr>
<tr>
<td></td>
<td>• 1434 UDP to the Microsoft Lync database (for initial setup only)</td>
</tr>
<tr>
<td></td>
<td>• 8443 to the Presence Web Service (CIMP server)</td>
</tr>
<tr>
<td></td>
<td>• 5222 to the Presence Web Service (CIMP server)</td>
</tr>
<tr>
<td></td>
<td>• 8083 to the Cisco IM and Presence Service</td>
</tr>
<tr>
<td></td>
<td>• 49152 – 57500 TCP: Random port in this range to the Lync database (for initial setup only)</td>
</tr>
<tr>
<td></td>
<td>• 61616 TCP port to and from BEMS servers in the same cluster (bidirectional)</td>
</tr>
<tr>
<td></td>
<td>• 61617 TCP (SSL) to and from BEMS servers in the same cluster (bidirectional)</td>
</tr>
<tr>
<td></td>
<td>• In a SharePoint Online environment, 433 to the following:</td>
</tr>
<tr>
<td></td>
<td>• login.microsoftonline.com</td>
</tr>
<tr>
<td></td>
<td>• *.sharepoint.com</td>
</tr>
<tr>
<td></td>
<td>• In an Azure Information Protection environment, 443 to the following:</td>
</tr>
<tr>
<td></td>
<td>• login.microsoftonline.com</td>
</tr>
<tr>
<td></td>
<td>• graph.microsoft.com</td>
</tr>
<tr>
<td></td>
<td>• *.aadrm.com</td>
</tr>
<tr>
<td></td>
<td>• In a Box environment, 443 to *.box.com</td>
</tr>
</tbody>
</table>

**Note:** For installing Connect for Microsoft Lync Server or or Skype for Business, if the Microsoft Lync Server or Skype for Business database server is using a static port then open that port. The range of ports is necessary only when the Microsoft Lync Server or Skype for Business database server is using dynamic ports.

**Important:** Devices must be able to connect to the Apple (APNS) and cloud messaging servers to receive push notifications from BEMS. If your Wi-Fi network restricts outbound access, make sure that the proper outbound ports are open for your devices.
<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal ports</td>
<td>The following ports are used by BEMS:</td>
</tr>
<tr>
<td></td>
<td>• 8080 or 8082 for use by the BlackBerry Connect service</td>
</tr>
<tr>
<td></td>
<td>• 8101 for SSH connectivity to BEMS</td>
</tr>
<tr>
<td></td>
<td>• 8443 for Push Notifications and Presence</td>
</tr>
<tr>
<td></td>
<td>• 8099 for use by the .NET Component Manager</td>
</tr>
<tr>
<td></td>
<td>• 8060 for use by the Lync Presence Provider (LPP)</td>
</tr>
<tr>
<td></td>
<td>• 6379 for use by Lync Presence Provider (LPP) in a Microsoft Lync or 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.</td>
</tr>
<tr>
<td>TCP/IP port access to the database</td>
<td>• 1433 to the Microsoft SQL Server default</td>
</tr>
<tr>
<td>Upload BEMS statistics</td>
<td>For BEMS to upload the BEMS statistics to the BlackBerry Dynamics NOC, BEMS-Core must be able to access the following:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://gwmonitor.good.com">https://gwmonitor.good.com</a></td>
</tr>
<tr>
<td></td>
<td>• TCP port 443</td>
</tr>
<tr>
<td></td>
<td>For more information, visit support.blackberry.com/community to read article 43542 and 36470.</td>
</tr>
<tr>
<td>Upload log files</td>
<td>For BEMS to be able to upload logs, it must have access to the following:</td>
</tr>
<tr>
<td></td>
<td>• <a href="https://login.good.com">https://login.good.com</a></td>
</tr>
<tr>
<td></td>
<td>• <a href="https://gwupload.good.com">https://gwupload.good.com</a></td>
</tr>
<tr>
<td></td>
<td>• TCP port 443</td>
</tr>
<tr>
<td></td>
<td>For more information, visit support.blackberry.com/community to read article 43542 and 36470.</td>
</tr>
</tbody>
</table>

1 A plus sign (+) indicates support for service packs and updates released subsequent to the core version.

2 BEMS requires visibility of all BlackBerry Proxy servers (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, etc.

**Setting up a Windows service account for BEMS**

For the required service account, "BEMSAAdmin" 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 use the same service account for the Connect and Presence services, you must give the service account the RTCUniversalReadOnlyAdmins privilege.
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 name (UID, distinct from the account password) must be strictly alphanumeric; no special characters are allowed with the (exception of: underscore (_) and hyphen (-). For example, BEMSAdmin.
- Account Password (distinct from the account name above ) must not contain these characters: semicolon (;), at sign (@), slash mark (/), and caret (^).
- Password Expires option must be set to Never for this account.
- This service account should be a member of local administrator group on the BEMS host machine.

Change the BEMS service account password

1. Log on to the BEMS server 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 the services.
4. For the Good Technology Connect service and Good Technology Presence service,
   - 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.
5. Log on to the BEMS dashboard.
6. Under BlackBerry Services Configuration, click Mail > Microsoft Exchange. If the Use Windows Integrated Authentication checkbox is clear, and the same service account is used, update the password, run a test, and then save the configuration.
7. If the Good Technology Connect and Good Technology Presence services use the same service account, update that password and save the configuration.

Configure permissions for the service account

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.

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.
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.

Configure the Java Runtime Environment

JRE 8 is required for BEMS support of intranet applications and other e-business solutions that are the foundation of corporate computing. After installing the JRE, the JAVA_HOME system environment variable must be set.

1. On the computer that hosts BEMS, right-click Computer (Windows Server 2008) or This PC (Windows Server 2012). Click Properties.
2. Click Advanced system settings.
3. Click the Advanced tab.
4. Click Environment Variables.
5. 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.
6. In the Variable value field, type the full path to the Java install folder for the 64-bit JRE. For example, type C:\Program Files\Java\jre1.8.0_<version> or C:\Program Files\AdoptOpenJDK \jdk-8.0<version>-hotspot\jre
   If you use an OpenJDK version and include the direct path to the java.exe file, the BEMS installer returns the error message: Could not find a valid Java virtual machine to load. You may need to reinstall a supported java virtual machine.
7. Click OK.
8. In the System variables section, locate the Path variable. Click Edit.
9. In the Variable value field, append the JAVA_HOME variable, separated by a semi-colon. For example, add ; %JAVA_HOME%\bin
10. Click OK. Click OK again.

Prerequisites: Connect for Microsoft Lync Server and Skype for Business

**Note:** 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 about load balancing requirements, visit https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/load-balancing.

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

- Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business requirements
- BlackBerry Connect service database requirements
- Prepare the Lync Topology for Connect
- SSL certificate requirements for Microsoft Lync Server or 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:

- Verify the Microsoft .NET Framework
- BlackBerry Connect service database requirements

Preparing the computer that hosts BEMS for use with Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business

If you plan to install BEMS for use with Microsoft Lync Server 2010, Microsoft Lync Server 2013 or Skype for Business, you must verify that the computer that you install BEMS on meets specific requirements.

**Note:** All instant messaging server platforms, including Microsoft Lync Server 2010, require the Connect service to be installed on a computer that runs Microsoft Windows Server 2012 or Microsoft Windows Server 2016.

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

Before you install BEMS, you must perform the following actions in the order that they are listed.

1. Install and enable a command-line shell and scripting tool.
   - On a computer that is running Windows Server 2016, Windows PowerShell is enabled by default. Open Windows PowerShell and run the following script: `Set-ExecutionPolicy -Scope CurrentUser RemoteSigned`.
   - On a computer that is running Windows Server 2012, if required, use the Windows Server Manager to add Windows PowerShell 3.0 as a feature. When the installation prompts you to restart the computer, click **Yes**.
     - Open Windows PowerShell and run the following script: `Set-ExecutionPolicy -Scope CurrentUser RemoteSigned`.

   - On a computer that is running Windows Server 2016, no action is required. Microsoft .NET Framework is installed and enabled by default.
   - On a computer that is running Windows Server 2012, use the Windows Server Manager to add Microsoft .NET Framework as a feature. When the installation prompts you to restart the computer, click **Yes**.

3. Complete one of the following tasks using the Windows Server Manager:
   - If you install BEMS on a computer that is running Windows Server 2016, no action is required.
   - If you install BEMS on a computer that is running Windows Server 2012, install **Media Foundation**. When the installation prompts you to restart the computer, click **Yes**.

4. Download and install Microsoft Unified Communications Managed API.
   **Note:** Consult your vendor documentation to determine if the Microsoft Unified Communications Managed API version is supported by your operating system.
   - If you use Skype for Business, download Microsoft Unified Communications Managed API 5.0 Runtime (UcmaRuntimeSetup.exe). To download the file, visit [www.microsoft.com/download](http://www.microsoft.com/download) and search for ID=47344.
   - If you use Microsoft Lync Server 2013, download Microsoft Unified Communications Managed API 4.0 Runtime (UcmaRuntimeSetup.exe). To download the file, visit [www.microsoft.com/download](http://www.microsoft.com/download) and search for ID=34992.
   - If you use Microsoft Lync Server 2010, contact Microsoft for the Microsoft Unified Communications Managed API 3.0 download.
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 environment, download and install the following files:
   - Microsoft Visual C++ 2012 x64 Minimum Runtime – 11.0.50727. To download the file, click here.
   - Microsoft Lync Server 2013 persistent chat server SDK. To download the file, visit https://www.microsoft.com/download and search for id=35458.

   If you enable persistent chat in a Microsoft Lync Server 2013 environment, download and install the persistent chat server SDK. To download the file, visit https://www.microsoft.com/download and search for id=35458.

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

**BlackBerry Connect service database requirements**

You must create a blank SQL database for the Connect service. The recommended name for this database is BEMS-Connect.

During installation, you are prompted to specify the database server and Microsoft SQL Server instance. When you enter this information, the BEMS installation files automatically create the schema required by the Connect service.

**Note:** If your environment includes a single BEMS cluster, only one SQL database is required for all computers hosting the BlackBerry Connect service.

**Preparing the Microsoft Lync Server and Skype for Business topology for BEMS**

The Connect service and Lync Presence Provider (LPP) are Microsoft Lync trusted-UCMA applications.

**Note:** You must be a member of the RTCUniversalServerAdmins and Domain Admins security groups to provision and publish new applications in the Microsoft Lync Server and Skype for Business Topology. If you have a designated Microsoft Lync Server or 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 trust application servers with the Microsoft Lync Server and Skype for Business, you must use the Microsoft Lync Server or 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 and 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 these changes to the Microsoft Lync Server and 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 Microsoft Lync Server or 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 Microsoft Lync Server or 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 Microsoft Lync Server or 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 BEMS Configuration content.

Important: If you change the instant messaging server from Microsoft Lync Server to Skype for Business, you must remove the existing provisioning of BEMS as a trusted application and trusted application pool and then establish trust with the Create a trusted application pool by preparing the initial computer hosting Skype for Business server. For steps on changing the instant messaging service, see Steps to upgrade BEMS and change the instant messaging service.

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

• Preparing the initial computer hosting BEMS
• Preparing additional computers hosting BEMS.

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 Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business.
2. Open the Management Shell.
3. On the computer that hosts the Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business, create the trusted application pool.
   a) To obtain the SiteID of your Microsoft Lync Server, type Get-CsSite. Press Enter. Record the SiteID.
   b) To display the Registrar service value for a selected site, type Get-CsSite <SiteID> | Select-Object -ExpandProperty Services. Press Enter. Record the Registrar service value.
   c) To configure the trusted application entry for the newly created trusted application pool for BEMS, type New-CsTrustedApplicationPool -Force -Identity <YourPoolFQDN> -Registrar <registrar> -RequiresReplication $false -Site <SiteID> -ComputerFQDN <BEMSFQDN>. Press Enter.
      • 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.

d) To create a trusted application entry, type `New-CsTrustedApplication -Force -ApplicationId <appid_connect> -TrustedApplicationPoolFqdn <YourPoolFQDN> -Port 49555. Press Enter.`

• Where `<appid_connect>` is the desired application ID of the BEMS Connect service.

For example, `New-CsTrustedApplication -Force -ApplicationId appid_connect -TrustedApplicationPoolFqdn BEMSAppPool.mycompany.com -Port 49555`

e) If you deploy the Presence service, create a second application entry. Type `New-CsTrustedApplication -Force -ApplicationId <appid_presence> -TrustedApplicationPoolFqdn <YourPoolFQDN> -Port 49777. Press Enter.`

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

For example, `New-CsTrustedApplication -Force -ApplicationId appid_presence -TrustedApplicationPoolFqdn BEMSAppPool.mycompany.com -Port 49777`

f) If you deploy the Presence service, create an application endpoint. Type `New-CsTrustedApplicationEndpoint -ApplicationId <appid_presence> -TrustedApplicationPoolFqdn <YourPoolFQDN> -SipAddress "sip:presence_<BEMSFQDN>@<SIPDomain>"`. For example, `New-CsTrustedApplicationEndpoint -ApplicationId appid_presence -TrustedApplicationPoolFqdn BEMSAppPool.mycompany.com -SipAddress "sip:presence_BEMSHost.mycompany.com@mycompany.com"

g) To publish the change to the Microsoft Lync Server or Skype for Business environment, type `Enable-CsTopology. Press Enter.`

**After you finish:** If you are installing multiple BEMS servers, see [Prepare additional computers hosting BEMS](#).

### 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 Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business using an account with RTCUniversalServerAdmins group permissions.

2. Open the **Management Shell**.

3. On the computer that hosts the Microsoft Lync Server 2010, Microsoft Lync Server 2013, or 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, type `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. Type `New-CsTrustedApplicationEndpoint -ApplicationId <appid_presence> -TrustedApplicationPoolFqdn <YourPoolFQDN> -SipAddress "sip:presence_<BEMSFQDN>@<SIPDomain>"`. Press Enter.
   • 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 the Microsoft Lync Server and Skype for Business environment, type `Enable-CsTopology`. Press Enter.

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".

Removing 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.

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

If your environment is running both a Microsoft Lync Server and 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 Microsoft Lync Server 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, type `Get-CsTrustedApplicationComputer -Identity <FQDN_of_the_bems_host>`. Press Enter. Record the Pool name.
   b) To display all the computers in the Pool name recorded in step 2a, type `Get-CsTrustedApplicationPool -pool <FQDN_of_the_pool_from_step_a>`. Record if more than one FQDN entry is listed.
   c) To display additional information about the above Trusted Application Pool, type `Get-CsTrustedApplicationPool -PoolFqdn <FQDN_of_the_pool_from_step_a>`. Press Enter.
d) To remove one BEMS instance from the trusted application pool when you have more than one BEMS instance in your organization’s environment, type `Remove-CsTrustedApplicationComputer -Identity <FQDN_of_the_bems_host>`. Press Enter.

e) To remove all BEMS instances from the Trusted Application Pool and remove the pool itself, type `Remove-CsTrustedApplicationPool -Identity <FQDN_of_the_pool_from_step_2a>`.

f) To publish the change to the Microsoft Lync Server environment, type `Enable-CsTopology`. Press Enter.

g) To verify that the trusted application pool is removed, type `Get-CsTrustedApplicationComputer -Identity <FQDN_of_the_bems_host>`.

SSL certificate requirements for Microsoft Lync Server, Skype for Business, and Presence

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.

**Mutual TLS (MTLS) certificates**

Connect and Lync Presence Provider (LPP) connections to the Microsoft Lync Server 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 Microsoft Lync Server deployments, certificates issued by the enterprise CA that 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 private certificate issued for BEMS by a trusted CA must be stored on the computer hosting BEMS. Console Root\Certificates <local_host_name>\Personal\Certificate folder.
- The BEMS computer’s private certificate and the Microsoft Lync Server’s internal computer certificate must both be trusted by root certificates in BEMS’s Console Root\Certificate <local_host_name> \Trusted Root Certification Authorities\Certificates folder.
- Intermediate certificates for both the BEMS private certificate and the Microsoft Lync Server internal computer certificate must be located in the BEMS Console Root\Certificates <local_host_name> \Intermediate Certification Authorities\Certificates folder.
- The Subject Name (SN) of the certificate must contain the Common Name (CN) of the fully qualified domain name (FQDN) of the computer that is hosting the BEMS instance (for example, CN=bemsserver.example.com).
- The Subject Alternative Name (SAN) must contain the DNS items of the FQDN for the trusted application pool and the FQDN of the computer that is hosting the BEMS instance. For more information about the trusted application pool name, see Prepare the initial computer hosting BEMS.
- The certificate must be signed by a CA that is mutually trusted by both the Microsoft Lync Server and BEMS.

**Note:** 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.
Create and add the BEMS SSL certificate for Microsoft Lync Server 2010, Microsoft Lync Server 2013, and Skype for Business

A SAN SSL Certificate, also known as Unified Communications SSL Certificate (UCC SSL), is mainly used by Microsoft Exchange Server 2007 or later for unified messaging. This certificate allows multiple server or domain names to use the same secure SSL certificate. In a SAN certificate, several alternatives of common names can be placed in the Alternative Name field.

**Note:** Any existing and appropriate SAN certificate, for example your Exchange SAN certificate, can be used to create a template, or you can create a new template from any existing template, which can then be used to create and configure the required certificate for a given service.

The name of the template is often the only way to distinguish its purpose. The certificate common name (CN), friendly names, and other properties 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 generating SSL certificates with subject alternative names, visit the Technet Library to see How to generate a certificate with subject alternative names (SAN).

Create a Personal Certificate for the local computer account for BEMS

Complete this task when you configure the computer hosting the Presence service only or both Presence and Connect service.

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 the `<BEMSFQDN>` of the computer that hosts the Connect service. For example, BEMSHost.mycompany.com.
   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 `<BEMSFQDN>` of the computer that hosts the Connect service. For example, BEMSHost@mycompany.com.
   c) Click **Add >**.
   d) Again, in the **Value** field, type the `<YourPoolFQDN>` of the BEMS Lync Pool FQDN as was recorded in step 3c of Prepare the initial computer hosting BEMS. For example, BEMSAppPool.mycompany.com.
Preparing the computer that hosts BEMS for use with Skype for Business using non-trusted application mode

If you plan to install BEMS for use with Skype for Business and configure the Connect service as non-trusted by Skype for Business, you must verify that the computer that you install BEMS on meets specific requirements.

Turn off antivirus software for computers running BEMS with BlackBerry Connect.

Note: Support for Skype for Business with the Connect service configured using non-trusted application feature requires the latest version of the BlackBerry Connect app. An updated BlackBerry Connect app will be released in the near future.

1. Install and enable Microsoft .NET Framework 4.6 or later. For more information about .Net Framework system requirements, visit https://docs.microsoft.com/en-us/dotnet/framework/get-started/system-requirements.
   • On a computer that is running Windows Server 2016, no action is required. Microsoft .NET Framework is installed and enabled by default.
   • On a computer that is running Windows Server 2012, use the Windows Server Manager to add Microsoft .NET Framework as a feature. When the installation prompts you to restart the computer, click Yes.

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

Prerequisites: Connect for Skype for Business Online

Note: 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.

• Skype for Business Online requirements
• BlackBerry Connect service database requirements

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

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

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

1. Install and enable Microsoft .NET Framework 4.6 or later. For more information about .Net Framework system requirements, visit https://docs.microsoft.com/en-us/dotnet/framework/get-started/system-requirements.
   • On a computer that is running Windows Server 2016, no action is required. Microsoft .NET Framework is installed and enabled by default.
• On a computer that is running Windows Server 2012, use the Windows Server Manager to add Microsoft .NET Framework as a feature. When the installation prompts you to restart the computer, click Yes.

2. Download and install Microsoft Unified Communications Managed API 5.0 Runtime (UcmaRuntimeSetup.exe). To download the file, visit www.microsoft.com/download and search for ID=47344.

   Note: Consult your vendor documentation to determine if the Microsoft Unified Communications Managed API version is supported by your operating system.

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

Presence prerequisites: Microsoft Lync Server, Skype for Business, and Skype for Business Online

For Microsoft Lync Server and Skype for Business, the Presence service has the same predeployment requirements as the Connect service. The Presence service does not require its own Microsoft SQL Server database. For more information about prerequisites, see the following: Prerequisites: Connect for Microsoft Lync Server and Skype for Business

- Environments that use Microsoft Lync Server or Skype for Business on-premises using trusted application mode, see Prerequisites: Connect for Microsoft Lync Server and Skype for Business.
- Environments that use Skype for Business Online or Skype for Business on-premises using non-trusted application mode, see Prerequisites: Connect for Skype for Business Online.

Note: Presence for Skype for Business Online or 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.

Prerequisites: BlackBerry Push Notifications service

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

In general, 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:

Cloud-based BEMS with on-premise Microsoft Exchange

1. You must expose Microsoft Exchange Web Services and Autodiscover from your on-premise 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-Premise BEMS with Cloud-based Exchange

1. You must expose Microsoft Exchange Web Services and autodiscover from cloud-based Microsoft Exchange to on-premise BEMS on port 443.
2. Although both basic authentication and Windows authentication are supported by BEMS, be advised that certain cloud vendors—for instance, Microsoft Office 365 and Rackspace—only support basic authentication. Check with your specific cloud vendor for details.

**On-premise BEMS with on-premise and cloud-based Microsoft Exchange**

1. You must expose Microsoft Exchange Web Services and autodiscover from cloud-based Microsoft Exchange to on-premise BEMS on port 443.
2. Although both basic authentication and Windows authentication are supported by BEMS, be advised that certain cloud vendors—for instance, Microsoft Office 365 and Rackspace—only support basic authentication. Check with your specific cloud vendor for details.
3. A BEMSAdmin mailbox must first be created on premise and then migrated to the cloud.
4. The BEMSAdmin account must have impersonation rights on both the on-premise and Microsoft Office 365 Microsoft Exchange systems. For details, visit support.blackberry.com/community to read article 40155.

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

- Configure the Autodiscover Service for Internet Access
- Configuring EWS for External Access

**Supported Load Balancer affinity using Microsoft Exchange Server 2010**

If your environment uses Microsoft Exchange Server 2010 to connect to BEMS, you can configure the Load Balancer to use Cookie-based or Source IP-based affinity.

Configuring affinity provides the ability for the load balancer to maintain a connection between the BEMS instance and the specific Microsoft Exchange Server node that BEMS is connected to. Configuring affinity in your Microsoft Exchange Server 2010 environment is important because in the Microsoft Exchange Server 2010, the Microsoft Exchange Web Services (EWS) subscriptions reside on the client access server (CAS). CAS nodes are usually referenced using a logical array name. When BEMS makes a request to the CAS, it makes a request for the user and the CAS returns the subscription that references that request for the user. You must make sure that the CAS that BEMS makes the EWS subscription request to is the same CAS that BEMS connects to with the subscription. BEMS batches the subscription requests and submits the batch request to the CAS. For more information about configuring affinity on the Load Balancer, refer to your Load Balancer documentation.

**Microsoft Exchange Web Services proxy support**

Microsoft Exchange Web Services (EWS) lets client applications communicate with the Microsoft Exchange Server using SOAP messages sent by HTTP. Proxying occurs when a client access server (CAS) role sends traffic to another client access server role. For example,

- CAS to CAS communication between two Microsoft Active Directory sites
- CAS to CAS communication between Microsoft Exchange Server 2010 and Microsoft Exchange Server 2013

The following CAS protocols and services are proxy enabled:

- Microsoft Exchange Web Services (EWS) and the availability service (part of EWS)
- Microsoft Exchange ActiveSync (EAS)
- Microsoft Outlook Web Access (OWA) and Exchange Control Panel (ECP)
- POP3 / IMAP

**Microsoft Exchange Web Services Namespace Configuration**

If you have Microsoft Exchange Server instances deployed in multiple Microsoft Active Directory sites, a unique internal Microsoft Exchange Web Services (EWS) URL must be configured for each site for the BlackBerry Push...
Notifications service to work properly. Consider the following scenario: an environment with two Microsoft Active Directory sites and each site has two Client Access Servers (CAS).

- Site 1: CAS 1, CAS 2
- Site 2: CAS 3, CAS 4

In this case, at least two unique internal Microsoft Exchange Web Services URLs are required, one for Site 1 and one for Site 2. The URLs look something like the following:

- Site1: https://site1cas.domain.com/EWS/Exchange.asmx
- Site2: https://site2cas.domain.com/EWS/Exchange.asmx

It is also valid to configure a unique internal Microsoft Exchange Web Services URL for each client access server.

Before modifying the internal Microsoft Exchange Web Services URL for your client access servers, first check which Microsoft Active Directory site the client access servers are in and what the current internal Microsoft Exchange Web Services URL is set to by running the following command on the Microsoft Exchange Server:

1. Open a command prompt.

The "Dc Site Name" output parameter indicates the Microsoft Active Directory site. For more information on how to use the NLTEST command, visit support.blackberry.com/community to read article 41948.

For information on how to check the internal URL on a CAS server, visit support.blackberry.com/community to read article 41943.

Create a mailbox for the BEMS service account

Using the Microsoft Exchange Management Console or Exchange shell, create a mailbox for the BEMS service account. For instructions, refer to the Microsoft Exchange Server resource for details and tutorials.

Grant application impersonation permission to the BEMS service account

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

1. Depending on your environment, open Microsoft Exchange Management Shell or Microsoft Exchange Online Powershell for Microsoft Office 365.

After you finish:

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.

Set Basic authentication for the Microsoft Exchange Web Services protocol

The BlackBerry Push Notifications service supports Basic, NTLM and Windows Authentication when connecting with Microsoft Exchange Server using Microsoft Exchange Web Services (EWS). Basic authentication is turned off by default on the Microsoft Exchange Server.

Optionally, if Basic authentication is preferred, the command that follows can be used to update Microsoft Exchange to use Basic authentication for EWS connectivity. Regardless of authentication method used on Microsoft Exchange for EWS, no extra configuration is necessary for BEMS.

1. Open Microsoft Exchange Management Shell.
2. Type `Set-WebServicesVirtualDirectory -Identity "Contoso\EWS(Default Web Site)" -BasicAuthentication $true`.
   Where `Contoso\EWS(Default Web Site)` is the identity for the Microsoft Exchange Web Services virtual directory.

**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 about using EWSEditor, visit support.blackberry.com/community to read article 40351.

**BlackBerry Push Notifications database requirements**

You must create a blank SQL database for the BlackBerry Push Notifications service. The recommended name for this database is BEMS-Core.

**Note:** Make sure 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.

**Verify the case sensitivity of the BlackBerry Push Notifications database**

Run the following SQL query: `SELECT DATABASEPROPERTYEX('dbname', 'Collation')`  
Where `dbname` is the name for 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.

**Prerequisites: Cisco Unified Communications Manager IM and Presence Service requirements for Presence**

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. If your environment is running Cisco Unified Communications Manager 10.5.1 or later, log in to the Cisco Unified Communications Manager Administration console. If your environment is running Cisco Unified Communications Manager earlier than 10.5.1, log in to Cisco Unified Presence 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) version 10.5.1 and later 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 running an older version of Cisco Unified Communications Manager and Cisco IM and Presence or you are 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 Cisco Unified Communications Manager (CUCM) and Cisco IM and Presence (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:
<table>
<thead>
<tr>
<th>Service</th>
<th>Certificates or CSRs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the Connect service only¹</td>
<td>• Enterprise Root CA certificate</td>
</tr>
<tr>
<td></td>
<td>• Tomcat Certificate Signing Request (from CUCM)</td>
</tr>
<tr>
<td></td>
<td>• Tomcat - CA signed certificate</td>
</tr>
<tr>
<td></td>
<td>• Tomcat - ECDSA CA signed certificate (in a Cisco 11.5 environment environment)</td>
</tr>
<tr>
<td></td>
<td>• Cup-xmpp Certificate Signing Request (from CIMP)</td>
</tr>
<tr>
<td></td>
<td>• Cup-xmpp CA signed certificate</td>
</tr>
<tr>
<td></td>
<td>• Cup-xmpp-ECDSA CA signed certificate (from CIMP in a Cisco 11.5 environment environment)</td>
</tr>
<tr>
<td>Configure the Presence service only¹</td>
<td>• Enterprise Root CA certificate</td>
</tr>
<tr>
<td></td>
<td>• Tomcat Certificate Signing Request (from CUCM)</td>
</tr>
<tr>
<td></td>
<td>• Tomcat - CA signed certificate</td>
</tr>
<tr>
<td></td>
<td>• Tomcat - ECDSA CA signed certificate (in a Cisco 11.5 environment environment)</td>
</tr>
<tr>
<td></td>
<td>• Cup Certificate Signing Request (from CIMP)</td>
</tr>
<tr>
<td></td>
<td>• Cup - CA signed certificate</td>
</tr>
<tr>
<td></td>
<td>• Cup-xmpp-ECDSA CA signed certificate (from CIMP in a Cisco 11.5 environment environment)</td>
</tr>
</tbody>
</table>

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. If your environment is running CUCM and CIMP 10.5.1 or later, complete the following tasks on the CUCM Publisher and the IM and Presence Publisher. If your environment is running CUCM and IM and Presence version earlier than 10.5.1, or 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 6h.
   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: Docs service**

The Docs service requires its own Microsoft SQL Server database. And, while having many of the BEMS core requirements in common, it has additional dependencies not required by the other services.

When you configure the BEMS service, you complete the following additional actions:
• Server software and operation system requirements
• Database requirements
• CMIS requirements

Server software and operating system requirements

In addition to core requirements for all BEMS services, the following prerequisites apply to the Docs service:

Network Capabilities and Resources

• The computer that hosts BEMS must be a domain member and have access to the Microsoft Active Directory.
• Network shares must be accessible from BEMS.
• Microsoft SharePoint sites must be accessible from BEMS.

Database Requirements

A blank Microsoft SQL Server database is required for a new installation of the BlackBerry Docs service. It is recommended that you name the database "BEMS-Docs". The installer extends the schema during the installation process.

If you are migrating an existing database from BlackBerry Share, see Appendix A: Migrating your Good Share database to BEMS-Docs.

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.

Note: 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.

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

Install the BEMS software

Before you begin:

• Make sure that you install BEMS on an English implementation of the operating system.
• If your organization uses AlwaysOn support for SQL Server, make sure you complete the steps in Appendix: AlwaysOn Availability support for SQL Server and 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.

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, complete one of the following tasks:
   • If you use an OpenJDK JRE, double-click InstallBEMS.bat.
   • If you use Oracle's Java, double-click GoodEnterpriseMobilityServer.<version number>.exe.

   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 that you are installing BEMS or the JAVA_HOME system variable isn't specified correctly, the error message Could not find a valid Java virtual machine to load. You may need to reinstall a supported java virtual machine. For more information on prerequisite requirements, see the Preinstallation checklists. For instructions on setting the JAVA_HOME system variable, see Configure the Java Runtime Environment.

5. In the BlackBerry Enterprise Mobility Server v<version number> setup screen, in the Introduction dialog box, click Next.
6. In the License Agreement dialog box, select I accept the terms of the License Agreement. Click Next.
7. In the Services dialog box, select the services you want to install. Click Next.

   Scroll to the bottom of the page to view all of the service options.

8. In the Prerequisite dialog box, click Next.

   Note: 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.

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 Setting up a Windows service account for BEMS. Click Next.
14. In the Database Information dialog box, perform the following actions:
<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
</table>
| **Specify the Microsoft SQL Server connection information for the BEMS-Core service database.** | a. **In the Host** field, type the instance name of your SQL Server. If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener.  

b. **In the Database name** field, type the name for the BEMS-Core database. For example, BEMS-Core.  

   - If the Core database is located on a default instance of the SQL Server (for example, MSSQLSERVER or SQLEXPRESS), type the SQL Server host name.  
   - If the Core database is located on a computer with an instance name other then the default instance of the SQL Server, type the `<server name>\<database instance name>:<port number>`. For example, bems01\MSSQLSERVER:1433.  

   **Note:** When you configure the database in the Dashboard, make sure you type `<server name>\<database instance name>:port number`

   If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group.  

c. **In the Port** field, type the port number that connects to the SQL Server.  

d. Optionally, in the **Additional Properties** field, 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 `MultiSubnetFailover=true`.  

e. By default, the setup application uses SQL Server authentication to connect to the BEMS database. Select **Windows Authentication**. Click Next. |
| **Enter the BEMS service account login credentials under which the BEMS-Connect Windows service run.** | a. **In the Login** field, type the BEMS service account login information (for example, `<domain123>.example.com\<BEMS service account username>`).  

b. **In the Password** field, type the BEMS service account password.  

c. Click Next. |
<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Specify the SQL Server connection information for the BEMS-Connect service database. | a. In the Host field, type the instance name of your SQL Server. If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener.  
b. In the Database name field, type the name for the BEMS-Connect database. For example, BEMS-Connect.  
c. In the Port field, type the port number that connects to the SQL Server. By default, this port is 1433  
d. Optionally, in the Additional Properties field, 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.  
e. By default, the setup application uses the SQL Server authentication to connect to the BEMS database. Select Windows Authentication. Click Next.  
| Enter the BEMS service account login credentials under which the BEMS-Presence Windows service run.  
**Note:** A database is not created for the Presence service. | a. In the Login field, type the BEMS service account login information (for example, `<domain123>.example.com\<BEMS service account username>`).  
b. In the Password field, type the BEMS service account password.  
c. Click Next.  
| Specify the SQL Server connection information for the BEMS-Docs service database. | a. In the Host field, type the instance name of your SQL Server. If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener.  
b. In the Database name field, type the name for the BEMS-Docs database. For example, BEMS-Docs. If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group.  
c. In the Port field, type the port number that connects to the Microsoft SQL Server.  
d. Optionally, in the Additional Properties field, 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.  
e. By default, the setup application uses SQL Server authentication to connect to the BEMS database. Select Windows Authentication.  
f. Click Next.  

15. In the Replace JCE Policy dialog box, click Next.  
16. In the Pre-installation Summary dialog box, click Install to install BEMS.  
17. In the Installing dialog box, complete one or more of the following actions
a) Click **Next** when the BEMS-Mail installation is complete.
b) Click **Next** when the BEMS-Connect installation is complete.
c) Click **Next** when the BEMS-Presence installation is complete.
d) Click **Next** when the BEMS-Docs installation is complete.

18. Optionally, in the **Installing, Upload Credentials** dialog box, you can provide your BlackBerry Online Portal credentials, cluster name and domain name. You can skip this screen and configure this information later in the BEMS Dashboard. Click **Next**.

If you skip this step during the installation and do not configure the dashboard, you are prompted for this information each time that you upgrade the BEMS instance. Providing this information allows BlackBerry to collect statistical information (for example, the version of BEMS that is installed) and makes uploading the BEMS logs to BlackBerry Technical Support Services easy. For more information about BEMS statistics, see **Enable upload of BEMS statistics**.

- Click **OK** to enter your credentials. The credentials prepopulate the **Enable upload of BEMS statistics** and **Log Upload Credentials** in the dashboard.
- Click **Skip** to continue with the installation. If the **Allow BEMS to send statistics information to BlackBerry** check box is selected and you provide the credentials in the **Log Upload Credentials** in the dashboard, the **Enable upload of BEMS statistics** are configured automatically.

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

The setup application opens the BEMS Dashboard at https://localhost:8443/dashboard. By default, the BEMS Dashboard locks after 30 minutes of inactivity.

**After you finish:** Complete the BEMS configuration in the BEMS dashboard.

**Upgrade BEMS**

When you upgrade BEMS, 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**.

**Before you begin:**
- Make sure you log in with the BEMS service account you created to install BEMS.
- Verify that you have the password for the BEMS service account.
- Stop the Good Technology Common Services on each computer in the cluster that hosts BEMS.
- If you upgrade BEMS in a cluster environment, back up the BEMS cluster database.

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** installation folder, complete one of the following tasks:
   - If you use an OpenJDK JRE, double-click **InstallBEMS.bat**.
   - If you use Oracle’s Java, double-click **GoodEnterpriseMobilityServer.<version number>.exe**.

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 that you are installing BEMS or the JAVA_HOME system variable isn’t specified correctly, the error message **Could not find a valid Java virtual machine to load. You may need to reinstall a supported java**
virtual machine. For more information on prerequisite requirements, see the Preinstallation checklists. For instructions on setting the JAVA_HOME system variable, see Configure the Java Runtime Environment.

5. In the BlackBerry Enterprise Mobility Server version number setup screen, in the Introduction dialog box, select Upgrade. Click Next.

6. In the License Agreement dialog box, select I accept the terms of the License Agreement.

7. Click Next.

8. In the Services dialog box, click Next

9. In the Prerequisite dialog box, click Next.

   Note: 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.

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. 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. 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. Click Next.

   If your environment uses AlwaysOn with multi-subnet deployment, in the Additional Properties field, type MultiSubnetFailover=true.

21.In the Replace JCE Policy Files dialog box, click Next.

22.In the Pre-installation Summary dialog box, click Install to install BEMS.

23.In the Upgrade Complete dialog box, complete the following actions:

   a) Click Next when the BEMS-Mail upgrade is complete.
   b) Click Next when the BEMS-Connect upgrade is complete.
   c) Click Next when the BEMS-Presence upgrade is complete.
   d) Click Next when the BEMS-Docs upgrade is complete.

24.If you upgraded from a version of BEMS earlier than 2.10 and didn't specify the upload credentials during a previous installation or in the Dashboard, you are prompted in the Installing, Upload Credentials dialog box to provide your BlackBerry Online Portal credentials, cluster name and domain name. Click Next.

Providing this information allows BlackBerry to collect statistical information (for example, the version of BEMS that is installed) and makes uploading the BEMS logs to BlackBerry Technical Support Services easy. For more information about BEMS statistics, see Enable upload of BEMS statistics. Complete one of the following steps:
• Click OK to enter your credentials. The credentials prepopulate the Upload BEMS Statistics and Log Upload Credentials in the dashboard.

• Click Skip to continue with the installation. If the Allow BEMS to send statistics information to BlackBerry check box is selected and you configure the Log Upload Credentials in the dashboard, the Enable upload of BEMS statistics are configured automatically.

25. 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.

26. Click Done.


Remove Connect and Presence services

When you change the instant messaging service from Microsoft Lync Server 2010 or Microsoft Lync Server 2013 to Skype for Business, you must remove the Connect and Presence service components that are configured for the Microsoft Lync Server from your BEMS instances.

Follow the instructions in Upgrade BEMS. When you run the setup application:

On the Services screen, clear the following checkboxes:

• Under Connect, clear the Provides instant messaging integration with checkbox.
• Under Presence, clear the Provides user presence information from checkbox.

After you finish: To add services, run the setup application and select the service component checkbox for each service that you want to add.

Perform a Silent Install or Upgrade

You can perform a silent new installation or upgrade using the silentInstall.bat file or a command prompt.

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.

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

Removing the BEMS software

1. Remove the BEMS software.
2. Remove the BEMS Connect service reference for BlackBerry Connect.

Remove the BEMS software

1. On the taskbar, click Start > Control Panel.
2. Click Uninstall a program.
3. Click the BlackBerry Enterprise Mobility Server. Click Uninstall.
4. Repeat step 3, for the following BEMS services:
   - BlackBerry Enterprise Mobility Server-Mail
   - BlackBerry Enterprise Mobility Server-Presence
   - BlackBerry Enterprise Mobility Server-Docs
   - BlackBerry Enterprise Mobility Server-Connect
5. In the BlackBerry UEM console, on the menu bar, click Policies and profiles.
6. Click Networks and connections > BlackBerry Dynamics connectivity profile.
7. Click the BlackBerry Dynamics connectivity profile that you want to remove the BEMS instance from.
8. Click Edit.
9. In the Additional servers section, remove the BEMS instances.
10. In the IP address ranges section, remove the BEMS instances.
11. In the App servers section, click X beside the BEMS instance that hosts the BlackBerry Connect entitlement.
12. Repeat step 11 for BlackBerry Work.
13. Click Save.

Remove the BEMS Connect service reference for BlackBerry Connect

1. Log in to the BlackBerry UEM console.
2. On the menu, click Apps.
3. Search for and click the BlackBerry Connect app that you want to remove the BEMS instance from.
4. On the Settings > BlackBerry Dynamics tab, in the App configuration section, click the App Configuration you want to remove the BEMS instance from.
5. On the Server Configuration tab, delete the BEMS instance.
6. Click Save.
Appendices

Appendix A: Migrating your Good Share database to BEMS-Docs

A Good Share deployment can migrate/repurpose its database for the BEMS-Docs service to support existing user transition from the BlackBerry Share client to BlackBerry Work. First, however, BEMS and the Docs Configuration Console must be installed in in the environment.

Client App Support Considerations

The following limitations must be considered in determining whether or not a migration is advisable:

- BlackBerry Share clients communicate with the BlackBerry Share server only; they are not supported by the BEMS-Docs service.
- BlackBerry Work Docs communicates with the BEMS-Docs service only; it is not supported by the Good Share server.

Given these inherent limitations, it is recommended that you continue to run your deployed BlackBerry Share servers in parallel with the BEMS-Docs service for a duration sufficient to conveniently transition your users from their BlackBerry Share client app to BlackBerry Work.

Note: After upgrading your Good Share database to BEMS-Docs, discontinue using the old Good Share Console and use only the BEMS Dashboard Home > Docs pages for administration going forward.

Otherwise, you will want to consider two basic migration scenarios:

- Migrating with continued BlackBerry Share client support
- Migrating to BlackBerry Work only (no BlackBerry Share client support)

Migrate to BEMS-Docs while continuing to support BlackBerry Share clients

1. Install the Docs service. When you are prompted to select the database for Docs, select the Good Share database.
   For instructions, see Install the BEMS software or Upgrade BEMS.

   Once the installation is complete and BEMS is running, both the BEMS-Docs service and Good Share server should be functional and sharing the same data. This means that policies, users, and data sources previously configured for Good Share should all be available in BEMS-Docs. Logged audit data continues to be available, and reports can be generated from the Good Share Web Console.

   Note: If you are using Windows Authentication for the BlackBerry Share database, Good Technology Common Services must run under a user who has access to the Good Share database.

2. When all Good Share users have switched to BlackBerry Work and BlackBerry Share clients are no longer being used, you can uninstall Good Share server and the Good Share Web Console.

Migrate to BlackBerry Work Only

If there is no requirement to support both BlackBerry Work and Good Share at the same time (i.e., concurrently), then the machine(s) used for Good Share can be repurposed in accordance with the following steps:

1. Uninstall Good Share server and the Good Share Web Console but do not remove the database.

2. Install BEMS and configure the Docs service.
   For instructions, see Install the BEMS software or Upgrade BEMS.
Again, if you are using Windows Authentication for the database, Good Technology Common Services must run under a user who has access to the BlackBerry Work database.

3. Launch the BEMS Dashboard, click Docs, then click Database, and here also select the database previously used by BlackBerry Work.

Upon completion of Step 3, all previously configured policies, users, data sources and settings are now available to the BEMS-Docs service and configurable in the Docs Configuration Console.

**Feature Differences (BEMS-Docs versus Good Share)**

The following feature changes will be noticed when comparing BEMS-Docs to Good Share server:

- Open-in application list is now managed in the BlackBerry Control application policy for BlackBerry Work. Any Open-in lists created in Good Share must now be added in BlackBerry Control.
- Keep in-sync feature is not supported.
- Permissions in data sources not supported
  - Allow Native email
  - Print
  - Open in
- Security settings no longer supported
  - Allow playing of media files – iOS only (stored outside of the secure container during playback)
  - Enable device to remember user password
  - Display event information for calendar alerts
  - Force user to save Pending Uploads

**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 2012, 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](https://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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create an AlwaysOn availability group.</td>
</tr>
</tbody>
</table>
### Step 2
Configure SQL Server for AlwaysOn availability.

### Step 3
Install the BEMS software.

### Step 4
Configure the BEMS services databases for AlwaysOn availability.

### Step 5
Configure AlwaysOn availability group failover for single and multi-subnets for the following services:
- 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.

**Note:** 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.

**Important:** 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.

**Before you begin:** 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 steps 1 to 7 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 BEMS.
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 BEMS.

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 BEMS.
Legal notice

©2019 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU 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.

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 QUALITY, 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
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada