Installation and Configuration Guide

BEMS in a Good Control and Good Proxy environment

Version 2.6.5.9

Published: 2017-11-03
SWD-20171103143641203

Contents

About this guide

1

This guide describes how to install, configure, and administer BEMS in your Good Control and Good Proxy environment.

This guide is intended for senior and junior IT professionals who are responsible for setting up and administering BEMS.

What is BEMS?

2

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.

Service	Description
BlackBerry Mail	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.
BlackBerry Connect	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.
BlackBerry Presence	The BlackBerry Presence service provides real-time presence status to third-party BlackBerry Dynamics applications—giving them a powerful add-in for mobile collaboration.
BlackBerry Docs	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.
BlackBerry Directory Lookup	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.
BlackBerry Follow-Me	The BlackBerry Follow-Me service supports the BlackBerry Dynamics Launcher on BlackBerry Work, and will soon be available on other BlackBerry Dynamics apps such as BlackBerry Connect and BlackBerry Access, keeping the BlackBerry Dynamics Launcher synchronized across multiple devices.
BlackBerry Certificate Lookup	The BlackBerry Certificate Lookup service retrieves S/MIME digital certificates from the user's Microsoft Active Directory account and matches the requested key usage. Only the recipient's public certificate is retrieved for matching.

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 Developers for Enterprise Apps.

Installing BEMS in a BlackBerry UEM environment

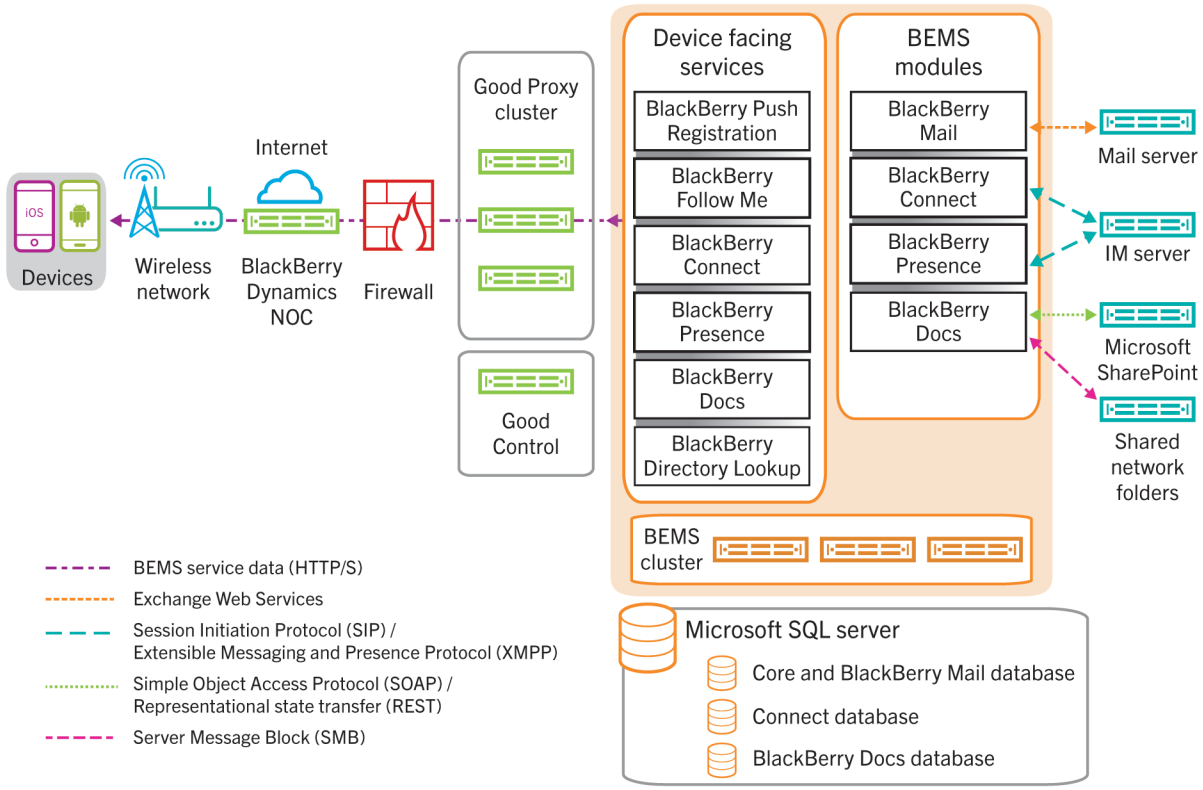
You can install BEMS in a BlackBerry Dynamics and BlackBerry UEM environment. Installing BEMS in a BlackBerry UEM version 12.6 or later environment provides additional services for BlackBerry Dynamics apps.

For more information, see the following guides:

- For information about BEMS hardware requirements,
    - in a BlackBerry UEM environment, see the BlackBerry UEM Planning content.
    - in a BlackBerry Dynamics environment, see the BlackBerry Dynamics Servers and BlackBerry Enterprise Mobility Server Planning content.
- For information about upgrading your Good Control and Good Proxy to BlackBerry Control and BlackBerry Proxy in a BlackBerry UEM environment, see the BlackBerry UEM Installation and upgrade content.

Architecture: BEMS

3

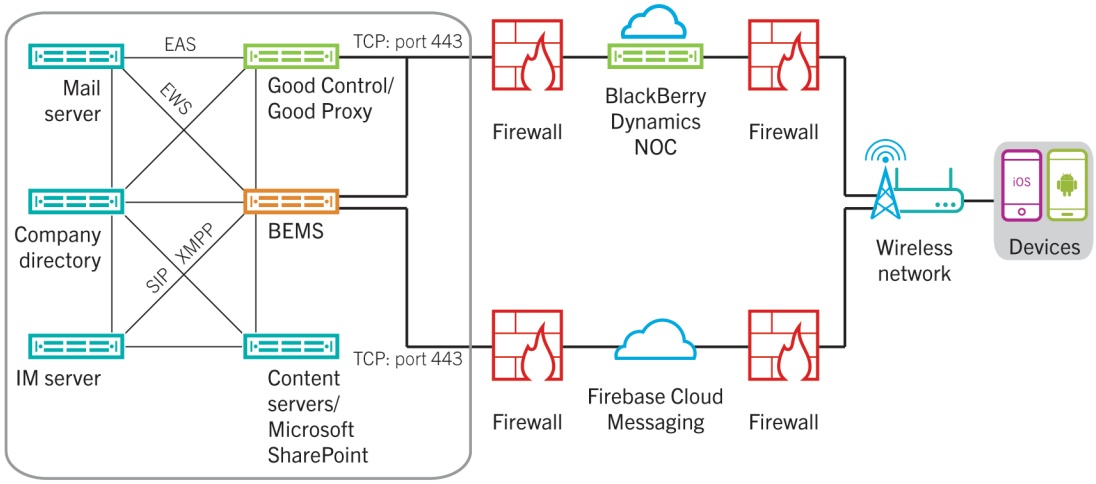


From this high-level architectural view, the diagram does not show how the BlackBerry Work application connects to Microsoft Exchange Server for accessing email. It shows how each BEMS service is accessed by BlackBerry Work on devices, which is BEMS role, to expose secure device-facing services used by BlackBerry Work and make them available to other BlackBerry Dynamics-powered apps. These services currently include BlackBerry Push Registration, BlackBerry Follow Me, BlackBerry Presence, BlackBerry Directory Lookup, and BlackBerry Docs.

Communicating using the protocols shown, the feature modules of BEMS integrate with your backend systems of record using a shared Microsoft SQL Server running multiple databases for Core/Mail, Connect, and Docs.

For high availability, BEMS is deployed as a cluster, with all of its device-facing services provided by all instances of BEMS in the cluster and made available to client devices through the BlackBerry Dynamics infrastructure. Each BlackBerry Dynamics-powered client app connects through a Good Proxy cluster deployed on-premise. Entitlement to use BEMS services is managed through Good Control.

A slightly different view looks like this again at a high level:



It is important to note in the diagram above that the BlackBerry Mail service utilizes the same database server as Good Control. The database server can be local to Good Control or remote.

Some necessary supporting infrastructure is required to support enterprise network operations. Such components include:

- Microsoft Exchange Server
- Microsoft Lync Server
- Skype for Business
- Cisco Unified Communications Manager for IM and Presence
- Microsoft Active Directory
- Good Control
- Good Proxy

For more information about the BEMS architecture in a BlackBerry UEM environment, see the BlackBerry Enterprise Products Guide.

Installation and upgrade

4

Steps to install BEMS

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

Step	Action
1	Verify the prerequisites.
2	Complete the preinstallation tasks.
3	Install the BEMS software.

Supported installation and upgrade paths

To upgrade GEMS to BEMS 2.6, 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 2.6 (2.6.2.5) and later to BEMS 2.6 SR1 using the setup application on the computer that hosts the previous version of BEMS.
- You can upgrade GEMS 2.2 SR1 (2.2.20.20) to BEMS 2.4 (2.4.18.19) and then upgrade to BEMS 2.6 SR1 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 prerequistes and can then install BEMS 2.4.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:

- If you are upgrading GEMS 1.6 and later, administrators must provide their Microsoft Active Directory user credentials to login to the BEMS Dashboard.
- If you are upgrading multiple instances in a cluster, you must upgrade each computer that hosts an instance of GEMS.
- If multiple GEMS 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.
- If you use special characters in the service account for a previous GEMS installation, they must be removed before you perform the upgrade. Special characters are not supported for the BEMS service account.

  Important: The account name is a different property than the account password, which does not support only the following special characters: semicolon (;), at sign (@), slash mark (/). The service account name does not support any special characters.

Steps to upgrade BEMS

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

Step	Action
1	Review the best practices for preparing to upgrade BEMS.
2	Verify the prerequisites.
3	Upgrade the BEMS schema.
4	Upgrade the BEMS software.

Steps to upgrade BEMS and change the instant messaging service

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

Step	Action
1	Upgrade the BEMS software.

Step	Action
2	Stop the Good Technology Connect service and Good Technology Presence service.
3	Remove the Connect and Presence services.
4	Uninstall the current Microsoft Unified Communications Managed API and install Microsoft Unified Communications Managed API 5.0.
5	Add the Connect and Presence services.
6	Remove BEMS from the trusted server entry records and trusted application pool.
7	Create a trusted pool application for BEMS on the computer that hosts Skype for Business.
8	If the trusted application pool FQDN changed, issue a new certificate to the host server.
9	Configure the services. • Connect service • Presence service
10	Start the Good Technology Connect service and Good Technology Presence service.

Prerequisites: Installing and configuring BEMS

4

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
- Global Catalog for BlackBerry Connect and BlackBerry Presence
- BlackBerry Docs requirements
- BlackBerry Directory Lookup requirements
- Good 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 Dynamics 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 the your environment and the computer hosting BEMS meet the following system and network requirements.

Item	Requirement
Software	Verify that you have Java 8 (latest update version) on the computer that hosts BEMS.

Item	Requirement
Operating system	Verify that the computer hosting BEMS is running an operating system that supports BEMS. For more information about the supported operating systems, see the BEMS Compatibility Matrix.
Supported Browsers	Verify that you have a supported browser on the computers that host the BEMS Dashboard and the Docs console
Administration rights	• User performing the installation must have local administrative privileges on the host machine • BEMS must be able to connect with Microsoft Exchange for PNS • BEMS must be in the same domain as the Microsoft Lync Server for Connect • BEMS must be able to communicate with the enterprise's Microsoft Active Directory • BEMS must have "logon as a service" right • Disable antivirus software before you install or upgrade the BEMS software • Exclude the BEMS directory from virus scanning • Local Windows firewall must be disabled **Important:** A Group Firewall Policy will cause the installer to fail its prerequisite checks, even if the local firewall is disabled.
Inbound TCP Ports	The following ports must be open and ready for BEMS and not blocked by any firewall: • 8080 from the Good Proxy server; or 8082, if SSL is required for inbound Good Proxy communications • 8443 from the Good Proxy server for Push Notifications, Presence, and Docs; from Microsoft Office Web Apps server for Docs • 49555 from the Microsoft Lync Server or Skype for Business for the Connect service • 49777 from the Microsoft Lync Server or Skype for Business for the Presence service • 61616 TCP port to and from BEMS machines in the same cluster (bidirectional) • 61617 TCP (SSL) to and from BEMS machines in the same cluster (bidirectional) **Important:** 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).
Outbound TCP Ports	The following ports must be open and ready for BEMS and not blocked by any firewall:

Item	Requirement
	• 443 to BlackBerry Dynamics NOC (gdweb.good.com) • 443 to Microsoft Exchange • 443 to Firebase Cloud Messaging (FCM) (for Android Push Notification) • 443 or 80 to Microsoft SharePoint • 443 to Microsoft Office Web Apps Server (OWAS) • 5061 to the Microsoft Lync Server or Skype for Business server • 17080 to the Good Proxy server • 17433 to the Good Proxy server[2] • 1433 to the Microsoft SQL Server (default) • 1434 UDP to the Microsoft LyncLync database (for initial setup only) • 8443 to the Presence Web Service (CIMP server) • 5222 to the Presence Web Service (CIMP server) • 49152 – 57500 TCP: Random port in this range to the Lync database (for initial setup only) • 61616 TCP port to and from BEMS machines in the same cluster (bidirectional) • 61617 TCP (SSL) to and from BEMS machines in the same cluster (bidirectional) **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.
Internal ports	The following ports are used by BEMS: • 8080, 8082 for use by the BlackBerry Connect service • 8101 for SSH connectivity to BEMS • 8443 for Push Notifications and Presence • 8099 for use by the .NET Component Manager • 8060 for use by the Lync Presence Provider (LPP)
TCP/IP port access to the database	• 1433 to the Microsoft SQL Server default

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

[2] BEMS requires visibility of all Good Proxy servers (17080/17433), regardless of whether KCD is enabled or not, so that if one Good Proxy fails, BEMS can communicate with the next Good Proxy in the cluster for authentication tokens, etc.

Setting up a Windows service account for BEMS

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

Important: If you 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.

Database requirements

Make sure that your environment is running a supported version of database server.

Allow SQL Server 2008 R2 Express with Tools to accept remote connections

1. Login to the database server through **Remote Desktop Connections**.
2. Click **Start** > **All Programs** > **Microsoft SQL Server** <***version***> > **Configuration Tools** > **SQL Server Configuration Manager**.
3. Expand **SQL Server Network Configuration**.
4. Double-click **Protocols for SQL**<***Version***>.
5. Right-click **TCP/IP** > **Properties**.
6. Click the **IP Addresses** tab.
7. Under **IPAll**, verify the following settings:
    - **TCP Dynamic Ports** field is blank.
    - **TCP Port** is set to 1433.
8. Click **OK**.

BlackBerry Dynamics requirements

The following minimum BlackBerry Dynamics server versions should be appropriately installed and configured according to the instructions in the Good Control/Good Proxy Servers Installation Guide.

- Good Control server 3.0.56.79 or later
- Good Proxy server 3.0.56.32 or later

Important: Your BlackBerry Dynamics servers must be operating before you install BEMS.

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.

Set the `JAVA_HOME` system environment variable

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*>.
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.

- Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business requirements
- Database requirements
- Prepare the Lync Topology for Connect
- SSL certificate requirements for Microsoft Lync Server or Skype for Business
- Global Catalog for Connect and Presence

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. If you're not using Microsoft Lync Server or Skype for Business, planned deployments of the Push Notifications service on a computer running Windows Server 2008 R2 requires that you install Microsoft .NET Framework 4.5.

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 2008, complete the following steps:
        1. Download Windows Management Framework 3.0. To download the file, visit www.microsoft.com/download and search for ID=34595.
        2. Select the **Windows6.1-KB2506143-x64.msu** checkbox. Complete the instructions on the screen.
        3. Open Windows PowerShell and run the following script: **Set-ExecutionPolicy -Scope CurrentUser RemoteSigned**.
2. Install and enable Microsoft .NET Framework 4.5
    - 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**.
    - On a computer that is running Windows Server 2008, both Microsoft .NET Framework 3.5 SP1 and Microsoft .NET Framework 4.5 are required. Complete the following steps:
        1. In Windows Server Manager, enable Microsoft .NET Framework 3.5 SP1
        2. Double-click **dotNetFx35.exe**. Complete the instructions on the screen.
        3. Download Microsoft .NET Framework 4.5. To download the file, visit www.microsoft.com/download and search for ID=30653.

4. Double-click **dotNetFx45_Full_setup.exe**. Complete the instructions on the screen.

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**.
   - If you install BEMS on a computer that is running Windows Server 2008, install **Desktop Experience**. 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 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 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\5.0.8308.0\Setup\
6. If you enable persistent chat in a Skype for Business environment, download 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 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.

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. To establish trust with the Microsoft Lync Server and Skype for Business, you must use the Management Shell to complete the following:

1. If necessary, remove the existing provisioning of BEMS as a trusted application and trusted application pool. For example, when you change the instant messaging server from Microsoft Lync Server to Skype for Business.
2. Create a trusted application pool by preparing the initial computer hosting BEMS.
3. Designate trusted applications for the use of the BEMS computer.
4. Create a trusted-computer entry for every BEMS in the environment.
5. Publish these changes to the Microsoft Lync Server and Skype for Business topology.
6. Create a Trusted Endpoint for the Presence service.

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.

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.

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***>.

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.

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

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 disastery 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.

SSL certificate requirements for Microsoft Lync Server 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 (MTLS1) 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 2010 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*>\Trusted Root Certification Authorities\Certificates folder.
- The Subject Name (SN) of the certificate must contain the Common Name (CN) for BEMS's fully qualified domain name (FQDN), such that CN=server.subdomain.domain.tld.
- The Subject Alternative Name (SAN) must contain the DNS for the trusted pool for the BEMS machine, as well as the BEMS machine FQDN. SANs let you protect multiple host names with a single SSL certificate.
- 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.

e. Click **Add** >.

15. Click **Apply**.
16. Click **OK**.
17. Click **Enroll**.
18. Click **Finish**.

After you finish: Grant the service account read access to the certificate.

1. Right-click the certificate, and click **All Tasks** > **Manage Private Keys**.
2. On the **Security** tab, add the service account.

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 via a callback address. Push notifications are ideally suited for tightly coupled clients like BlackBerry Work and other BEMS supported apps to which the server has reliable access and the client is IP addressable. When the BlackBerry Push Notifications service is configured, Microsoft Exchange Web Services events are sent asynchronously from the mailbox server to the client.

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 goodpkb.force.com/PublicKnowledgeBase to read article 40155.

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

- Configuring 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 2007

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 requred, 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.
2. Type **nltest /dsgetdc:mydomain.com**. Press **Enter**.

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

For information on how to check the internal URL on a CAS server, visit http://support.blackberry.com/kb 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. If you are not familiar with how to create a mailbox on Microsoft Exchange Server, 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.

Execute the following Microsoft Exchange Management Shell command to apply Application Impersonation permissions to the BEMSAdmin service account:

1. Open Microsoft Exchange Management Shell.
2. Type **New-ManagementRoleAssignment -Name:<*ImpersonationAssignmentName*> -Role:ApplicationImpersonation -User:<*ServiceAccount*>**. For example, **New-ManagementRoleAssignment -Name:BlackBerryAppImpersonation -Role:ApplicationImpersonation -User:BlackBerryAdmin**.

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 http://support.blackberry.com/kb 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 BEMSDB.

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, you should check 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.

Presence prerequisites: Microsoft Lync Server and Skype for Business

For Microsoft Lync Server and Skype for Business, the Presence service has the same predeployment requirements as the Connect service. The Presence service, however, does not require an SQL database. Refer to the complete list of Connect prerequisites. If you want to configure Presence to use the Global Catalog for Connect and/or Presence, you need to perform the following steps. Note that Presence is supported in Microsoft Lync Server, Skype for Business, and Cisco Jabber environments.

1. On the computer that hosts Presence, navigate to the **LyncPresenceProviderService.exe.config** file. By default, the LyncPresenceProviderService.exe.config file is located <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Presence folder.
2. In the <appSettings> section of the file, locate the following values and update them as required:

- <addkey = "AD_USERS_SOURCE" value= "LDAP" />
- <addkey = "AD_USERS_SOURCE_DOMAIN" value="" />

3. If the Good Technology Presence service is running, restart the service.

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 and cup-xmpp 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 and cup-xmpp certificates. The Cisco Tomcat service runs on both CUCM and CIMP servers. The cup and cup-xmpp 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:

Service	Certificates or CSRs
Configure the Connect service only[1]	• Enterprise Root CA certificate • Tomcat Certificate Signing Request (from CUCM) • Tomcat - CA signed certificate • Cup-xmpp Certificate Signing Request (from CIMP) • Cup-xmpp CA signed certificate
Configure the Presence service only[1]	• Enterprise Root CA certificate • Tomcat Certificate Signing Request (from CUCM)

Service	Certificates or CSRs
	• Tomcat - CA signed certificate • Cup Certificate Signing Request (from CIMP) • Cup - CA signed certificate

[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, and cup-xmpp/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, and cup-xmpp).

   a. Click **Upload Certificate/Certificate chain**.

   b. In the **Certficiate 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. Verify that the trust certificate type displays **CA-signed**.
6. Request a CSR.

   a. Click **Generate CSR**. The new CSR will overwrite the existing CSR for that certifcate.

   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 Certifciate request lines.

7. 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.

8. 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.

9. 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**.

10. 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 I – 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

The BlackBerry Directory Lookup service requires a database, and that you set up a Windows Service Account for BEMS in support of your Exchange environment.

The following pre-requisites are required unless they have been configured for another service, such as the BlackBerry Push Notifications service, in which case the service account, Microsoft Exchange environment settings, and Microsoft Exchange Web Services (EWS) database can be shared.

- Creating an Microsoft Exchange mailbox for the service account
- Granting application impersonation permissions to the service account
- Setting authentication for the EWS protocol
- Setting up Microsoft Exchange Autodiscover
- Setting up a SQL database

Prerequisites: Follow-Me service

BEMS Follow-Me service requires a database, and that you set up a Windows Service Account for BEMS in support of your Microsoft Exchange environment.

Note: The following pre-requisites are required unless they have been configured for PNS or another service, in which case the service account, Microsoft Exchange environment settings, and EWS database can be shared.

- Creating an Microsoft Exchange Mailbox for the service account
- Granting Application Impersonation permissions to the service account
- Setting Authentication for the EWS protocol
- Setting up Microsoft Exchange Autodiscover
- Setting up a SQL database

Prerequisites: Certificate Lookup Service

BEMS Certificate Lookup requires a database, and that you set up a Windows service account for BEMS in support of your Microsoft Exchange Server environment.

Note: The following pre-requisites are required unless they have been configured for Push Notifications service or another service, in which case the service account, Microsoft Exchange environment settings, and Microsoft Exchange Web Services (EWS) database can be shared.

- Creating an Exchange Mailbox for the service account
- Granting Application Impersonation permissions to the service account
- Setting Authentication for the Microsoft Exchange Web Services protocol
- Setting up Exchange Autodiscover
- Setting up a SQL database

Installing or upgrading the BEMS software

5

Install the BEMS software

Before you begin: If your organization uses AlwaysOn support for SQL Server 2012 or SQL Server 2014, make sure you complete the steps in Appendix J: AlwaysOn support for SQL Server 2012 and 2014 and 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.

1. Log in to the computer that you want to install BEMS on using the BEMS service account.
2. Copy the installation files to the computer.
3. Extract the content to a folder on the computer.
4. In the **GoodEnterpriseMobilityServer** installation folder, double-click **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**.
5. In the **GoodEnterpriseMobilityServer<*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:

Task	Steps
Specify the Microsoft SQL Server connection information for the BEMS-Core service database.	1. In the **Host** field, type the instance name of your SQL Server. If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener. 2. In the **Database name** field, type the name for the BEMS-Core database. For example, BEMSDB. • 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*>:<*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. 3. In the **Port** field, type the port number that connects to the SQL Server. 4. 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 service run.	1. In the **Login** field, type the BEMS service account login information (for example, <*domain123*>.example.com\<*BEMS service account username*>). 2. In the **Password** field, type the BEMS service account password. 3. Click **Next**.
Specify the SQL Server connection information for the BEMS-Connect service database.	1. In the **Host** field, type the instance name of your SQL Server. If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener. 2. In the **Database name** field, type the name for the BEMS-Connect database. For example, BEMS-Connect.

Task	Steps
	If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group. 3. In the **Port** field, type the port number that connects to the SQL Server. By default, this port is 1433 4. 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 service run. **Note:** A database is not created for the Presence service.	1. In the **Login** field, type the BEMS service account login information (for example, <*domain123*>.example.com\<*BEMS service account username*>). 2. In the **Password** field, type the BEMS service account password. 3. Click **Next**.
Specify the SQL Server connection information for the BEMS-Docs service database.	1. In the **Host** field, type the instance name of your SQL Server. If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener. 2. In the **Database name** field, type the name for the BEMS Connect database. For example, BEMS-Docs. If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group. 3. In the **Port** field, type the port number that connects to the Microsoft SQL Server. 4. Optionally, in the **Additional Properties** field, specify any connection properties. For example, name1=value1; name2=value2, and so on. For more information, see Setting the connection properties. If your environment uses AlwaysOn with multi-subnet deployment, type **MultiSubnetFailover=true**. 5. By default, the setup application uses SQL Server authentication to connect to the BEMS database. Select **Windows Authentication**. Click **Next**.

15. In the **Install Services** dialog box.
16. In the **Replace JCE Policy** dialog box, click **Next**.

17. In the **Pre-installation Summary** dialog box, click **Install** to install BEMS.
18. In the **Installing** dialog box, complete 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.
19. Optionally, in the **Installing, Upload Credentials** dialog box, you can provide your BlackBerry Online Portal credentials and cluster name. You can skip this screen and configure this information later in the BEMS Dashboard.
20. 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.

Upgrading the schema for BEMS

It is recommended that you upgrade the BEMS Core and Mail services schema before you upgrade the BEMS software in clustered environments. Complete one of the following schema upgrade tasks:

- Option 1: Large environments
- Option 2: Small environments

Option 1: Upgrade the schema for BEMS

1. Back up the BEMS Core database.
2. Stop the Good Technology Common Services on each computer that hosts GEMS 2.2 or earlier, except for the BEMS you are upgrading.
3. Complete the instructions in Upgrade BEMS.
4. Start the Good Technology Common Services on each computer that hosts BEMS.
5. Upgrade each BEMS instance in your environment.

Option 2: Upgrade the schema for BEMS

1. Back up the BEMS Core database.

2. Stop the Good Technology Common Services on each computer in the cluster that hosts GEMS.
3. On one of the computers that hosts GEMS, download the **GoodEnterpriseMobilityServer.<*version*>. zip** installation files.
4. Extract the contents to a folder on the computer.
5. In a command prompt (run as administrator), navigate to the **dbmanager<*version*>with dependencies.jar** file. By default, the dbmanager file is located in <*drive*>:\GoodEnterpriseMobilityServer\DBManager. Complete the following tasks:

Task	Description
Update the GEMS Core database schema.	• If you use Microsoft SQL Server authentication to access the Core database, type **java -jar dbmanager-<*version*>-jar-with-dependencies.jar -moduleName jsonstore - dbType sqlserver -action upgrade -dbHost "HOSTNAME" -dbName "DATABASENAME" - dbPort "" -integratedAuth false -userName "USERNAME" - password "PASSWORD"** ◦ Where *version* is the version of the dbmanager jar file. ◦ Where *hostname* is the the name of the computer hosting the Core database. If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener. ◦ Where *databasename* is the name of the Core database. For example, BEMSDB. If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group. ◦ Where *username* is the BEMS service account name. ◦ Where *password* is the password for the the service account. • If you use Windows authentication to access the Core database, type **java -jar dbmanager-<*version*>-jar-with-dependencies.jar - moduleName jsonstore - dbType sqlserver -action upgrade -dbHost "HOSTNAME" -dbName "DATABASENAME" - dbPort "" - integratedAuth true**. ◦ Where *version* is the version of the dbmanager jar file. ◦ Where *hostname* is the the name of the computer hosting the Core database. If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener. ◦ Where *databasename* is the name of the Core database. For example, BEMSDB. If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group.

Task	Description
Update the GEMS Mail database schema.	• If you use Microsoft SQL Server authentication to access the Mail database, type **java -jar dbmanager-<*version*>-jar-with-dependencies.jar -moduleName pushnotify - dbType sqlserver -action upgrade -dbHost "HOSTNAME" -dbName "DATABASENAME" - dbPort "" -integratedAuth false -userName "USERNAME" -password "PASSWORD"** Where *version* is the version of the dbmanager jar file. ◦ Where *hostname* is the the name of the computer hosting the Mail database. If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener. ◦ Where *databasename* is the name of the Mail database. For example, BEMSDB. If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group. ◦ Where *username* is the BEMS service account name. ◦ Where *password* is the password for the the service account. • If you use Windows authentication to access the Mail database, type **java -jar dbmanager-<*version*>-jar-with-dependencies.jar -moduleName pushnotify - dbType sqlserver -action upgrade -dbHost "HOSTNAME" -dbName "DATABASENAME" - dbPort "" -integratedAuth true**. ◦ Where *version* is the version of the dbmanager jar file. ◦ Where *hostname* is the the name of the computer hosting the Mail database. If your environment uses AlwaysOn enter the FQDN of the AlwaysOn Listener. Where *databasename* is the name of the Mail database. If your environment uses AlwaysOn enter the name of the database that is added to the AlwaysOn Availability Group.

6. Start the Good Technology Common Services on each computer in the cluster that hosts BEMS.

After you finish: Upgrade the BEMS software.

Perform a Silent Install or Upgrade

You can perform a silent new installation or upgrade.

In a command prompt, type <***BEMS Installer***> **-i silent -f** <***response file***>

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.

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\).

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.

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.

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 BlackBerry 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, double-click **GoodEnterpriseMobilityServer.**<***version number***>**.exe**. If a Windows message appears and requests permission for **InstallAnywhere Self-Extractor** to make changes to the computer, click **Yes**.
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**. Click **Next**.
7. In the **Services** dialog box, click **Next**
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 continue with the installation.

9. 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.

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, complete the following actions:
    a. Type the username of the BEMS service account.
    b. Type the password for the BEMS service account.
    c. Type the domain.
14. Click **Next**.
15. In the **Database Information** dialog box, complete the following actions:
    a. Type the password for the user account that is used for the BEMS-Core service database to connect to the SQL Server. Click **Next**.
    b. Type the password for the service account under which the BEMS-Connect service database runs. Click **Next**.
    c. Type the password for the service account under which the BEMS-Presence service database runs. Click **Next**.
    d. Enter the information for the BEMS Docs service database to connect to the SQL Server. If your environment uses AlwaysOn with multi-subnet deployment, in the **Additional Properties** field, type **MultiSubnetFailover=true**. Click **Next**.
16. In the **Install Services** dialog box, type the password for the service account under which BEMS-Presence service runs. Click **Next**.
17. In the **Database Information** dialog box, type the password for the BEMS-Docs service database to connect to the SQL Server. Click **Next**.
18. In the **Replace JCE Policy** dialog box, click **Next**.
19. In the **Pre-installation Summary** dialog box, click **Install** to install BEMS.
20. In the **Installing** 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.

21. Select **Yes** or **No** when you are prompted to make the upgraded BEMS the master configuration for the cluster.
22. In the **Install Complete** dialog box, verify that the **Start BEMS services** checkbox is selected. Click **Done**.

    If you clear the **Start BEMS services** checkbox, the BEMS installer stops the BlackBerry Common Services.

The setup application opens the BEMS Dashboard at https://localhost:8443/dashboard.

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.

Configuring BEMS Core

5

When you configure BEMS-Core, you perform the following actions:

1. Configure the BlackBerry Dynamics server in BEMS
2. Add dashboard administrators
3. Optional, enable log file compression
4. Install the BEMS SSL certificate
5. Install CA certificates

Configure the BlackBerry Dynamics server in BEMS

Your BEMS environment must be configured to trust the Root CA for the Good Proxy HTTPS configuration or implement the Karaf workaround. For instructions, see Importing and configuring certificates.

Before you begin: BlackBerry Dynamics servers must be operating before the Docs service can be configured for BlackBerry Dynamics.

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

Task	Steps
If a Good Proxy server is not defined	1. Click **Add BlackBerry Proxy**. 2. In the **Host Name** field, type the Good Proxy server host name. 3. In the **Protocol** drop-down list, select the protocol used to communicate with the Good Proxy server. • If you select HTTPS, the **Port** field prepopulates to 17433. • If you select HTTP, the **Port** field prepopulates to 17080. 4. Click **Test** to test the connection.

Task	Steps
	5. Repeat steps 1 to 4 to add additional Good Proxy servers for redundancy continuity.
If one or more Good Proxy servers are defined	No action is required. Previously defined Good Proxy servers are listed.

4. Select the **Apply to other nodes in the BEMS cluster** check box to communicate the Good Proxy server information to all of the BEMS nodes in the cluster.
5. Optionally, select the **Enforce the SLL Certificate validation when communicating with BlackBerry Dynamics** check box when you use the https protocol to communicate with the BlackBerry Dynamics server.
6. Click **Save**.

Add dashboard administrators

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

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **BEMS Configuration**.
2. Click **Dashboard Administrators**.
3. Click **Add Group**.
4. In the **Active Directory Security Group** field, type the name of the Microsoft Active Directory security group.
5. Click **Save**.
6. Repeat steps 3 to 5 to add additional security groups.

Enable log file compression

You can compress the log files that are generated and saved in the default log folder or folder you specified during the installation of BEMS. Currently, log files are generated and rotated when they reach 100 MB in size. When you enable log compression, log files can be larger than 100 MB. When a log file exceeds 100 MB, it is compressed and saved to the appropriate log file folder. By default, log file compression is disabled.

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

2. Click log **Log Settings**.
3. Select the **Enable Log Compression**.
4. Click **Save**.

Importing CA Certificates for BEMS

By default, BEMS is only aware of public CA certificates. If BEMS must communicate with a server that does not have a public CA certificate, then you must import the non-public CA certificate into the BEMS host Java keystore. BEMS may connect to the following servers in your environment:

- Microsoft Exchange Server
- Active Directory Federation Service (ADFS)
- Good Proxy
- Microsoft SharePoint
- Microsoft Office Web Apps

Import non-public certificates to BEMS

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

    Verify the JAVA_HOME System variable is set to the correct Java bin directory. For instructions about setting the JAVA_HOME system variable, see Configure the Java Runtime Environment.
2. Obtain a copy of the non-public CA certificate from the server that BEMS must communiate with. For more information, contact your administrator of your Microsoft Exchange Server, Good Proxy, or Microsoft SharePoint servers.
3. On the BEMS host, make a backup of the Java keystore file. By default, the Java keystore file is located at %JAVA_HOME% \lib\security\cacerts, where JAVA_HOME is confirmed in step 1.
4. Copy the non-public CA certificate to the Java keystore directory in step 3.
5. Open a command prompt and change directory to the Java keystore directory in step 3.
6. Type the following command to import the non-public CA certificate into the Java keystore: **keytool -importcert -trustcacerts -alias <*your_cert_alias*> -file <*your_cert*>.cer -keystore cacerts -storepass changeit**
    - Where *your_cert_alias* is the unique name that you are assigning the certificate in the cacerts file. This alias cannot already exist in the cacerts file.

- Where *your_cert* is the file name of the non-public certificate. If this is the path to the file, add quotation marks (" ") around the full path, filename, and extension.

7. Repeat Steps 2 to 6 for each non-public CA certificate.
8. In the Windows Service Manager, restart the Good Technology Common Services service.

Importing and configuring certificates

Consider the following when you import certificates:

- Import a new SSL certificate, if you want to replace the BEMS auto-generated SSL certificate.

Replacing the auto-generated SSL certificate

By default, BEMS is remotely accessible using HTTPS only. During installation, a BEMS Java keystore called gems.jks created and located in <*drive*>\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<*version*>\etc\keystores\. If you previously created a self-signed certificate, then your existing certificate and certificate password are retained.

The default password for the gems.jks keystore is "changeit."

When you replace the auto-generated SSL certificate, you perform the following actions:

1. Create a new keystore, generate a CSR request, and obtain a signed certificate from a CA.
2. Move the certificate into the BEMS keystore.
3. Update the certificate passwords in BEMS.

Note: The browser will report that your SSL certificate is untrusted because it is a self-signed certificate.

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

1. On the computer that hosts BEMS, create a folder (for example, C:\bemscert).
2. Create a new Java keystore and key pair.
   a. Open a command prompt.
   b. Navigate to the folder that you created in step 1.
   c. Type **keytool -genkeypair -alias serverkey -keyalg RSA -keystore bemsnew.jks -keysize 2048 -dname "CN=<*FQDN of BEMS host*>, OU=<*BEMS name*>, O=<*domain*>, L=<*location*>, S=<*state or province*>, C=<*country*>" -validity <*number of days before the certificate expires*> -storepass <*mystorepassword*>**.

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

For more information about keystore commands, see Keystore commands.

d. Press **Enter**.

e. Type a password for the serverkey certificate's private key. To set the serverkey password to be the same as the keystore password, press **Enter**.

f. Optionally, to view the contents of the certificate before you submit it to a CA, type **keytool -list -v -keystore bemsnew.jks -storepass <*mystorepassword*>**

3. Generate a CSR for the BEMS Java keystore. In the command prompt, type **keytool -certreq -alias serverkey -file bemsnewcert.csr -keystore bemsnew.jks -storepass <*mystorepassword*> -keypass <*mykeypassword*>**

   If the serverkey password and the keystore password are the same, type **keytool -certreq -alias serverkey -file bemsnewcert.csr -keystore bemsnew.jks -storepass <*mystorepassword*> -keypass <*mystorepassword*>**

4. Submit the CSR to a CA.

5. Receive the CA-signed certificate from the CA and save it to the folder that you created in step 1.

6. Import the CA-signed certificate to the request. In the command prompt, type **keytool -importcert -keystore bemsnew.jks -storepass <*mystorepassword*> -file <"*certificate filename received in step 5*"> -alias serverkey**

   For example, **keytool -importcert -keystore bemsnew.jks -storepass mystorepassword -file "bemsnew certnew.cer" -alias serverkey**

7. Optionally, to view the new contents of the keystore, type **keytool -list -v -keystore bemsnew.jks -storepass <*mystorepassword*>**

Move the certificate into the BEMS keystore

The Java keytool is used to import the certificate into the Java keystore. The default location of this tool on the BEMS host is %JAVA_HOME%\bin. For example, C:\Program Files\Java\jre1.8.0_<*version*>\bin.

Complete one of the following tasks:

If the keystore filename is	Task
not gems.jks	Copy the new keystore file, bemsnew.jks, from C:\bemscert to <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution \gems-quickstart-<*version*>\etc\keystores.
gems.jks	Copy the keystore file, gems.jks, from C:\bemscert to <*drive*>:\Program Files \BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<*version*>\etc\keystores

If the keystore filename is	Task
	1. Stop the Good Technology Common Services service from the Windows Service Manager. 2. Navigate to <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<*version*>\etc\keystores. 3. Rename the gems.jks file to gems_bak.jks. 4. Copy the gems.jks file from C:\bemscert to <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<*version*>\etc\keystores.

After you finish: Update the certificate passwords in BEMS

Update the certificate passwords in BEMS

For BEMS to access your certificate private key, you must include the challenge password in the jetty.xml file. The password must be obfuscated. This can be done with the BEMS SSL Tech Tool. For instructions, visit support.blackberry.com/kb to read article 41823.

Before you begin: On the computer that hosts BEMS, download the BEMS Tech Tools and extract the sslcert folder.You can download the BEMS Tech Tools here.

1. Generate the obfuscated challenge password for your serverkey certificate private key and keystore password.

   Note: When you run the BEMS SSL Tech Tool to obfuscate the password, the BEMS SSL Tech Tool generates a new gems.jks file. You can then delete the gems.jks file that the tool generates. The BEMS SSL Tech Tool also generates a log file, SelfSignCertificate.log.0, for review. This file contains the same information as the screen outputs.

   a. In a command prompt, navigate to the extracted sslcert utility folder.

   b. Type **sslcert.bat** <***mykeypassword***> <***mystorepassword***> <***fqdn of BEMS host***>

      For example: **sslcert.bat mykeypassword mystorepassword bemshost.example.com**

   c. Copy the screen outputs to a text file for later reference.

2. Backup the jetty.xml file. By default the jetty.xml file is located at <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<*version*>\etc.

3. Update the **keyStore**, **trustStore**, **keyStorePassword**, **trustStorePassword**, and **keyManagerPassword** in the jetty.xml file with the obfuscated password. For examples, see Jetty.xml file reference.

   a. In a text editor, open the jetty.xml file.

   b. Locate the <Call name="addConnector"> section.

      Note: Make sure you locate the Call name tag that is not commented out.

c. If the new keystore filename has changed from the default gems.jks to bemsnew.jks, locate <Set name="keyStore"> and <Set name="trustStore"> elements and update them as required.

d. Locate the <Set name="keyStorePassword"> and <Set name="trustStorePassword"> elements and update them with the obfuscated passwords from the sslcert text outputs, Key Store Password and Trust Store Password, respectively. The text outputs are the obfuscated values of the keystore password, referenced as <*mystorepassword*> in step 1b.

e. Locate the <Set name="keyManagerPassword"> element and update it with the new obfuscated password from the sslcert text output, Key Manager Password. The text output is the obfuscated value of the keypass password, referenced as <*mykeypassword*> in step 1b.

4. Restart the Good Technology Common Services service from the Windows Service Manager.

5. Test the new certificate by accessing the BEMS Dashboard in a browser. Its certificate information now reflects the newly imported certificated.

Jetty.xml file reference

The keystore file is referenced in jetty.xml. Its default location of the jetty.xml file is on the computer hosting BEMS at <*BEMS Machine Path*>\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<*version*>\etc\

The relevant snippet from jetty.xml referencing the location of the keystore file and its associated password would look like the following:

```
<Call name="addConnector">
<Arg>
<New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
<Arg>
<New class="org.eclipse.jetty.http.ssl.SslContextFactory">
<Set name="keyStore"><SystemProperty default="." name="jetty.home"/>/etc/keystores/
gems.jks</Set>
<Set name="trustStore"><SystemProperty default="." name="jetty.home"/>/etc/keystores/
gems.jks</Set>
<Set name="keyStorePassword">OBF:1vn21ugu1saj1v9i1v941sar1ugw1vo0</Set>
<Set name="keyManagerPassword">OBF:1uh01xmu1k8k1juc1k5m1wg21kmk1w</Set>
<Set name="trustStorePassword">OBF:1vn21ugu1saj1v9i1v941sar1ugw1vo0</Set>
</New>
</Arg>
<Set name="port">8443</Set>
<Set name="maxIdleTime">30000</Set>
</New>
</Arg>
</Call>
```

The passwords are obfuscated. The keyStorePassword and the trustStorePassword are typically identical and represent the Java keystore password. The keyManagerPassword is the challenge password for the certificate.

Certificate format

Any certificate used should be PKCS #12 and the private key must contain a challenge password. In addition, make sure that the certificate has the appropriate key chain. For example, the root and intermediate certificate.

Configuring HTTPS for BEMS to Good Proxy

By default, the Java keystore on the computer that hosts BEMS does not contain the CA certificate for the Good Proxy server. The Good Proxy server uses a certificate that is signed by Good Control CA, a private Certificate Authority. This means the BEMS cannot verify the Good Proxy server's SSL certificate; and, therefore, any HTTPS connection made from BEMS to the Good Proxy server fails.

The Good Proxy CA certificate is in a Java keystore on the Good Control server. The default location of this file is C:\Program Files (x86)\Good Technology\Good Control\jre\lib\security\cacerts.

Among the many certificates in this keystore is one with the alias "gdca". Export this certificate and import it into the BEMS Java keystore. The default password for the keystore is changeit.

Import the required certificate into the Java keystore on BEMS

1. Verify the Java directory is specified in the environment PATH. For instructions, see Configure the Java Runtime Environment. If necessary, confirm the version of Java that BEMS is using by complete the following steps:
   a. In a command prompt, type **set | findstr "JAVA_HOME"**.
   b. Press **Enter**.

   Verify the JAVA_HOME system variable is set to the correct Java bin directory.
2. Copy the Good Control Java keystore from C:\Program Files (x86)\Good Technology\Good Control\jre\lib\security\cacerts to the computer that hosts BEMS and place it in a convenient location. For example, C:\gemscert.
3. Rename the file. For example, cacerts.gdca. The name is arbitrary.
4. Open a command prompt and navigate to C:\gemscert.
5. Export the Good Control CA certificate. In a command prompt, type **keytool -exportcert -alias gdca -file gdca.cer -keystore cacerts -storepass changeit**
6. On the computer that hosts BEMS, make a backup of the Java keystore file. The default location of the Java keystore is C:\Program Files\Java\jre1.8.0_<*version*>\lib\security\cacerts.
7. Copy the Java keystore file to C:\gemscert.
8. Import the Good Control CA certificate into the BEMS Java keystore. Type **keytool -importcert -trustcacerts -alias gdca -file gdca.cer -keystore cacerts -storepass changeit**
9. Copy the updated keystore file to its original Java keystore location. See step 7.
10. Restart the Good Technology Common Services from the Windows Service Manager.

Download certificates from the Cisco Unified Communications Manager and Cisco IM and Presence servers into the BEMS Java keystore

You must import the following certificates from the Cisco Unified Communications Manager (CUCM) and Cisco IM and Presence (CIMP) servers. For multi-server certificates, only one certificate per cluster must be imported. If the certificate is not a multi-server certificate, a copy must be downloaded from each CUCM and CIMP server in a cluster and imported separately.

- Tomcat.der
    - If your environment uses a multi-server certificate, a single copy of the certificate downloaded from the CUCM Publisher and CIMP Publisher servers is required.
    - If your environment does not use a multi-server certificate, a copy of the certificate downloaded from each CUCM and CIMP node is required.
- Cup.der
    - A copy of the certificate downloaded from each CIMP node is required.
- Cup-xmpp.pem
    - If using a multi-server certificate, a single copy of the certificate downloaded from the CIMP Publisher is required.
    - If not using a multi-server certificate, a copy of the certificate downloaded from each CIMP node is required.

1. Log on to the appropriate CUCM server.
2. In the top-right **Navigation** drop-down list, click **Cisco Unified OS Administration**.
3. Click **Security** > **Certificate Management**.
4. Download the certificate named tomcat as a .der file.
5. Log on to the appropriate CIMP server.
6. In the top-right **Navigation** drop-down list, click **Cisco Unified IM and Presence OS Administration**.
7. Click **Security** > **Certificate Management**.
8. Download the cup-xmpp certificate as .pem file.
9. Download the cup certificate as .der file.

After you finish: Import these certificates into the BEMS Java keystore. For instructions, see Import third-party server certificates into the BEMS Java keystore

Import third-party server certificates into the BEMS Java keystore

If your environment enforces the use of SSL certificate validation when BEMS communicates with the Microsoft Exchange Server, LDAP server or other third-party server, you must export the certificate and import it into the BEMS Java keystore.

Before you begin: The third-party server certificate is saved to your desktop.

1. Open a command prompt.
2. Import the third-party server certificate chain that you saved to your desktop. Type **keytool -importcert -trustcacerts -alias <*your_server_cert_alias*> -file <*your_cert*>.cer -keystore <*drive*>:\Program Files\Java\jre<*version*>\lib\security\cacerts**.
3. Restart the Good Technology Common Services from the Windows Service Manager.

Keystore commands

The following table lists the keystore commands that are available at the command line. For more information about using the Java keytool, visit docs.oracle.com/javase/8/docs/technotes/tools/windows/keytool.html.

Action	Command
Check which certificates are currently in the keystore	**keytool -list -v -keystore <*keystore file*>**
Export a list of the certificates that are currently in the keystore	**keytool.exe -list -v -keystore lib\security\cacerts > c:\bemscert\cacertsoutput.txt**
Export a certificate from the keystore	**keytool -exportcert -alias <*alias_name*> -file <*file_name*>.crt -keystore <*keystore file*>**
Check a standalone certificate	**keytool -printcert -v -file <*filename*>.crt**
Delete a certificate from the keystore	**keytool -delete -alias <*alias_name*> -keystore <*keystore file*>**
Import a signed primary certificate to an existing BEMS Java keystore	**keytool -importcert -trustcacerts -alias <*alias_name*> -file <*file_name*>.crt -keystore <*keystore file*>**
Import a certificate into BEMSJava keystore	**keytool -importcert -trustcacerts -alias <*cert_alias_name*> -file <*your_cert*>.cer -keystore "<*drive*>:\Program Files\Java\jre1.8.0_<*version*>\lib\security\cacerts"**

Uploading BEMS log and statistical information

The BEMS Dashboard provides several aids for collecting troubleshooting data.

Troubleshooting aid	Description
Log Upload Credentials	Enter your username and password that you use to log on to the BlackBerry Online Portal. **Note:** These credentials are not stored, and are only used to ensure that this BEMS is authorized for log uploads.
Upload Logs	Use this tool to send logs directly to BlackBerry Support. Mail and Docs services logs are supported. **Note:** When you specify the date range, the time zone displayed is that of the BEMS server and the dates selected are used in reference to that time zone.
Upload BEMS statistics	Use this tool to send BEMS statistics to the BlackBerry Infrastructure and BlackBerry Dynamics NOC periodically. By default, uploading diagnostic information is disabled.

Specify log upload credentials

Before you begin: Make sure you have the login credentials you use to access the BlackBerry Online Portal. These credentials are not stored, they are used to verify that the BEMS server is authorized for log uploads to BlackBerry technical support for review. This page is prepopulated if you configured the Upload Credentials screen during the installation of the BEMS software.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **Troubleshootimg**.
2. Click **Log Upload Credentials**.
3. In the **BlackBerry Online Portal Username** field, type the username that you use to access the Online Portal.
4. In the **BlackBerry Online Portal Password** field, type the password that you use to access the BlackBerry Online Portal.
5. Click **Test**.
6. Click **Save**.

Upload log files

You can upload log files for the Mail service and Docs service.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **Troubleshooting**.
2. Click **Upload Logs**.
3. Specify a date range for the logs to include.
   The time zone displayed is that of the BEMS server and the date range you specify is in reference to that time zone.

4. Click **Upload Logs**.

Enable upload of BEMS statistics

You can enable BEMS to send periodic diagnostic information to BlackBerry technical support. The statistical information might include the following information:

- Number of users assigned to the instance*
- Name of instance*
- Name of the cluster
- Version of BEMS
- List of instances*
- Feature set for instance*
- Feature set for cluster*
- Services installed, status of the instance*
- JVM Version
- Last restart time
- System bugs
- Operating system
- Schema version
- System health

* The Mail service must be installed for this information to be retrieved. This page is prepopulated if you configured the Upload Credentials screen during the installation of the BEMS software.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **Troubleshooting**.
2. Click **Upload BEMS statistics**.
3. Select the **Allow this BEMS server to send diagnostic information to BlackBerry Support** checkbox.
4. Type your cluster name and domain name. By default, the Upload Interval is 30 minutes.
5. Click **Save**.

Configuring BEMS services

6

You can configure one or more services and in any order based on your organization's requirements. When you configure the BEMS services, you configure one or more of the following:

- BlackBerry Push Notifications
- BlackBerry Connect
- BlackBerry Presence
- BlackBerry Docs
- BlackBerry Dynamics Launcher
- BlackBerry Certificate Lookup

Configuring the Push Notifications service

When you configure BEMS for Push Notifications support of the BlackBerry Work app, which includes mail, contacts, and calendar, you perform the following:

- Enable Microsoft Exchange ActiveSync (EAS)
- Configure the Mail service in the BEMS dashboard
- Configure Good Control
- Configure the Push Notifications service for high availability

Enabling Microsoft Exchange ActiveSync

Microsoft Exchange ActiveSync is a protocol designed for the synchronization of email, contacts, calendar, tasks, and notes from the messaging server to the BlackBerry Work app. BEMS does not participate in Exchange ActiveSync activity, but Exchange ActiveSync must be properly enabled for BEMS to support BlackBerry Work apps with the Push Notifications service.

When you deploy the BlackBerry Work app to your users, make sure that Exchange ActiveSync is enabled on port 443 and that connections are permitted to the Good Proxy server.

Note: By default, ActiveSync is enabled when you install the client access server (CAS) role on the computer that's running Microsoft Exchange Server 2010, Microsoft Exchange Server 2013, or Microsoft Exchange Server 2016.

For more information on Exchange ActiveSync and how it works with BlackBerry apps, see the Microsoft Exchange ActiveSync (EAS) Security Information and Guidance Guide.

Configuring Push Notifications service

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

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

1. Database
2. Microsoft Exchange Server
3. Web Proxy
4. Android Push Notifications
5. Stop Notifications
6. User Directory Lookup
7. Certificate Directory Lookup

Configure the SQL database for Push Notifications service

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Mail**.
2. Click **Database**.
3. In the **Server** field, type the Microsoft SQL Server host name and instance. For example, <*SQLServer_hostname*> \<*instance_name*>.
4. In the **Database** field, type the database name. For example, BEMSDB.

   If you are configuring the database for an AlwaysOn Availability Group, see Appendix J: AlwaysOn support for SQL Server 2012 and 2014.
5. In the **Windows Authentication** drop-down list, complete one of the following tasks:

Task	Steps
Windows Authentication	1. Select **Windows Authentication**. 2. Click **Test**.
SQL Server Login Authentication	1. Select **SQL Server Login**. 2. Enter the SQL Server username and password. 3. Click **Test**.

6. Click **Save**.
7. Restart the Good Technology Common Services in the Windows Services Manager.

Configure BEMS to communicate with the Microsoft Exchange Server

Before you begin: The service account has impersonation rights on the Microsoft Exchange Server.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Mail**.
2. Click **Microsoft Exchange**.
3. Under **Enter Service account details**, complete one of the following actions to allow BEMS to communicate with the Microsoft Exchange Server:
   - Select the **Use Windows Integrated Authentication** checkbox.
   - Enter the username and password for the service account.
4. Under the **Autodiscover and Exchange Options** section, complete one of the following actions:

Task	Steps
Override Autodiscover URL	If you select to override the autodiscover process, BEMS does not perform an autodiscover and uses the override URL to obtain user information from the Microsoft Exchange Server. 1. Select the **Override Autodiscover URL** checkbox. 2. In the **URL endpoint for all Autodiscover requests** field, type the autodiscover endpoint.
Autodiscover and Microsoft Exchange Server options	1. By default, the **Enable SCP record lookup** checkbox is selected. If you clear the checkbox, BEMS does not perform a Microsoft Active Directory lookup of Autodiscover URLs. 2. Optionally, you can select the **Use SSL connection when doing SCP lookup** checkbox to allow BEMS to communicate with the Microsoft Active Directory using SSL. If you enable this feature, you must import the Microsoft Active Directory certificate to each computer that hosts an instance of BEMS. 3. Optionally, select the **Enforce SSL Certificate validation when communicating with Microsoft Exchange and LDAP server** checkbox. 4. By default, the **Allow HTTP redirection and DNS SRV record** checkbox is selected. If you clear the checkbox, you disable HTTP Redirection and DNS SRV record lookups for retrieving the Autodiscover URL when discovering users for BlackBerry Work Push Notifications.

5. In the **End User Email Address** field, type an email address to test connectivity to the Microsoft Exchange Server using the service account.

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

6. Click **Save**.

Troubleshooting the Push Notifications database

BEMS cannot connect to the Push Notifications database

Possible cause

The Microsoft Exchange configuration information was applied before the Database information.

Possible solution

1. Restart the Good Technology Common Services.
2. Verify the Database information. For instructions, see Configure the SQL database for Push Notifications service
3. Repopulate the Microsoft Exchange Server information. For instructions, see Configure BEMS to communicate with the Microsoft Exchange Server

Configure a web proxy server for the Push Notifications service

Because APNS pushes are sent using the BlackBerry Dynamics NOC, which resides outside of your enterprise network, a proxy server might be required to access the BlackBerry Dynamics NOC.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings** click **BEMS Configuration**.
2. Click **Web Proxy**.
3. Select the **Use Web Proxy** checkbox.
4. In the **Proxy Address** field, enter the FQDN of the web proxy server.
5. In the **Proxy Port** field, type the port number.
6. In the **Proxy Server Authentication Type** drop-down list, select an authentication type. By default, the authetication is set to **None**.

   If you choose Basic or NTLM authentication, enter the credentials and, optionally, the Domain.
7. Select the **Use the same web proxy settings to connect to an externally hosted Exchange** checkbox, if you want to use the web proxy to communicate with a hosted Microsoft Exchange Server (cloud deployed).
8. Select the **Apply to other nodes in the BEMS cluster** check box to communicate the Good Proxy server information to all of the BEMS nodes in the cluster.

9. Click **Test** to verify the connection to the proxy server.
10. Click **Save**.
11. Restart the Good Technology Common Services in the Windows Services Manager.

Android Push Notifications

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Mail**.
2. Click **Android Push Notification**.
3. In the **GCM Sender ID** field, type the Sender ID value of the project you created in Firebase.
4. In the **GCM API key** field, enter the Server key value of the project you created in Firebase.
5. Click **Save**.

Create Firebase Cloud Messaging API keys

These are the details for obtaining keys for the Firebase Cloud Messaging (FCM) API, which is used by BEMS to be able to send new mail notifications to Android devices. Google now uses the new service Firebase, replacing the Google Cloud Messaging (GCM) API site and project spaces. For more information about creating the Firebase Cloud Messaging API Keys, visit http://support.blackberry.com/kb to read article 44617.

Before you begin: You must have a Google account.

1. In a browser, open https://console.firebase.google.com/ and log in with a valid account.
2. Click **Create New Project**.
3. In the **Create a project** dialog box, type a project name and select the Country/region you are located in.
4. Click **Create Project**.
5. In the upper left-hand side of the screen, click  > **Project settings**.
6. Click **Cloud Messaging**.
7. Copy the value of **Server key**. This is used as the GCM API Key value in the BEMS Dashboard.
8. Copy the value of **Sender ID**. This is used as the GCM Sender ID value in the BEMS Dashboard.

Configure Stop Notifications

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

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Mail**.
2. Click **Stop Notifications**.

3. In the **User Email Address** field, type the email address of the user you want to stop notifications for.
4. Click **Save**.

Configure User Directory Lookup

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

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

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

   e. Optionally, in the **LDAP Base DN** field, provide a base DN for the LDAP search. If this field is not completed, BEMS tries to find the base DN in the namingContexts attribute.
   f. In the **Authentication Type** drop-down list, select an authentication type.
      - If you select **Basic**, enter the LDAP Logon User name and password.
      - If you selected the **Enable SSL LDAP** checkbox, and select **Certificate** authentication, enter the keystore password and add the certificate file.
   g. In the **User search key** field, type a username or email address to search for.
   h. Click **Test**.
6. Click **Save**.

Searching for users by phone number

BEMS supports users searching for other users in the GAL by phone number.

To allow BEMS to support this feature, your environment must meet the following requirements:

- The Microsoft Active Directory phone attributes must be indexed and enabled for ANR
- The phone number must be in one of the following formats:
  - +1 (555) 123 4567
  - +1.555.123.4567
  - +1-555-123-4567
  - 15551234567
  - 555.123.4567
  - +1 5551234567

By default, the phone attribute is disabled for GAL search.

Enable contact lookup by phone number

To allow users in your environment to lookup contacts using their phone number, use the Microsoft Active Directory schema MMC snap-in to index and enable ANR for the applicable phone attributes.

Before you begin: The phone number must be in a supported format. For a list of supported formats, see Searching for users by phone number.

1. Click the **Attributes** folder in the snap-in.
2. In the right panel, right-click the desired attribute, and then click **Properties**.
3. Select the **Index this attribute** check box.
4. Select the **Ambiguous Name Resolution (ANR)** check box.
5. Click **OK**.
6. If you have multiple phone attributes, repeat steps 2 to 5 for each attribute.

Configure the Certificate Directory Lookup

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

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Mail**.
2. Click **Certificate Directory Lookup**.
3. Optionally, select the **Include expired certificates in results** checkbox.

4. By default, the **Enable Contact Lookup** checkbox and **Enable GAL Lookup** checkbox are selected.
5. Optionally, select the **Enable LDAP Lookup** checkbox.
6. If you select LDAP lookup, you can use it to validate digital certificate connections to the LDAP server.
   a. In the **LDAP Server Name** field, type the name of the LDAP Server. For example, ldap.<*DNS_domain_name*>.
   b. In the **LDAP Server port** field, type the port number of the LDAP Server. By default, the port number is 389.
   c. Optionally, select the **Enable SSL LDAP** checkbox to tunnel data through an SSL-encrypted connection. If you enable SSL LDAP, the port number defaults to 636.
   d. Optionally, edit the **LDAP User Name Query Template** field. The LDAP user name query searches for a user by their user name. BEMS replaces the "{key}" with the user name when performing the query. The default template is

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

   e. Optionally, in the **LDAP Base DN** field, provide a base DN for the LDAP search. BEMS will try to find the base DN in the namingContexts attribute if this entry is not set. If this field is not completed, BEMS tries to find the base DN in the namingContexts attribute.
   f. In the **Authentication Type** drop-down list, select an authentication type.
      - If you select **Basic**, enter the LDAP Logon User name and password.
      - If you selected the **Enable SSL LDAP** checkbox, and selecte **Certificate** authentication, enter the keystore password and certificate file.
   g. In the **End User Email Address** field, type an enduser email address to search for.
   h. Click **Test**.
7. Click **Save**.

Configuring support of the BlackBerry Work apps

When you configure BEMS for support of the BlackBerry Work apps, you perform the following actions:

- In Good Control, configure Exchange ActiveSync for BlackBerry Work
- In Good Control, entitle BlackBerry Dynamics apps
- Device provisioning and activation

Note: The BlackBerry Work app must be published in Good Control. For instructions on how to add an application in Good Control, see "Registering a New Application" in the Good Control console's online help.

In Good Control, configure Exchange ActiveSync for BlackBerry Work

In Good Control, the BlackBerry Work app must be configured for Exchange ActiveSync before it can be configured to use Push Notifications service. This allows users to enroll in Exchange ActiveSync when they activate their BlackBerry Work app. For more information on how to configure Exchange ActiveSync for BlackBerry Work, see the "Enabling Exchange ActiveSync (EAS)" section in the BlackBerry Work Product Guide for Administrators.

In Good Control, entitle BlackBerry Dynamics apps

Users must be entitled to view or run the BlackBerry Dynamics apps. Good Control has an Everyone group that automatically includes all users. The easiest way to entitle apps for all your users is to entitle the apps in the Everyone group.

1. In Good Control, under **Apps**, click **App Groups**.
2. Click the **Edit** icon beside **Everyone**.
3. Beside **Entitled Enterprise Apps**, click **Add More**.
4. In the **View** drop down box, select **All Applications**.
5. Select BlackBerry Work, BlackBerry Connect, and any other apps that you are entitled to.
6. Click **OK**.

In Good Control, whitelist BEMS

You must whitelist the computer that hosts BEMS in Good Control to enable proper communication between the Good Control server and BEMS.

1. In Good Control, under **Policies**, click **Connectivity Profiles**.
2. Under **Base Profile**, click **Master Connection Profile**.
3. Under **Additional Servers**, click **Edit**.
4. Click **Add**.
5. In the **Additional Server** dialog box, complete the following actions:
    - In the **Host Name** field, type the FQDN of the BEMS machine.
    - In the **Port** field, type **8443**.
    - In the **Primary GP Cluster** drop-down list, select a Good Proxy Cluster.
    - Optional, specify a secondary Good Control cluster.
6. Click **Add**.
7. Repeat steps 3 to 6 for each additional computer that hosts BEMS with Good Proxy Clusters.
8. Click **Save**.

Add BEMS to the BlackBerry Work application server list

The BlackBerry Work client checks the BlackBerry Work server list for available BEMS instances hosting the Presence service and requires a BEMS machine to be configured for the Good Enterprise Services entitlement app.

If multiple BEMS instance are listed, you can use BlackBerry Work's Preferred Presence Server Configuration parameter to set up a presence affinity association. For instructions, see Configure Presence affinity for BlackBerry Work.

1. In Good Control, under **Apps**, click **Manage Apps**.
2. Click **BlackBerry Work**.
3. On the **BlackBerry Dynamics** tab, under **Server**, click **Edit**. Complete the following actions:
   - In the **Host Name** field, type the FQDN of the BEMS computer.
   - In the **Port** field, type **8443**.

   Note: If you do not import a publicly verifiable certificate into the BEMS Java keystore, access to the BEMS Dashboard from a browser shows an untrusted SSL certificate and you must upload the BEMS certificate to Good Control.
4. To add additional BEMS instances, click  and repeat step 3.
5. Click **Save**.

Configuring the Push Notifications service for high availability

High availability for the Push Notifications service is based on clustering. The Push Notifications service supports high availability by adding additional servers running Push Notifications. The BEMS instances that host the Push Notifications services that you designate to participate in high availability must share the same database.

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

1. During the installation of additonal Push Notifications service instances, on the Database Information screen you specify the same database for each instance.
2. Whitelist each computer hosting an instance of the Push Notifications instance and port in Good Control.
3. Add each new computer hosting the Push Notifications instance to the BlackBerry Work application server list.

Configuring the Push Notifications service for disaster recovery

Recommended disaster recovery measures for Push Notifications service are based on an active/warm standby clustering model.

Before adding a Push Notifications service instance for disaster recovery, you complete the following actions:

1. Configure database replication for the Push Notifications service database from your primary site to your disaster recovery site. SQL log shipping is recommended. Consult your database administrator for assistance.

2. Make sure that the appropriate network ports are open to allow the Push Notifications service servers within your disaster recovery site to communicate with the database, Microsoft Exchange Server, and Good Proxy servers in your disaster recovery and primary site.

When you configure a disaster recovery Push Notifications service instance, you complete the following actions:

1. Configure the disaster recovery Push Notifications service instance to use the primary database in the cluster. For instructions, see Configure the SQL database for Push Notifications service.
2. Configure the disaster recovery Push Notifications service instance to use the primary Good Proxy server in the cluster.
3. Whitelist the disaster recovery computer that hosts the Push Notifications service server and port in Good Control. For instructions, see In Good Control, whitelist BEMS .
4. Configure your disaster recovery Push Notifications service instance in Good Control for the BlackBerry Work app. For instructions, see Adding BEMS to the BlackBerry Work Application Server List.For instructions, see . Make sure you set the priority setting to Secondary or Tertiary.

   Note: After the disaster recovery Push Notifications service instance is installed and configured, stop the Good Technology Common Services to place the Push Notifications service instance in warm standby.

In a disaster recovery situation in which you want to failover, you complete the following actions:

1. Stop the BlackBerry Common service on all your primary Push Notifications service instances.
2. Failover your Push Notifications service database on your database server. For example, make the Push Notifications service database active.
3. Failover your databse FQDN DNS to your disaster recovery database server.
4. If you cannot failover your database FQDN DNS, log in to the BEMS Dashboard and update the Push Notifications service database information to point to your disaster recovery database server, then restart the Good Technology Common Services.
5. Start the Good Technology Common Services on your disaster recovery Push Notifications service instance.
6. If you also failed over your Good Proxy servers as part of this process, you must update the Good Proxy information in the BEMS dashboard for the Push Notifications service.

Push Notifications service logging and diagnostics

Performance logs and diagnostic information for BEMS and the BlackBerry Push Notifications service are located in the BEMS Web Console. To set and change the administrator's password, see Changing the BEMS services account password.

The log files are stored in the BEMS installation directory. By default, the log files are located in: <*drive*>:\Program Files \BlackBerry\BlackBerry Enterprise Mobility Server\.

The BEMS log is located in: <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\BlackBerry Server Distribution\gems_quickstart-<*version*>\data\log\.

View relevant logs in the BEMS Web Console

The BEMS Web Console provides advanced configuration and tuning options for BEMS. It should be used with care as it offers advanced maintenance capabilities intended for expert users of the system.

1. Open a browser and go to the Apache Karaf Web Console Configuration web site located at **http://<*fqdn_of_the_bems_host*:8443/system/console/configMgr** and login as administrator with the appropriate Microsoft Active Directory credentials.
2. On the menu, click **OSGi** > **Log Service**.
3. Scroll through the log activity. It's listed in chronological order.

After you finish: You can view the logs from the BEMS installation directory.

Set the detailed Notifications Cutoff Time

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

1. Open a browser and go to the Apache Karaf Web Console Configuration web site located at **http://<*fqdn_of_the_bems_host*:8443/system/console/configMgr** and login as administrator with the appropriate Microsoft Active Directory credentials.
2. On the menu, click **OSGi** > **Configuration**.
3. Click **Good Technology Email Push Coalescing**.
4. In the **pushDowngradeCutoffSec** field, increase or decrease the value, in seconds, as required. The default value is 43200 seconds or 12 hours. The maximum value is 259200 seconds, or 3 days.
5. Click **Save**.

Checking EWS Listener and Push Channels

BEMS provides diagnostic web addresses to help you determine if Push Notifications service is working properly. You must access the diagnostic web address locally on the computer that hosts thePush Notifications service.

The following table lists the web addresses you can query on BEMS to verify if the Push Channels and EWS Listener are working:

Diagnostic URLs	Sample output	Comments
Push Channels **http://127.0.0.1:8181/pushnotify/pushchannels**	`[{"registrationId":"acooc@demolair.com#3EFED82C-BE27-4A71-BF64-7F68424122B4","account":"acooc@demolair.com","pushToken":"8FAE82462C794005BFC90C7A4B654B523CDB2FCC59A922BDAFBAFD30D2460614","bundleId`	If the outputs are NULL ([]), check the log for the reasons why. If outputs are not found, then refer to the

Diagnostic URLs	Sample output	Comments
	":"com.good.gcs.g3.enterprise","ewsProfileId":"51","deviceType":"ios"}]	SSH console for additional detail.
EWS Listener **http://127.0.0.1:8181/ewslistener/user**	[{"connectionId":45946713,"email":"acooc@demolair.com","stage":"Streaming","lastErrorTime":null,"status":null}]	Using the first check, you see a push channel registration if the device successfully connected to BEMS. Then, if your Exchange Configuration is set up properly you see a streaming EWS Listener subscription.

Configuring the Connect service

The Connect service governs instant messaging and presence capabilities of the BlackBerry Connect app.

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

1. Configure the Connect service in the BEMS Dashboard.
2. Configure Good Control for BlackBerry Connect
3. Enable SSL using Good Proxy.
4. Enable BlackBerry collaboration suite users from multiple domains within the same forest.

Configuring the Connect service in the BEMS dashboard

The Connect service components are not accessible until you enter the service account credentials for BEMS. BEMS uses this information to securely connect to Microsoft Services like Microsoft Active Directory, Microsoft Lync Server, Microsoft Exchange Server, Skype for Business server, and Microsoft SQL Server. The service account credentials are not stored after the browser session ends and must be entered each time you access the Connect service.The service account must have RTCUniversalReadOnlyAdmins rights. If an account has not yet been created, contact your Windows domain administrator to request an account.

Before you configure the BlackBerry Connect service, make sure you prepare the Microsoft Lync Server or Skype for Business topology for BEMS. For instructions, see Preparing the Microsoft Lync Server and Skype for Business topology for BEMS

Note: If you make changes to the BEMS dashboard, you must first stop the Good Technology Connect service, make the changes, and then start the Good Technology Connect service for the changes to take affect.

When you configure the Connect service, you configure the following components:

- Database
- BlackBerry Dynamics
- Microsoft Lync Server 2010, Microsoft Lync Server 2013, Skype for Business, or Cisco Jabber
- Optionally, Microsoft Exchange Server
- Optionally, Web proxy

Configure the database

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Connect**.
2. If necessary, click **Service Account** and enter the BEMS service account credentials.
3. Click **Database**
4. Enter the Microsoft SQL Server and database name.
5. In the **Authentication Type** drop-down list, select one of the following options:
    - If you select **Windows Authentication**, the type the credentials for the service account configured for the Connect service.
    - If you select **SQL Server Login**, type the username and password used to access the Microsoft SQL Server database.
6. Click **Test** to verify the connection with the database.
7. Click **Save**.
8. Restart the Good Technology Connect service.

Configure BEMS connectivity with BlackBerry Dynamics

Before you begin: Make sure that the Good Control and Good Proxy servers are installed and operating. For more information, see the Good Control/Good Proxy Server Installation Guide.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Connect**.
2. Click **Service Account**.
3. Enter the service account username and password.
4. Click **Save**.
5. Click **BlackBerry Dynamics**.
6. In the **Hostname** field, type the Good Proxy server hostname.
7. In the **Port** field, type the port. Select the communication type to use http or https.

    Note:

- If the Connect service uses Cisco Unified Communications Manager IM and Presence and you select HTTPS, you must upload the Good Proxy server's CA certificate to the BEMS Connect server's Windows keystore. For instructions, see Export the Good Control CA certificate to configure Connect to use SSL.
- If the Connect service uses Microsoft Lync Server or Skype for Business and you select HTTPS, the trusted certificate must be installed in the Windows keystore. For instructions, see Import the Good Control certificate to the BEMS Windows keystore.

8. Click **Test** to verify the connection to the Good Proxy server.
9. Click **Save**.

Configure Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business for the Connect service

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Connect**.
2. If necessary, click **Service Account** and enter the BEMS service account credentials.
3. Click **Lync 2010**, **Lync 2013**, or **Skype for Business**. The system queries the instant messaging server to verify that the appropriate BEMS instant messaging server topology is added. This can take a few moments.
4. In the **Application ID** drop-down list, select <***appid_connect.mycompany.com***>.

   If the drop-down list is empty, either the BEMS <*instant messaging server type*> topology is not setup correctly or the service account does not have permissions to query these settings.
5. Click **Test** to verify the connection to the instant messaging server.
6. Click **Save**.

Configuring the BlackBerry Presence and BlackBerry Connect services in a multicluster Cisco Unified Communications Manager for IM and Presence environment

You can configure the BlackBerry Presence and BlackBerry Connect services for users that are located in multicluster Cisco Unified Communications Manager for IM and Presence deployments to locate and communicate with each other.

Configuring your Cisco Unified Communications Manager for IM and Presence multicluster environment with the BEMS Presence and Connect service allows users to connect and communicate with users in the same Presence domain and located in separate clusters.

Steps to configure multiple Cisco Unified Communications Manager IM and Presence environments for BlackBerry Connect and BlackBerry Presence services

When you configure multiple Cisco Unified Communications Manager IM and Presence environments for BlackBerry Connect and BlackBerry Presence services, you perform the following actions:

Step	Action
1	Make sure your multi-cluster environment has the following configured: • DNS SRV records for Cisco Jabber Service Discovery. For instructions, see " Service Discovery" in the Cisco Jabber Planning Guide for your version of Cisco Jabber. • Cisco Intercluster Lookup Service (ILS) between the CUCM clusters in your environment. For instructions, see "Intercluster Lookup Service" in the Cisco Unified Communications Manager Features and Services Guide for your version of Cisco Unified Communications Manager. • Intercluster Peering between the CIMP clusters in your environment. For instructions, see " Intercluster Peer Configuration" in the Cisco Unified Communications Manager Configuration and Administration Guide for your version of the Cisco Unified Communications Manager.
2	Create the following users and passwords on each CUCM server in each multi-cluster domain. These must be the same, including case sensitivity on each server. BEMS uses these users and password to authenticate to the CUCM server for user Presence information. For BlackBerry Connect • AXL application user username and password. For BlackBerry Presence • Application user and password. For instructions, see Create an Application User. • UDS Username (Dummy user). For instructions, see Create a Dummy User.
3	Download the required certificates from each cluster. • Tomcat.der • Cup.der • Cup-xmpp.pem • CUCM SSL certificate. Visit the Cisco Devnet to see Download the Cisco Unified CM SSL Certificate
4	Import the certificates into the Java keystore. For instructions, see Import the required certificate into the Java keystore on BEMS.
5	Configure the BlackBerry Connect service.
6	Configure the BlackBerry Presence service.

Configure Cisco Jabber for the Connect service

With BEMS installed, the initial configuration dashboard URL used will not match the self-signed certificate that was created. You can replace localhost with the FQDN that you specified during the installation, and bookmark this for future use.

Before you begin:

- Stop the Good Technology Connect service.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Connect**.
2. If necessary, click **Service Account** and enter the BEMS service account credentials.
3. Click **Jabber**.
4. In the **IM and Presence SIP domain** field, enter the SIP domain.
5. If your environment consists of multiple IM and Presence service clusters, select the **Enable Service Discovery** checkbox and enter the following information:
    - Enter the **AXL Administrator Username** and **AXL Administrator Password**.
    - If the voice service and XMPP service domains are not the same in your environment, in the **Service Domain field**, enter the domain where the SRV records are located.
6. In the **Cisco Unified Communications Manager User Data Service (UDS) FQDN** field, enter the FQDN of the Cisco Unified Communications Manager server that Jabber Presence Provider (JPP) needs to access and query the contact cards.
7. In the **Cisco Unified Communications Manager User Data Service (UDS) port** field, enter the Cisco Unified Communications Manager server port number that JPP uses with the ciscoUDSServer to query the contact cards. For example, 8443.
8. In the **Cisco Unified Communications Manager IM and Presence XMPP client service FQDN** field, enter the FQDN of the Cisco Unified Communications Manager IM and Presence server.

    Cisco Jabber uses CUCM LDAP only. It does not use directory lookup.
9. Start the Good Technology Connect service.

After you finish:

- Connect policies applied to user devices must specify Cisco Jabber as the IM platform in use. Configure these polices, in the Good Control console. Go to Policy Sets > policy_name > APPS tab > App Specific Polices > Good Connect > Server Configuration and from the Platform dropdown, select Cisco Jabber.
- Configure Good Control for Connect. For instructions, see Configuring Good Control for BlackBerry Connect

Configure BEMS to access Microsoft Exchange Server conversation histories

Enable this component connection if you want to access saved conversations from Microsoft Exchange Server.

Before you begin:

- The conversation history is enabled on the enterprise Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business for which you are configuring BlackBerry Connect.
- You prepared the Microsoft Lync Server or Skype for Business topology for BEMS. For instructions, see Preparing the Microsoft Lync Server and Skype for Business topology for BEMS

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Connect**.
2. If necessary, click **Service Account** and enter the BEMS service account credentials.
3. Click **Microsoft Exchange**.
4. Select the **Enable Conversation History** checkbox. Complete the following actions:
    - In the **Please enter the Microsoft Exchange Server information** field, type the web address of your Microsoft Exchange Server.
    - In the **Exchange Server Type** drop-down list, select the Microsoft Exchange Server version that is in your environment.
    - In the **Server Write Interval** field, type the frequency, in minutes, that each unique conversation is sent to the Microsoft Exchange Server.
    - If required, select the **Requires Credential** checkbox. Type the user name and password used to access the Microsoft Exchange Server.
5. Click **Test**.
6. Click **Save**.

Configure the BEMS Internet connection using a proxy server

Complete this task if your company uses a web proxy server to connect to the Internet.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Connect**.
2. If necessary, click **Service Account** and enter the BEMS service account credentials.
3. Click **Web Proxy**.
4. Select the **Use Web Proxy** checkbox.
5. Type the proxy web address and port number.
6. In the **Proxy Authentication Type** drop-down list, select one of the following authentication types:
    - **Basic** authentication requires a user name and password by the Connect service to authenticate a request.
    - **Digest** authentication is more secure because it applies a hash function to the password before sending it over the network.
    - **None**, if no authentication is required.

Note: If you specify an authentication type, the Connect service username and password are automatically populated based on the Windows domain service account you assigned to the Connect service under Configuring Windows Services.

7. Optionally, specify a domain.
8. Optionally, click **Test** to verify the connection to the web proxy.
9. Click **Save**.

Configuring Good Control for BlackBerry Connect

When you use BEMS in a Good Control environment, you must complete the following tasks to prepare Good Control:

- Add the BEMS instances to Good Control's application management handler to specify the available servers that the BlackBerry Connect app can connect to.
- Specify the domains and servers in your network that host a BEMS instance that BlackBerry Connect apps can connect to.
- Configure BlackBerry Connect app settings, such as displaying disclaimer text and allowing users to perfrom app diagnostics.
- Install and activate BlackBerry Connect.

For more information about configuring Good Control for BlackBerry Connect, see the BlackBerry Connect Administration content.

Enabling persistent chat

The persistent chat feature allows users to create topic-based discussion rooms and participate in rooms. If you enable persistent chat in Microsoft Lync Server 2013 or Skype for Business, you can enable it in your BEMS environment.

For more information about enabling persistent chat for BlackBerry Connect, see the BlackBerry Connect Administration content.

Configuring the Connect service for high availability

Configuring Connect for high availability is not supported for Connect using Cisco Jabber.

When you configure the Connect service for high availability, you perform the following actions:

1. Configure each new Connect instance to use the existing database.
2. Configure each new Connect instance to point to the same Good Proxy server.
3. Whitelist each new Connect server host and port in Good Control.
4. Configure each new Connect instance in Good Control for the BlackBerry Connect app.

Configuring the Connect service for disaster recovery

Disaster Recovery for the BlackBerry Connect service is based on an active/warm standby clustering model. Disaster recovery is not supported for BlackBerry Connect using Cisco Jabber.

Before you add a BlackBerry Connect instance for disaster recorvery, you complete the following actions:

1. Evaluate your Microsoft Lync Server or Skype for Business disaster recovery strategy.

   If you have separate Front End pools for disaster recovery, create a separate Trusted Application Pool for your Connect instances. This separate Trusted Application Pool should be associated with the disaster recovery Front End pool. Associate all disaster recovery BlackBerry Connect instances to this Trusted Application Pool. If you don't have separate Front End pools for disaster recovery, then using a single Trusted Application Pool, but make sure your Lync or Skype for Business disaster recovery strategy properly preserves the Trusted Application Pool in event of a failover.

   Consider the following for Microsoft Lync Server or Skype for Business front-end pool:

   Your environment has the following Microsoft Lync Server or Skype for Business Front-End pools:

   - Pool1 is for general use
   - Pool2 is for high availabilty use

   You create a Trusted Application Pool for Pool1. It is recommended you create an additonal Trusted Application Pool for the high availability instances. The additional Trusted Application Pool is created in your front-end high availability pool.

2. Make sure that the appropriate network ports are open to allow BlackBerry Connect servers in your disaster recovery site to communicate with database, Microsoft Lync Server or Skype for Business Server, Microsoft Lync Server or Skype for Business database, and Good Proxy servers in your disaster recovery and primary site.

Add a new Connect service instance for disaster recovery

1. Create a Connect database on the database server in the disaster recovery site. Use the schema files that came with the BEMS software to manually extend the schema. Only one database is needed for all disaster recovery Connect instances.
2. Do not provide the name of the Connect database during the disaster recovery Connect installation.
3. After the installation, configure Connect to use the database in the disaster recovery site.
4. Configure your disaster recovery Connect instance to use the secondary Good Proxy server in the cluster.
5. Whitelist your disaster recovery Connect server host and port in Good Proxy. For instructions, see the 'Add the BEMS instances to the connectivity profiles in Good Control topic in the BlackBerry Connect Administration content.
6. Configure your disaster recovery Connect instance in BlackBerry UEM for the BlackBerry Connect App. For instructions, see Configuring Good Control for BlackBerry Connect. Make sure you set the priority setting to Secondary or Tertiary.

After you finish: After the disaster recovery Connect instance is installed and configured, stop the Good Technology Connect service. This places the disaster recovery Connect instance in warm standby.

Failover in disaster recovery

1. Stop the Good Technology Connect service on all your primary Connect instances.
2. Start the Good Technology Connect service on your disaster recovery Connect instance.

Specify the Good Proxy the BlackBerry Connect service contacts in a cluster

You can specify the Good Proxy server that the Connect service contacts first. When you specify the Good Proxy, it forces BEMS to always communicate with this Good Proxy server first for any BlackBerry Dynamics messages. The Connect service uses the Good Proxy server to create a list of Good Proxy servers to use. If the Good Proxy server that you specified in the BEMS Dashboard fails, then the Connect service contacts the next primary Good Proxy server in the list.

By default, this feature is disabled.

Before you begin:

- More then one Good Proxy is installed and configured in clusters in your environment.
- BEMS is configured to use a Good Proxy.

1. In Good Control, under **Settings**, click **Clusters**.
2. On the **GP clusters** tab, click the proxy server that you want BEMS to use.
3. Click **Update**.
4. On the computer that hosts BEMS, in a text editor, open the **GoodConnectServer.exe.config** file. By default, the file is located in <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\BlackBerry Connect\.
5. Add the following key and value to the file: type **<add key=ENABLE_CONFIGURED_GP_PIN" value=true** />.
6. Save the file.
7. Restart the Good Technology Connect service.

Using friendly names for certificates in BlackBerry Connect

The friendly name of a certificate can be helpful when multiple certificates with similar subjects exist in a certificate store. Friendly names are properties in the X.509 certificate store that associate aliases with certificates so they can be easily identified.

You can restrict certificates used for BlackBerry Connect to a Friendly Name by completing the following actions

1. If you do no have one, create and enroll a certificate.
2. Change the certificate friendly name and description.
3. Setting the new certificate friendly name string value in the BlackBerry Connect Server configuration file (GoodConnectServer.exe.config).

If you do not already have a certificate, you can create and verify a BEMS SSL certificate for Lync. For more information, see Create and add the BEMS SSL certificate for Microsoft Lync Server 2010, Microsoft Lync Server 2013, and Skype for Business.

Change the certificate friendly name description

1. Open the Microsoft Management Console (MMC).
2. Click **Console Root**.
3. Click **File** > **Add/Remove Snap-in**.
4. In the **Available snap-ins** column, click **Certificates** > **Add**.
5. Select **Computer account**. Click **Next**.
6. Select **Local Computer**. Click **Finish**.
7. Click **OK**.
8. Click **Certificates (Local Computer)** > **Personal** > **Certificates**.
9. Double-click the certificate you want to change.
10. Click the **Details** tab.
11. In the **Show** drop-down list, click **<All>**.
12. Click **Edit Properties**.
13. In the **Friendly name** field, type a friendly name.
14. In the **Description** field, type a description.
15. Click **Apply**.
16. Click **OK**. Click **OK** again.

After you finish: Specify the certificate's friendly name in the configuration file for the Connect service.

Add the certificate friendly name to the BlackBerry Connect server configuration file

Before you begin: Specify the certificate friendly name.

1. In a text editor, open the **GoodConnectServer.exe.config** file. By default, the GoodConnectServer.exe.config file is located in <*install path*>\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Connect\.
2. At the end of the file, type **<add key="RESTRICT_CERT_BY_FRIENDLY_NAME" value="<*cert_friendly_name*>"/>**. The key value is case sensitive.
3. Save your changes.
4. Restart the Good Technology Connect service.

Configuring the Connect service for SSL communications

By default, SSL is disabled, but the Connect service can be configured to run securely using SSL/TLS (HTTPS) to communicate with the BlackBerry Connect app.

BEMS requires a signed server SSL certificate from a third-party Certificate Authority (CA).

When you enable SSL support, you perform the following actions:

1. Submit a CSR request to a certificate authority. You must install the certificate on the server that generated the CRS.
2. Import the signed certificate to the computer that hosts the Connect service
3. Bind the SSL certificate to the Connect service SSL port
4. Add the new certificate information to the BEMS configuration file
5. Optionally, configure Good Control to send requests over SSL.
6. Configure the Connect service to use SSL with Good Proxy.

Import the signed certificate to the computer that hosts the Connect service

1. Log in to the computer hosting BEMS with the service account.
2. Open the Microsoft Management Console (MMC).
3. Click **Console Root**.
4. Click **File** > **Add/Remove Snap-in**.
5. In the **Available snap-ins** column, click **Certificates** > **Add**.
6. Select **Computer account**. Click **Next**.
7. Select **Local Computer**. Click **Finish**.
8. Click **OK**.
9. Expand **Certificates**.
10. Expand **Personal**.
11. Right-click Certificates and click **All Tasks** > **Request New Certificate**.
12. In the **Certificate Enrollment** wizard, follow the onscreen instructions to enrol for a Computer certificate.
13. Click **Enroll**.
14. Verify that the new certificate appears and the **Intended Purposes** column displays **Client Authentication, Server Authentication**.
15. Click **Finish**.

After you finish:

1. Copy the thumbprint of the imported certificate.
   a. Double-click the imported certificate.
   b. Click the **Details** tab.
   c. In the **Show** dropdown list, click **Properties Only**.
   d. In the **Field** column, click **Thumbprint**.
   e. Copy the hexidecimal values into a text editor. Delete the spaces between the hexadecimal values. For example, if you copied 80 82 41 2f... it becomes 8082412f...
   f. Keep the text editor open.
2. Bind the signed certificate to the Connect service SSL port.

Bind the SSL certificate to the Connect service SSL port

Before you begin:

- Import the CA-signed certificate to the computer that hosts the Connect service.
- Export the signed certificate thumbprint to a text editor.

1. If required, login to the computer that hosts the Connect service with the service account.
2. Open a command prompt (run as administrator).
3. Check that a certificate is not already bound to port 8082. Type **netsh http show sslcert**.

   If a certificate is bound to port 8082, type **netstat -abn > netstatoutput.txt** to output the list of ports and processes to which they are bound. You must first delete the certificate before binding the new certificate or select a new port to bind the SSL. If you choose to bind the certificate to another port, consider this modification when configuring the Connect service. To delete the existing certificate, type **netsh http delete sslcert ipport=0.0.0.0:8082**

   For more information about netsh, visit the Technet Library to see Netsh Commands for Hypertext Transfer Protocol (HTTP).

4. Bind the certificate to the SSL port. In a command prompt (run as administrator), type **netsh http add sslcert ipport=0.0.0.0:<*port*> certhash=<*thumbprint*> appid={AD67330E-7F41-4722-83E2-F6DF9687BC71}**

   Where <*thumbprint*> is the thumbprint of the signed certificate that you exported to the text editor. For instructions, see Import the signed certificate to the computer that hosts the Connect service.

5. Press **Enter**.
6. To verify the certificate binding, type **netsh http show sslcert**.

After you finish:

1. Add the new certificate information to the BEMS configuration file.
2. Configure the Good Control to send requests over SSL.

Add the new certificate information to the BEMS configuration file

Before you begin: Backup the BlackBerry Connect server configuration file.

1. To modify the server configuration to use the correct SSL certificate, navigate to the **GoodConnectServer.exe.config** file. By default, the file is located in <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Connect\.
2. In a text editor (run as administrator), edit the **GoodConnectServer.exe.config** file.
3. Locate `<add key="BASE_URL" value="http://*:8080/"/>`.
4. Change the line to `<add key="BASE_URL" value="https://*:8082/"/>`.
5. Save your changes.
6. Restart the Good Technology Connect service

After you finish: Configure Connect to use SSL with Good Proxy.

Change the application server settings in Good Control to send requests over SSL

You must also add https:// to the servers and assign them to the new SSL port.

Before you begin: If you installed a server without SSL, including implementations of BlackBerry Connect and BlackBerry Connect Server, the server has its FQDN added and associated with the new SSL port. If you installed non-SSL BlackBerry Connect servers and Connect service servers, you must remove them from Good Control.

1. In Good Control, under **Apps**, click **Manage Apps**.
2. Click **BlackBerry Connect**.
3. Click the **BlackBerry Dynamics** tab.
4. In the **Server** section, click **Edit**, and complete one of the following actions: .
   - Click  to add a server.
   - Click  to change an existing server.
5. In the **Host Name** field, type the FQDN of the GEMS-Connect server.
6. In the **Port** field, type the SSL port number. By default, this port number is 8080 or 8082.
7. Repeat steps 4 to 6 for each GEMS-Connect server.
8. In the **Configuration** text box, type **DEFAULT-SSL**=**TRUE**.

Change user affinity-clustering

1. In Good Control under **Policies**, click **Policy Sets**.
2. Select the policy set you want to govern BlackBerry Connect.

3. On the **Apps** tab, click **App Specific Policies** > **BlackBerry Connect**.
4. Click the **Server Configuration** tab.
5. In the **Connect Server Hosts** text box, change the port numbers to the new SSL port for BEMS.

Export the Good Control CA certificate to configure Connect to use SSL

By default, the Good Proxy server uses a certificate that is signed by Good Control CA, a private CA. This means Connect will not trust the certificate. For Connect to trust the Good Proxy server's certificate, you must upload Good Control's CA certificate to the GEMS-Connect server's Windows keystore.

1. In a browser, in the address bar, type the Good Control web address.
2. On the address bar, click the lock icon.
3. Click **More information**.
4. Click **Security**, then click **View Certificate**.
5. Click the **Details** tab.
6. In the **Certificate Hierarchy** section, expand the BlackBerry Connect CA entry.
7. Click **Export**.
8. Save the file on your desktop.

After you finish: Import the CA certificate into the Windows keystore.

Import the Good Control certificate to the BEMS Windows keystore

1. Open the Microsoft Management Console.
2. Click **Console Root**.
3. Click **File** > **Add/Remove Snap-in**.
4. Click **Certificates**.
5. Select **Computer Account** > **Local computer** > **OK**.
6. Expand **Certificates (Local Computer)** > **Trusted Root Certification Authorities**.
7. Right-click **Certificates**, and click **All Tasks** > **Import**.
8. Click **Next**.
9. Browse to where you saved the Good Control CA certificate that you exported. For example <*drive*>:\bemscert\gdca.cer. Click **Open**.
10. Click **Next**.
11. Click **Finish**. Click **OK**.

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

Upload the CA Certificate to Good Control

If your certificate is signed with an internal certificate authority, for example, a private CA, you must upload the CA certificate to Good Control. Doing this allows the BlackBerry Connect client to trust your certificate. If you do not upload your private CA certificate to Good Control, BlackBerry Connect cannot connect to the BlackBerry Connect service.

1. Obtain a copy of your CA certificate. Consult your certificate administrator if you do not have access to the CA certificate.
2. In Good Control, under **Settings**, click **Certificates**
3. Click the **Server Certificates** tab.
4. Click  and navigate to the CA certificate and upload it.
5. Click **Apply**. Good Control automatically distributes the CA certificate to all BlackBerry Dynamics apps, including BlackBerry Connect.

Enable BlackBerry collaboration suite users from multiple domains within the same forest

To support BlackBerry collaboration suite users from multiple domains within the same forest, use the Microsoft Active Directory schema MMC snap-in to enable users to be accessed from the global catalog.

1. Click the **Attributes** folder in the snap-in.
2. In the right panel, right-click the desired attribute, and then click **Properties**.
3. Select the **Replicate this attribute to the Global Catalog** check box.
4. Click **OK**.
5. Verify that the following attributes are published to the global catalog:
    - msrt-primaryuseraddress
    - mail
    - telephoneNumber
    - displayname
    - title
    - mobile
    - givenName
    - sn
    - sAMAccountName

- msRTCSIP-UserEnabled
- msRTCSIP-UserAddress

6. In a text editor, open the GoodConnectServer.exe.config file. By default, the file is located in <*drive*>:\Program Files \BlackBerry\BlackBerry Enterprise Mobility Server\Good Connect folder.
7. In the <appSettings> section of the file, locate the following values and update as required:
   - <addkey = "AD_USERS_SOURCE" value= "GC" />
   - <addkey = "AD_USERS_SOURCE_DOMAIN" value="<root GC domain; LDAP format>"/>
8. Restart the Good Technology Connect service.

Configuring Windows Services

The BlackBerry Connect server is now listed in Windows Services. You can view the service status and the service account user you entered for the Connect service.

For Connect to run as another domain user, the alternate domain user must:

- Have access to the private key of the computer certificate.
- Be enabled to “Log on as a service” through the Local Security Policy tool.

Configure permissions for the service account

1. On the computer that hosts BlackBerry Connect, run the **Local Security Policy** administrative tool.
2. In the left pane, expand **Local Policies**.
3. Click **User Rights Agreement**.
4. Configure the BlackBerry Connect service account for the **Log on as a service** permission.

Troubleshooting BlackBerry Connect Issues

Failed to start BlackBerry Connect server

Possible cause	Possible solution
If the Application-log displays `Failed to start GoodConnectServer: Microsoft.Rtc.Signaling.ConnectionFailureEx`	Correct the OCS_SERVER value in the configuration file.

Possible cause	Possible solution
`ception: Unable to establish a connection. ---> System.Net.Sockets.SocketException: No such host is known`, then the hostname value in the configuration file for the key OCS_SERVER does not exist or is not recognized as a valid server.	
If the Application-log displays `Failed to start BlackBerryConnectServer: Microsoft.Rtc.Signaling.ConnectionFailureException: Failed to listen on any address and port supplied`, then the port number specified for UCMA_APPLICATION_PORT in the configuration file is either blocked by a firewall or used by another application.	Unblock port if it is a firewall issue or choose another port number.
If the Application-log displays `Failed to start BlackBerryConnectServer: WCFGaslampServiceLibrary.OCSCertificateNotFoundException: Certificate not found`, then the certificate's subjectName doesn't contain the local host's FQDN and the private key for the certificate isn't enabled for the user which executes the BEMS software.	Enable private keys for this certificate for the user running the BEMS machine.

The endpoint was unable to register

Possible cause

If the Application-log displays `Temporarily Unavailable Microsoft.Rtc.Signaling.RegisterException: The endpoint was unable to register. See the ErrorCode for specific reason`, then the port number specified in OCS_PORT_TLS is not valid.

Possible solution

Correct OCS_PORT_TLS value in the configuration file.

Remote disconnected while outgoing tls negotiation was in progress

Possible cause

If the Application-log displays `Remote disconnected while outgoing tls negotiation was in progress --> System.Net.Sockets.SocketException: An existing connection was forcibly closed by the remote host`, then the OCS_TRANSPORT was specified as TLS, however the port number provided was TCP.

Possible solution

Change the OCS_PORT_TLS to 5061.

Error message: The process was terminated due to an unhandled exception. Microsoft.Rtc.Internal.Sip.TLSException

Possible cause

The SSL certificate was not created with the correct cryptographic service provider and key spec. The KeySpec property sets or retrieves the type of key generated. Valid values are determined by the cryptographic service provider in use, typically Microsoft RSA.

Possible solution

Verify that the Provider, ProviderType, and KeySpec values are the same as the examples below or the CA must reissue a new SSL and appropriate provider and key spec values.

1. On the computer that hostsBEMS, open the Windows PowerShell and type the following command: **certutil.exe –v –store "my" <*name of ssl cert*>" > c:\temp\ssl.txt**
2. In a text editor, open the **ssl.txt** file. By default, the ssl.txt file is located in <*drive*>:\temp.
3. Search for **CERT_KEY_PROV_INFO_PROP_ID**.
4. The SSL certificate information should return the following information:

```
CERT_KEY_PROV_INFO_PROP_ID(2):
Key Container = 9ad85141c0b791ad17f0687d00358b70_dd7675d5-867d-479c-90b0-
cd24435fe903
Provider = Microsoft RSA SChannel Cryptographic Provider
ProviderType = c
Flags = 20
KeySpec = 1 -- AT_KEYEXCHANGE
```

Configuring the BlackBerry Presence service

When you configure the BlackBerry Presence service to support BlackBerry Work and other third-party apps running on the BlackBerry Dynamics platform, you perform the following actions:

- Configure BlackBerry Presence in the BEMS Dashboard.
- Manually configure the Presence service for multiple application endpoints.
- Configure Good Control for Presence.

Configuring the BlackBerry Presence service in the BEMS Dashboard

The BlackBerry Presence service exposes the Lync Presence Provider (LLP) to third-party BlackBerry Dynamics applications.

When you configure the BlackBerry Presence service, you complete the following actions:

- Log in with the service account credentials
- If not completed, configure BlackBerry Dynamics
- Optionally, configure the BlackBerry Presence service settings
- Configure Microsoft Lync Server 2010, Microsoft Lync Server 2013, and Skype for Business for the BlackBerry Presence service
- Configure Jabber for the BlackBerry Presence service

Logging in to the Presence service

The BlackBerry Presence service components are unavailable until you provide the correct service account credentials for BEMS. BEMS uses this information to securely connect to Microsoft Services like Microsoft Active Directory, Microsoft Lync Server, Microsoft Exchange Server, Skype for Business server, and Microsoft SQL Server. The service account must have RTCUniversalReadOnlyAdmins rights. If an account has not yet been created, contact your Windows domain administrator to request an account.

Note: The service account credentials are not stored after the current browser session ends and must be entered each time you access the Presence service. Stop the Good Technology Presence service before you configure the service account for BEMS.

Allow Presence subscriptions to users in specified domains using Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business

Your organization can use whitelisting to control which users in internal and federated domains can request subscriptions to the Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business. By allowing users in internal and federated domains to request subscriptions, this allows users to communicate between federated domains. By default this feature is

disabled and only internal users can request subscriptions and communicate directly. When this feature is configured, you can manage the allowed list from all computers hosting the Presence service.

When your organization enables whitelisting, users in a domain that is not allowed are restricted from requesting subscriptions to the instant messaging server and communicate directly. Consider the following scenarios when you enable domain white listing:

- If you enable white listing of a domain, but do not specify one or more domains, all domains are restricted from requesting subscriptions.
- If you enable white listing and specify one or more domains, only internal and those users in the specified domains are allowed to request subscriptions to the instant messaging server. If a contact is not a user in the whitelisted domain, the user presence is displayed as unknown.
- If you do not enable whitelisting of a domain, then users in any domain can request subscriptions to the instance messaging server.

Configure the BlackBerry Presence service settings

You can specify the settings for the BlackBerry Presence service or keep the default settings.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Presence**.
2. Click **Service Account** and type the login credentials for the BEMS service account.
3. Click **Settings**.
4. Optionally, in the **Subscription Expiration Time** field, type an expiration time in seconds. The Subscription Expiration Time is the time interval when BlackBerry Work contacts the Presence service for user presence status updates. By default, this is 180 seconds.
5. Select the **Enable domain whitelisting** checkbox.
6. In the **Domains whitelist** dialog box, click  .
7. In the **Domains whitelist** text box, type the names of the domains for which users you want to allow requests for subscriptions. When adding multiple domains, you can add the domains using one or more of the following formats to separate the domains:
    - Comma, followed by a space
    - Semi-colon, followed by a space
    - Space
    - New line
8. Click  .
9. Click **Test**.
10. Click **Save**.

Remove a domain and restrict users from requesting subscription requests

You can remove domains and restrict users of that domain from requesting subscription requests

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Presence**.
2. If necessary, click **Service Account** and type the login credentials for the BEMS service account.
3. Click **Settings**.
4. In the **Domains whitelist** dialog box, click the X beside the domain you want to remove from the list.
5. Click **Save**.
6. In Microsoft Lync environments, manually restart LPP and relaunch the BlackBerry Work app.
7. In Cisco Jabber environments, manually restart common services and relaunch the BlackBerry Work app.
8. Restart the Good Technology Presence service.

Configure Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business for the Presence service

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Presence**.
2. If necessary, click **Service Account** and type the login credentials for the BEMS service account.
3. Click **Lync 2010**, **Lync 2013**, or **Skype for Business**. The system queries the instant messaging server to verify that the appropriate BEMS instant messaging server topology is added. This can take a few moments to complete.
4. In the **Application ID** drop-down list, select the instant messaging server Presence Provider application ID.

   If the drop-down list is empty, either the BEMS <*instant messaging server type*> topology is not setup correctly or the service account does not have permissions to query these settings. .
5. In the **Application Endpoint** drop-down list, select the corresponding application endpoint.
6. Click **Test** to verify the connection to the instant messaging server.
7. Click **Save**.

Configure Jabber for the Presence service

Complete this task only if you have a Cisco CM IM and Presence server in your environment.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Presence**.
2. If necessary, click **Service Account** and type the login credentials for the BEMS service account.
3. Click **Jabber**.
4. In the **Cisco Unified Communications Manager User Data Service (UDS) FQDN** field, enter the FQDN of the Cisco Unified Communications Manager server that Jabber Presence Provider (JPP) needs to access and query the contact cards.

5. In the **Cisco Unified Communications Manager User Data Service (UDS) port** field, enter the Cisco Unified Communications Manager server port number that JPP uses with the ciscoUDSServer to query the contact cards. For example, 8443.
6. In the **Presence SIP domain** field, enter the domain that the Cisco Unified CM IM and Presence server is located in.
7. In the **Cisco Unified Communications Manager Server User** field, enter the Cisco Unified Communications Manager enduser. This is the user you created in Create a Dummy User. If you install multiple BEMS instances, you must use the same user account for each instance.
8. Enter the enduser password.
9. In the **REST-based Client Configuration Web Service Endpoint** field, enter the web address of the computer hosting the REST-based Presence Web Service. This must be the Cisco IM and Presence server that the dummy user is assigned to. For example, https://<*Cisco IM and Presence FQDN*>:8443/EPASSoap/service.
10. In the **REST-based Presence Web Service Endpoint** field, enter the web address of the computer hosting the REST-based Presence Web Service. This must be the Cisco IM and Presence server that the dummy user is assigned to. For example, https://<*Cisco IM and Presence FQDN*>:8083/presence-service.
11. In the **Application Username** field, enter the username of the application user. If you install multiple BEMS instances, you must use a different username for each instance.
12. In the **Application Password** field, enter the password of the application user.
13. Optionally, in the **BEMS Presence Keystore file Location** field, enter the keystore file that you imported into the default Java keystore in the topic Replacing the auto-generated SSL certificate.
14. Click **Test** to verify the fields are completed. The test does not verify that the information in the fields are accurate.
15. Click **Save**.

Manually configure the Presence service for multiple application endpoints

You can manually configure multiple application endpoints for BlackBerry Presence to load balance Presence requests between multiple endpoints on a single BEMS instance. Multiple application endpoints are not supported for Cisco Jabber.

Before you begin: You must have a Microsoft Lync Server 2010, Microsoft Lync Server 2013, or Skype for Business setup in your environment.

1. On the computer that hosts BEMS, navigate to the **LyncPresenceProviderService.exe.config** file. By default, the LyncPresenceProviderService.exe.config file is located in <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Presence.
2. In a text editor, open the **LyncPresenceProviderService.exe.config** and record the values for the following properties:
    - UCMA_APPLICATION_NAME
    - LYNC_TRUSTED_APPLICATION_POOL

- UCMA_ENDPOINT_SIP

3. Determine a naming convention for the additional Trusted Application Endpoints (virtual SIP addresses). By default, the format for the existing SIP Addresses is sip:presence_<*BEMSFQDN*>@<*SIPDomain*>. For example, sip:presence_BEMSServer1-01.example.com@example.com, sip:presence_BEMSServer1-02.example.com@example.com, and so on.
4. Create the additional Trusted Application Endpoints in the Microsoft Lync Server or Skype for Business topology using the information from steps 2 and 3 above. For instructions on creating additional Trusted Application Endpoints, see Prepare additional computers hosting BEMS.
5. In a text editor, open **LyncPresenceProviderService.exe.config**.
6. Locate the <**ucmaEndpointSips**> section. Add the value of the new additional application endpoints that you published in step 4.

   For example,

   ```
   <ucmaEndpointSips>
       <collection>
         <add item="sip:presence_BEMSServer1.example.com@example.com" />
         <add item="sip:presence_BEMSServer1-01.example.com@example.com" />
         <add item="sip:presence_BEMSServer1-02.example.com@example.com" />
       </collection>
     </ucmaEndpointSips>
   ```

7. Specify the maximum contact subscriptions that each application endpoint can manage. By default, the MAX_SUBSCRIPTIONS_PER_ENDPOINT is 1000. You can specify a subscription value between 1 and 5000. For example, if you specify that each application endpoint can manage 2000 contact subscriptions, you would locate the MAX_SUBSCRIPTIONS_PER_ENDPOINT key and change the value as required.

   ```
   <add key="MAX_SUBSCRIPTIONS_PER_ENDPOINT" value="2000" />
   ```

   Note: Specifying the MAX_SUBSCRIPTIONS_PER_ENDPOINT, doesn't load balance the subscriptions across all endpoints, it assigns 2000 subscriptions to the first endpoint before assinging the next 2000 subscriptions to the next endpoint.

8. Save the file.
9. Restart the Good Technology Presence service from the Windows Service Manager.

Configuring Good Control for BlackBerry Presence

BlackBerry Presence is one of three services, along with BlackBerry FollowMe and BlackBerry Directory Lookup, enabled through Good Control using the Good Enterprise Services entitlement app. You add BEMS as the application server to Good Enterprise Services entitlement once to enable all three services.

If you configured BlackBerry Work when you configured the BlackBerry Push Notifications no additional configuration is required.

Add BEMS to the BlackBerry Work application server list

The BlackBerry Work client checks the BlackBerry Work server list for available BEMS instances hosting the Presence service. Therefore, the list must be populated with at least one BEMS machine configured for the BlackBerry Enterprise Services entitlement app.

When multiple BEMS hosts are listed, you can use BlackBerry Work's Preferred Presence Server Configuration parameter to set up a presence affinity association.

1. In Good Control, under **Apps**, click **Manage Apps**.
2. Click **Good Work**.
3. Click the **BlackBerry Dynamics** tab.
4. In the **Server** section, click **EDIT**.
5. In the **Host Name** field, type the FQDN of the computer that hosts BEMS.
6. In the **Port** field, type **8443**.
7. For each additional computer hosting BEMS, click  and then complete steps 4 to 6.
8. Click **Save**.

After you finish: Unless you import a publicly verifiable certificate into the BEMS Java keystore, access to the BEMS dashboard from a browser will show an untrusted SSL certificate and you must upload the BEMS certificate to Good Control.

Configure Presence affinity for BlackBerry Work

BlackBerry Presence affinity for BlackBerry Work is configured in the Good Control Application Policies. Presence affinity is optional, but once set, Presence affinity takes precedence.

CAUTION: When a distributed computer system is truly load balanced, each request is routed to a different server. This load balancing approach is diminished when server affinity techniques are applied.

1. In Good Control, under **Policies**, click **Policy Sets**.
2. Click the policy you want to apply.
3. Click the **Apps** tab.
4. Expand **App Specific Policies**, and click **BlackBerry Work**.
5. On the **App Settings** tab, in the **Preferred Presence Server Configuration** section, in the **Server Hosts** field, type the FQDN of the computer that hosts BEMS and a colon followed by port 8443. For example, *<FQDN of the GEMS host1>*:8443,*<FQDN of the GEMS host2>*:8443
6. Click **Update**.
7. Repeat steps 2 to 6 for each policy that governs BlackBerry Work Presence.

Configuring the Presence service for high availability

The BlackBerry Presence service supports high availability by adding additional BEMS servers running the Presence service.

When you configure Presence for high availability, you perform the following actions:

1. Configure each new Presence instance to use the same Good Proxy server.
2. Whitelist each new Presence server host and port in Good Control.
3. Configure each new Presence instance in Good Control for the BlackBerry Work App.
4. Configure each new Presence instance in Good Control for the Good Enterprise Services entitlement app.
5. If you have Presence user affinity configured, add the new Presence instances to your affinity list.

Your environment has the following Microsoft Lync Server or Skype for Business front-end pools:

- Pool1 is for general use
- Pool2 is for high availabilty use

If you create a Trusted Application Pool for Pool1, it is recommended you create an additonal Trusted Application Pool for the high availability instances. The additional Trusted Application Pool is created in your front-end high availability pool.

Configuring Presence service for disaster recovery

Disaster recovery for BlackBerry Presence is based on an active/warm standby clustering model.

Before you add a Presence instance for disaster recorvery, you complete the following actions:

1. Evaluate your Microsoft Lync Server or Skype for Business disaster recovery strategy.

   If you have separate Front End pools for disaster recovery, it is recommended that you create a separate Trusted Application Pool for your BlackBerry Connect instances. This separate Trusted Application Pool should be associated with the disaster recovery Front End pool. Associate all disaster recovery BlackBerry Connect instances to this Trusted Application Pool. If you don't have separate Front End pools for disaster recovery, then using a single Trusted Application Pool is fine, although you must make sure your Lync disaster recovery strategy properly preserves the Trusted Application Pool in event of a failover.

   Note: Presence and Connect can use the same Trusted Application Pool for disaster recovery.

2. Ensure that the appropriate network ports are open to allow Connect servers in your disaster recovery site to communicate with with database, Microsoft Lync Server or Skype for Business Server, Microsoft Lync Server or Skype for Business database, and Good Proxy servers in your disaster recovery and Primary site.

Add a new Presence service instance for disaster recovery

1. Create a BlackBerry Presence instance to use the secondary Good Proxy server in the cluster.

2. Whitelist your disaster recovery Presence server host and port in Good Proxy. For instructions, see the 'Add the BEMS instances to the connectivity profiles in Good Control topic in the BlackBerry Connect Administration content.
3. Configure your disaster recovery Presence instance in Good Proxy for the BlackBerry Connect app.
4. Configure your disaster recovery Presence instance in Good Control for the BlackBerry Connect Enterprise Services Entitlement app.

After you finish: After the disaster recovery Presence instance is installed and configured, stop the Good Technology Presence service. This places the Presence instance for disaster recovery in warm standby.

Failover in disaster recovery

1. Stop the Good Technology Connect service on all your primary Connect instances.
2. Start the Good Technology Connect service on your disaster recovery Connect instance.

Using friendly names for certificates in Presence

The friendly name of a certificate can be helpful when multiple certificates with a similar subject exist in a certificate store. Friendly names are properties in the X.509 certificate store that associate aliases with certificates so they can be easily identified.

You can restrict certificates used for BlackBerry Presence to a friendly name by completing the following actions

1. If you do no have one, create and enroll a certificate.
2. Change the certificate friendly nand description.
3. Setting the new certificate friendly name string value in the BEMS Lync Presence Provider (LLP) service configuration file (LyncPresenceProviderService.exe.config).

If you do not already have a certificate, you can create and verify a BEMS SSL certificate for Lync. For more information, see Create and add the BEMS SSL certificate for Microsoft Lync Server 2010, Microsoft Lync Server 2013, and Skype for Business.

Change the certificate friendly name description

1. Open the Microsoft Management Console (MMC).
2. Click **Console Root**.
3. Click **File** > **Add/Remove Snap-in**.
4. In the **Available snap-ins** column, click **Certificates** > **Add**.
5. Select **Computer account**. Click **Next**.
6. Select **Local Computer**. Click **Finish**.
7. Click **OK**.

8. Click **Certificates (Local Computer)** > **Personal** > **Certificates**.
9. Double-click the certificate you want to change.
10. Click the **Details** tab.
11. In the **Show** drop-down list, click <**All**>.
12. Click **Edit Properties**.
13. In the **Friendly name** field, type a friendly name.
14. In the **Description** field, type a description.
15. Click **Apply**.
16. Click **OK**. Click **OK** again.

After you finish: Specify the certificate's friendly name in the configuration file for the Connect service.

Add the certificate friendly name to the Presence server configuration file

Before you begin: Specify the certificate friendly name.

1. In a text editor, open the **LyncPresenceProviderService.exe.config** file. By default, the LyncPresenceProviderService.exe.config file is located in <*install path*>\Technology\BlackBerry Enterprise Mobility Server \BlackBerry Presence\.
2. At the end of the file, type <**add key**="**RESTRICT_CERT_BY_FRIENDLY_NAME**" **value**="<***cert_friendly_name***>"/>. The cert_friendly_name is case sensitive.
3. Save your changes.
4. Start the Good Technology Presence service.

Troubleshooting Good Presence Issues

Finding log files

By default, a server log file is created for each BEMS server and is stored daily on the computer that hosts BEMS.

BEMS names the log files gems_<*server_name_time stamp*>.log.

By default, the BEMS log files are stored daily in C:\BlackBerry\bemslogs.

Note: The timestamp is reset daily at 0:00. It is also reset each time that the service is restarted and when the file size is a maximum of 100 MB.

By default, the BEMS Presence log files are stored in C:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Presence\Logs\

Global catalog for Connect and Presence

7

The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multi-domain Active Directory Domain Services (AD DS) forest. global catalogs are typically used in a single AD DS forest that has more than one domain. A global catalog provides a way for products and services to access data that is available in other domains in the same forest. For more information about global catalogs, visit the Technet Library to see What Is the Global Catalog?.

You can configure the Connect service to use the global catalog so that the Connect service can find users who exist in other domains within your AD DS forest. This enables the BlackBerry Connect app to search for people in those other domains and start conversations with them, or add them to the contact list. For instructions on configuring the Connect service to use the global catalog, see Enable BlackBerry collaboration suite users from multiple domains within the same forest.

You can also configure the Presence service to use the global catalog so that the Presence service can subscribe the receive presence information for Lync users who exist in other domains within your AD DS forest. This is helpful if you are using a Presence client, such as BlackBerry Work, by users who email with others who reside in other domains in your AD DS forest. For instructions on configuring the Presence service to use the global catalog, see Prerequisites: Connect for Microsoft Lync Server and Skype for Business.

To provide this service, in addition to configuring the Connect and Presence services to use the global catalog, you must replicate a couple of additional Lync related attributes to the global catalog. Whether this is for one or both services, this only needs to be done once.

Enable Lync related attributes to the global catalogue

Complete this task on the Domain controller in your environment.

1. Open the Run command.
2. Type **schmmgmt.msc**. Press **Enter**.
3. In the left navigator window, click **Active Directory Schema**.
4. In the middle window, double-click **Attributes**.
5. Double-click **Mail**.
6. Select the **Replicate this attribute to the Global Catalog** checkbox. Click **OK**.
7. Repeat steps 5 and 6 for the attribute **msRTCSIP-PrimaryUserAddress**.

8. Repeat steps 5 and 6 for the attribute **msRTCSIP-UserEnabled**.

Updating the Connect and Presence services using Lync Director

8

The Lync Director role provides functionality for users accessing the Microsoft Lync Server, internally and externally. For more information about the Lync Director, visit the Technet Wiki and see Lync Director.

To support this capability, the Microsoft Lync Server is deployed as one or more pools, based on Standard Edition or Enterprise Edition Microsoft Lync Server. Users can be homed on only a single pool. Clients can be configured to find their Lync pool automatically. However, the DNS records that support this functionality can point to only a single pool. In a multi-pool environment, this "primary" pool will have to redirect users to their correct home pool. This is an overhead on the primary pool. The Lync Director is used to offload this redirection functionality. The Director does not home any users itself but instead redirects the user to their correct pool home. The requirement for the Lync Director is therefore for multi-pool environments with high user numbers.

Once the user has been redirected to their correct pool, the Lync Director plays no further role in communications between the client and the pool server.

Specify the Connect and Presence services to use a Lync Director

1. On the BEMS host, stop the **BlackBerry Connect** service and the **BlackBerry Presence** service.
2. Complete the following actions:

Task	Steps
Update the BlackBerry Connect configuration file	1. On the BEMS host, navigate to the GoodConnectServer.exe.config file. By default, the GoodConnectServer.exe.config file is located in <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Connect. 2. In a text editor, open the GoodConnectServer.exe.config file.
Update the BlackBerry Presence configuration file	1. On the BEMS host, navigate to the LyncPresenceProviderService.exe.config file. By default, the LyncPresenceProviderService.exe.config file is located in <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Presence.

Task	Steps
	2. In a text editor, open the LyncPresenceProviderService.exe.config file.

3. Locate the LYNC_SERVER key and update the value with the FQDN of the Director pool that you want to us.
4. On the BEMS host, start the Good Technology Connect service and Good Technology Presence service.

Configuring the BlackBerry Docs service

9

You use the BEMS dashboard to configure and maintain document/file repositories (for example, file shares, Microsoft SharePoint, Box, and CMIS-supported content management systems) and user access policies for mobile app users of the service.

When you configure the BlackBerry Docs service, you configure the following components:

1. Configure the Web Proxy.
2. Configure the Database.
3. Confirm the Repositories.
4. Configure storages.
5. Configure the Settings.
6. Configure Audit.

Configure a web proxy server for the Docs service

If you use a web proxy to connect your enterprise servers to the Internet for Microsoft SharePoint and Microsoft Office Web Apps (OWAS), you must enable Use Web Proxy and configure its address, port, and authentication type for the Docs service.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **Good Services Configuration**, click **Docs**.
2. Click **Web Proxy**.
3. Select the **Use Web Proxy**.
4. In the **Proxy Address** field, type the FQDN of the web proxy server.
5. In the **Proxy port** field, type the port number of the proxy server.
6. In the **Proxy Server Authentication Type** drop-list, click an authentication type. If you select Basic or NTLM authetication, enter the required login credentials.
7. Click **Test** to verify the connection to the proxy server.
8. Click **Save**.

Configure the database for the BlackBerry Docs service

In configuring your Microsoft SQL Server database for BEMS-Docs, you have a choice of using either Windows Authentication or SQL Authentication for granting access to the database by BEMS. After restarting the Good Technology Common Services, perform the steps below for either Windows Authentication or SQL Authentication.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Database**
3. Enter the Microsoft SQL Server name and password.
4. In the **Authentication Type** drop-down list, select one of the following options:.
    - If you select **Windows Authentication**, the credentials for the Windows service account configured for the BlackBerry Connect service are used.
    - If you select **SQL Server Login**, enter the Microsoft SQL Server username and password.
5. Click **Test** to verify the connection with the Microsoft SQL Server database.
6. Click **Save**.
7. Restart the Good Technology Common Services service.

Repositories

The Docs service furnishes your end users with access to stored enterprise data from their mobile devices. A Docs repository (also called a "share") lives on an enterprise server containing files shared by authorized users.

Before you configure your repositories, complete the initial configuration of your Security Settings, and then configure Good Control to entitle your users so that they can access the repositories you add and define later from their devices. With respect to Docs, see Managing Repositories for detailed guidance on setting up and maintaining your enterprise shares in BEMS and the associated user access.

Storages

The Docs service supports a number of storage services, including File Share, Microsoft SharePoint, Box, and CMIS-based providers such as Alfresco, Documentum, HP RM, IBM Filenet, etc.

The Docs service supports the ability to add or delete access to any of these storage providers and their repositories from BEMS.

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

Configure the Docs security settings

Docs security settings control acceptable Microsoft SharePoint Online domains, the URL of the approved Microsoft Office Web Apps (OWAS), the appropriate LDAP domains to use, and whether you want to use Kerberos constrained delegation for user authentication. Delegation allows a service to impersonate a user account to access resources throughout the network. Constrained delegation limits this trust to a select group of services explicitly specified by a domain administrator.

Before you begin: Kerberos constrained delegation for the BlackBerry Docs service is configured in your environment. For instructions, see Configuring Kerberos constrained delegation for Docs

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Settings**.
3. Select the **Enable Kerberos Constrained Delegation** checkbox to allow Docs to use Kerberos constrained delegation.
4. Separated by a comma, enter each of the Microsoft SharePoint Online domains you plan to make available. For more information, see Configuring support for Microsoft SharePoint Online and Microsoft OneDrive for Business.
5. Enter the URL for your approved **Office Web App Server**.
6. Provide you Microsoft Active Directory user domains (separated by commas), then enter the corresponding **LDAP Port**. LDAP (Lighweight Directory Access Protocol) is used to look up users and their membership in user groups.
7. Select the **Use SSL for LDAP** checkbox for secure communication with your Microsoft Active Directory servers.
8. Add the **Workspaces Public Key**. Adding the public key allows BEMS and the BlackBerry Workspaces server to communicate with each other. For more information about locating the public key, see the Workspaces Appliance-X content.
9. Click **Save**.
10. Restart the Good Technology Common Services for the changes to take effect.

Configure your Audit properties

Your Audit settings enable or disable Docs service audit logs. If audit logs are enabled, then actions are logged to the database, including user downloads, deletions, browsing history, and files created.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.

2. Click **Audit**.
3. On the **Audit Settings** tab, select the **Enable Audit Logs** checkbox.
4. In the **Audit Operations** section, select the audit operations you want the logs to include logging for.
5. Click **Save**. It can take up to two minutes for the changes to take effect.
6. On the **Audit Purge** tab, in the **Purge audit logs from the database before** field, select a purge-before date. Click **Purge** to remove audit records logged to the database earlier than the purge date selected.

After you finish:

Configure Good Control to entitle your users, using application groups, to use the Docs service. Following user entitlement, see Managing Repositories to set up your file shares, SharePoint sites, and Box storage.

Configuring Docs for Active Directory Rights Management Services

Active Directory Rights Management Services (AD RMS) from Microsoft allows documents to be protected against access by unauthorized people by storing permissions to the documents in the document file itself. Access restrictions can thus be enforced wherever the document resides or is copied or forwarded to. For documents to be protected with AD RMS, the application the document is associated with must be RMS aware. For more information about AD RMS, visit the Technet Library to see Active Directory Rights Management Services Overview. This page also lists limitations to the technology including not being able to restrict content from being copied using third-party screen capture programs.

In Docs/BlackBerry Work, support for RMS protected documents is provided through the Microsoft Office Web Apps server with viewing and editing enabled through the BlackBerry Access browser. Note that while BlackBerry Access browser is a BlackBerry Dynamics application with all the secure features it provides, it has only partial support support for RMS features. For example, users might be able to do the following in BlackBerry Access which might not be possible with RMS aware client:

- Share the Microsoft Office Web Apps URL that is used to render the document viewing/editing with other BlackBerry Dynamics applications. The URL expires in thirty minutes but during this time, other BlackBerry Dynamics applications might be able to access it without any authentication. For example, if shared with Good Work, the URL can be emailed to others. If shared with a BlackBerry Dynamics application allows printing, then page that is rendered might be printed. Mitigation would be to enable user agent in BlackBerry Access policy and then use it to create filtering rules in Microsoft Office Web Apps server so that only BlackBerry Access is able to access the URL. The Microsoft IIS URL Rewrite extension can be used to create the rules.
- Users can save what is on screen as a web clip and this screenshot file can be shared with other BlackBerry Dynamics applications. Mitigation is to disable web clips in BlackBerry Access policy.
- When editing a document, copy and paste of content would be possible but by default polices only within the BlackBerry Dynamics secure container environment. Ensure that the protection provided is adequate given these limitations and satisfies your RMS protection requirements before enabling this support.

Rights Management Services restrictions

The following Rights Management Services (RMS) restrictions are respected by the Docs service:

- View right is required to view documents.
- Edit right is required to edit documents.
- Print or Export rights are required to convert documents to PDF.
- If a user is the owner of a document and the "Grant owner full control" right is set, then viewing, editing, and converting to PDF is allowed.
- If the current date is beyond the content expiry date, then no access to the document is allowed except when the user is owner and the "Grant owner full control" right is set.
- Revocation of rights is respected.
- Use licenses are acquired on every use of the document.
- Both template-based and custom protection on documents are honored.

Docs deployment for Active Directory Rights Management Services support

1. On the computer that hosts BEMS, install the Rights Management Services Client 2.1. To download the client, visit www.microsoft.com/downloads and search for ID=38396.
2. If using self-signed certificates in AD RMS server, add the SSL certificate for https://<*AD RMS server URL*> to trusted CA list.
3. In Internet Explorer, add https://<*AD RMS server URL*> to the Local Intranet site list.
4. Install the Docs service with BEMS common services service running as a domain user.
5. If a super users group is not already configured in AD RMS server, configure one. Then add BEMS process user (BEMS common services service user) to this AD RMS super users group.
6. On the AD RMS server, find the file %systemdrive%\Inetpub\wwwroot_wmcs\Certification\ServerCertification.asmx and add Read and Read & Execute permissions for the following:
    - the "AD RMS Service Group".

      Note: The AD RMS Service Group is a local group and not a domain group.
    - the computer account for each of the BEMS servers.
    - The BEMS common services service user.

Configuring Good Control for Docs service

When you configure Good Control for the Docs service, you perform the following actions:

1. Entitle users, configure the Docs service entitlement.
2. Add the BEMS server to Good Control.
3. Publish the Docs app.
4. Configure user affinity.

Entitle users, configure the Docs service entitlement

1. In Good Control, under **Apps**, click **Manage Apps**.
2. On the **Enterprise** tab, in the **Filter Name** field, type a search string for "Feature - Docs Service Entitlement".
3. In the search results, click **Feature - Docs Service Entitlement**.
4. Click the **BlackBerry Dynamics** tab.
5. Beside the **GD Entitlement ID** section, click **Edit**.
6. In the **Policy Set Override** drop-down list, select a policy that you want to override the default policy.
7. Click **Save**.

Configure the Docs service entitlement, add BEMS to Good Control

1. In Good Control, under **Manage Apps**, click **Apps**.
2. On the **Enterprise** tab, in the **Filter Name** field, type a search string for "Feature - Docs Service Entitlement".
3. In the search results, click **Feature - Docs Service Entitlement**.
4. Click the **BlackBerry Dynamics** tab.
5. Beside the **Server** section, click **Edit**.
6. Add the computer that hosts BEMS and port 8443.
7. Click **Save**.

Publish the Docs app for all users

When you publish the Docs app, you publish it for all users.

1. In Good Control, under **Apps**, click **App Groups**.
2. Beside the **Everyone** group, click .
3. Beside **Entitled enterprise apps**, click .
4. Select the **Feature - Docs Service Entitlement - ALL** checkbox.
5. Click **OK**.

Enable server affinity for Docs in BlackBerry Work

CAUTION: When a distributed computer system is load balanced, each request is routed to a different server. This load balancing approach is diminished when server affinity techniques are applied. If you set affinity, it takes precedence.

1. In Good Control, under **Policies**, click **Policy Sets**.
2. Click the policy you want to apply.
3. Click the **Apps** tab.
4. Expand **App Specific Policies**.
5. Click **BlackBerry Work** or **Good Control**.
6. Click the **App Settings** tab.
7. Under **Preferred Docs Server Configuration**, in the **Server Hosts** field, type the FQDN of the computer that hosts BEMS and a colon followed by port 8443. For example, *<FQDN of the GEMS server>*:8443.

   You can add additional preferred servers. Each server you add must be separated with a comma and no spaces.
8. Click **Update**.
9. Repeat steps 1 to 6 for each policy that you want to use with the Docs service.

Configuring the Docs instance for high availability

When you configure Docs for high availability, you perform the following actions:

1. Configure each new Docs instance to use the existing database.
2. Configure each new Docs instance to point to the same Good Proxy server.

3. Whitelist each new Docs server host and port in Good Control.
4. Configure each new Docs instance in Good Control for the BlackBerry Work app.For more information about entitlements and to configure the Docs instance in BlackBerry UEM and to configure Docs for BlackBerry Work, see the BlackBerry UEM and BlackBerry Dynamics Getting Started content

Configuring the Docs service for disaster recovery

Disaster Recovery for Docs is based on an active/warm standby clustering model.

Before you add a Docs instance for disaster recovery, you complete the following actions:

1. Evaluate the disaster recovery strategy for your network resources such as File Share, Microsoft SharePoint, Microsoft Office Web Apps (OWAS), and so forth, then make sure your network resources are accessible from your disaster recovery site in the event a disaster recovery situation arises.
2. Configure database replication for the Docs database from your primary site to your disaster recovery site. SQL log shipping is recommended. Consult your database administrator for assistance.
3. Ensure that the appropriate network ports are open to allow Docs servers in your disaster recovery site to communicate with the database, network resources, and Good Proxy servers in your disaster recovery and Primary sites.

Add a new Docs instance for disaster recovery

High availability for the Docs service is based on clustering. The Docs service supports high availability by adding additional computers hosting BEMS and running the Docs service in a cluster.

1. Configure your disaster recovery Docs instance to use the Docs database in your primary site.
2. Configure your disaster recovery Docs instance to use the primary Good Proxy server in the cluster.
3. Whitelist your disaster recovery computer hosting the Docs service and port in Good Control. For instructions, see In Good Control, whitelist BEMS .
4. Configure your disaster recovery Docs instance in Good Control for the BlackBerry Work App. For instructions, see Add BEMS to the BlackBerry Work application server list. Make sure the **Priority** is set to **Secondary** or **Tertiary**.

After you finish: After the disaster recovery Docs instance is installed and configured, stop the Good Technology Common Services. This places the disaster recovery Docs instance in warm standby.

Failover in disaster recovery

1. Stop the BlackBerry Common Services on all your Primary Docs instances

2. Failover your Docs database on your database server (for example, make the Docs database in your disaster recovery site active).
3. Failover your database FQDN DNS to your disaster recovery database server.

   If you were not able to failover the database DNS, then you must login to the BEMS Dashboard and update the Docs database information to point to your disaster recovery database server. Restart the BlackBerry Common Services for the new database settings to take effect.
4. Start the Good Technology Common Services on your disaster recovery Docs instance.
5. If you also failed over your Good Proxy servers in this process, you must update the Good Proxy information in the BEMS Dashboard for the Docs service.

Managing Repositories

10

BEMS has the following repository storage providers:

Storage repository	Description
File Share	A secure directory on an enterprise file server containing shared files and sub-directories which can be remotely accessed.
SharePoint	A secure web server containing shared files which are accessed via the Internet.
Box	A secure cloud storage account furnished by box.com containing shared files which can be accessed via the Internet.
CMIS-based	Content Management Interoperability Services (CMIS) is an open standard that allows different content management systems to inter-operate over the Internet.

A repository is further categorized in the Docs service by who added and defined.

Storage repository	Description
Admin-defined	Storage provider sites added and maintained by BEMS administrators to which individual users and user groups are granted access.
User-defined	Sites added by individual end users from their mobile devices to which you, as the BEMS administrator, may rescind and reinstate mobile-based access in accordance with your enterprise IT acceptable-use policies.

Configuring repositories

The Repository configuration page has the following three tabs that you can configure:

Tabs	Description
Admin defined	Allows you to create and manage repositories, add and remove users and user groups, and assign users and user groups file access and use permissions.
User defined	Allows you to add and remove users and user groups, enable and disable user and user group the ability to create user-defined shares, and grant and rescind permissions to perform a range of file-related actions on their user-defined shares.

Tabs	Description
Users	Allows you to search for a user in a Microsoft Active Directory domain to view the repositories permitted by path or override, and who defined the share (for example, admin or user).

Admin-defined shares

Shares are document repositories for a particular storage provider. You can further organize your administrator-defined shares into lists. A named (defined) share, however, can only belong to one list. This is enforced to help you avoid unwanted or unintended duplication.

When you define repositories and lists, you perform the following actions:

Step	Action
1	Define a repository.
2	Define repository list.
3	define user and user group access permissions.

Granting User Access Permissions

Access permissions are defined for a single repository or inherited from an existing list of repositories. Permissions can be selectively granted to existing Microsoft Active Directory domain users and user groups. At least one user or user group must be added to the repository definition to configure access permissions.

The following table lists the access permissions and the default setting that are available.

Permission	Permissions Attributes	Default setting
List (Browse)	View and browse repository content (for example, subfolders and files) in a displayed list, and sort lists by Name, Date, Size, or Kind	Enabled
Delete Files	Remove files from the repository.	Enabled
Read (Download)	Download repository files to the user's device and open them to read	Enabled

Permission	Permissions Attributes	Default setting
Write (Upload)	Upload files (new/modified) from user's device to the repository for storage	Enabled
Cache (Offline Files)	Temporarily store a cache of repository files on the device for offline access	Enabled
Open In	Open a file in a format-compatible app on the device	Enabled
Create Folder	Add new folders to the repository	Enabled
Copy/Paste	Copy repository file content and paste it into a different file or app	Enabled
Check In/Check Out	When a file is checked out, the user can edit, close, reopen, and work with the file offline. Other users cannot change the file or see changes until it is checked back in	Enabled (SharePoint only)

Change administrator access permissions

1. On the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Repositories**.
3. Click the **Admin Defined** tab.
4. Click a repository or list.
5. Under **Access Permissions**, beside the user or user group, select or clear the permission checkbox that you want to change.
6. Click ⊗ beside a user or user groups that you want to remove.
7. Click **Save**.

Define a repository

Microsoft Active Directory users and groups must be added to a repository definition or a list definition before access permissions can be configured. Users and groups added automatically receive the default access permissions.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Repositories**.
3. Click the **Admin Defined** tab.
4. Click **New Repository**.

5. In the **Display Name** field, type the name of the repository to that will be displayed to users granted mobile access to the repository.

   The repository name must be unique and can contain spaces. The following special characters cannot be used due to third-party limitations:

   - Microsoft SharePoint 2007, Microsoft SharePoint 2010, Microsoft SharePoint 2013, and Microsoft SharePoint 2016: ~ " # % & * : < > ? / \ { | }
   - File Share: \ / : * ? " < > |
   - Box: \ /|

6. In the **Storage** drop-down list, select a storage provider.

   If you select **SharePoint**, and the share is running SharePoint 2013 or later, select the **Add sites followed by users on this site** checkbox to make this feature available to users of this share. It will only work, however, if SharePoint's MySite plugin is enabled.

7. In the **Path** field, specify the path to the share.

   - If you select **File Share** as the storage type, Path can include Microsoft Active Directory attributes. For example, \\fileshare1\<*SAMAccountName*> or <*homeDirectory*>.
   - If the Storage type is **SharePoint** or **Box**, enter a fully qualified URL with or without Microsoft Active Directory attributes.
   - For storage providers using CMIS support that you have added to BEMS, both AtomPub and Web Services web addresses are supported. A repository ID may be optionally specified and a path inside the repository may also be optionally specified. If no repository ID is specified, then all repositories that a user has access to are listed to the user. If no path is specified, then the listing starts at the repository root. Following is the format of the paths for BEMS Docs repositories for accessing CMIS repositories:

     <*ATOM-PUB-URL*>?RepositoryId=<*REPOSITORY-ID*>&RelativePath=<REPOSITORY-PATH>

     <*WEB-SERVICES-URL*>?RepositoryId=<*REPOSITORY-ID*>&RelativePath=<REPOSITORYPATH>&BindingType=WebService

     - Where ATOM-PUB-URL and WEB-SERVICES-URL is specific to the CMIS vendor. Contact your CMIS vendor for more information.
     - REPOSITORY-ID is the CMIS repository ID (optional).
     - REPOSITORY-PATH is the path inside the CMIS repository (optional).

8. Optionally, in the **List** drop-down list, select an existing list to which you want this repository to belong. If no list is defined, you can create one later or leave this field blank.
9. If a List is selected, select the **Enable inheriting of access control of repository list** checkbox to apply the Access Permissions of the List to the repository. If the checkbox is not selected, you must define specific access permissions for this share (repository).
10. In the **Access Permissions** section, click **Add Users/Groups**.

11. In the **Search In** field, enter a new domain or keep the default domain.
12. Select **Users** or **Groups**.
13. In the **Search for Users in Active Directory** field, type a full or partial search string. Click **Search**.
14. In the search results, select one or more entries.
15. Optionally, select the **Use Different Credentials** and enter a username and password to configure a different Username and Password for accessing this repository by these users.
16. Click **Add**.
17. Click **Save**.

Change a repository

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Repositories**.
3. Click the **Admin Defined** tab.
4. Click a repository you want to change.
5. Make the required changes.
6. Click **Save**.

Define a Repository List

Use Lists to assign users to multiple repositories and to organize your repositories by common characteristics. This allows you to batch-configure user access permissions. Included repositories can inherit the configured user access permissions of the list or maintain permissions independent of the list.

Microsoft Active Directory users and groups must be added to a repository definition or a list definition before access permissions can be configured. Users and groups added automatically receive the default access permissions.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Repositories**.
3. Click the **Admin Defined** tab.
4. Click **New List**.
5. In the **Display Name**, enter the name that will be displayed to authorized users on their mobile devices.
6. In the **Select Repositories to include** field, select the defined repositories to include.
7. Click **Save**.

After you finish:

1. Add new users and groups to the list definition.
2. Grant user access permissions.

Add users and user groups to repositories and list definitions

Microsoft Active Directory users and groups must be added to a repository definition or a list definition before access permissions can be configured. Users and groups added automatically receive the default access permissions.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Repositories**.
3. On the **Repositories Configuration** page, click the **Admin Defined** tab.
4. Click a repository or list.
5. Under **Access Permissions**, click **Add Users/Groups**.
6. In the **Search In** field, enter a new domain or keep the default domain.
7. Select **Users** or **Groups**.
8. In the **Search for Users in Active Directory** field, type a full or partial search string. Click **Search**.
9. In the search results, select one or more entries.
10. Optionally, select the **Use Different Credentials** checkbox and enter a username and password to configure a different username and password for accessing this repository by these users.
11. Click **Add**.

After you finish: Grant user and user groups access permissions.

Allow user-defined shares

You can allow users to define their own "named" data sources on admin-defined repositories for which they have already been granted permission.

When you allow users to define their own repositories, you perform the following actions:

1. Enable user-defined shares permissions
2. Change user access permissions

Enable user-defined shares permissions

1. In the **Good Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.

2. Click **Repositories**.
3. Click the **User Defined** tab.
4. Select the **Enable 'User Defined Shares'** checkbox to allow your mobile users to define their own data sources.
5. Optionally, select the **Automatically add sites followed by users** checkbox for authorized Microsoft SharePoint 2013 repositories with the required MySite plugin enabled.
6. Under **Storages** section, select one or more storages.
   At least one storage option must be selected or the entire user-defined option is disabled.
7. Under **Access Permissions** section, click **Add Users/Groups**.
8. In the **Search In** field, enter a new domain or keep the default domain.
9. Select **Users** or **Groups**.
10. In the **Search for Users in Active Directory** field, type a full or partial search string. Click **Search**.
11. In the search results, click one or more entries.
12. Optionally, select the **Use Different Credentials** and enter a username and password to configure a different Username and Password for accessing this repository by these users.
13. Click **Add**. The users and groups added automatically receive the default access permissions.
14. Click **Save**.

Access permissions

Permissions can be selectively granted to existing Microsoft Exchange ActiveSync domain users and user groups. The most restrictive permissions (admin-defined or user-defined) are applied.

The following table lists the permissions that are provided by default when you add users and groups to the User-defined shares

Permission	Permissions Attributes	Default setting
List (Browse)	View and browse repository content (for example, subfolders and files) in a displayed list, and sort lists by Name, Date, Size, or Kind	Enabled
Delete Files	Remove files from the repository.	Enabled
Read (Download)	Download repository files to the user's device and open them to read	Enabled
Write (Upload)	Upload files (new/modified) from user's device to the repository for storage	Enabled

Permission	Permissions Attributes	Default setting
Cache (Offline Files)	Temporarily store a cache of repository files on the device for offline access	Enabled
Open In	Open a file in a format-compatible app on the device	Enabled
Create Folder	Add new folders to the repository	Enabled
Copy/Paste	Copy repository file content and paste it into a different file or app	Enabled
Check In/Check Out	When a file is checked out, the user can edit, close, reopen, and work with the file offline. Other users cannot change the file or see changes until it is checked back in	Enabled (SharePoint only)
Add New Repositories	Permits new repositories to be added from the user's mobile device.	Disabled

Change user access permissions

1. On the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Repositories**.
3. Click the **User Defined** tab.
4. Under **Access Permissions**, beside the user or user group, select or clear the permission checkbox that you want to change.
5. Click ⊗ beside a user or user groups that you want to remove.
6. Click **Save**.

View user repository rights

In some scenarios, you may need to search for a particular user to review which repositories are configured for their access, as well as the specific permissions granted. For example, when a user is one member of a Microsoft Active Directory group configured for repositories and is not listed individually in your admin-defined or user-defined repository configurations and you want to consider making specific changes to the user's access permissions.

1. In the **Good Enterprise Mobility Server Dashboard**, under **Good Services Configuration**, click **Docs**.
2. Click **Repositories**.

3. Click the **Users** tab.
4. In the **Search Users** field, begin typing the user's Microsoft Active Directory account name. If you don't see the user you want, extend or narrow the search string or click **Switch Domains** to search a different Microsoft Active Directory domain.
5. Click the user name. The **Defined by** column specifies if the repository is admin-defined or user-defined.
6. Click the name of the repository or on the row to view the user's access permissions.
7. Optionally, in the **Override Path for this user** field, enter an override path.

Enable users to access Box repository using a custom Box email address

On the Home screen of the computer hosting BEMS, complete one of the following actions:

Attributes	Task
The Box email address matches one of the following Microsoft Active Directory attributes: • mail • userPrincipalName • proxyAddresses • targetAddress	No action is required.
The Box email address matches a Microsoft Active Directory attribute other than the attributes listed above.	Set the config value, **LDAPUserCheckAttribute**, to specify the Microsoft Active Directory attribute that contains the custom Box email address. 1. On the computer hosting BEMS, open a command prompt and navigate to the client.bat file. By default, the file is located at <*drive*>:\Program Files \BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution \gems-quickstart-<*version*>\bin. 2. Type **client.bat -u *domain name**username***. Press **Enter**. • Where *domain name* is the name of the domain BEMS is located in. • Where *username* is the name of an administrator account on BEMS. 3. Type the password for the BEMS user account. Press **Enter**. 4. Set the LDAPUserCheckAttribute. Type **docs:config *Config-Name Config-Value***.

Attributes	Task
	• Where *Config-Name* is LDAPUserCheckAttribute. • Where *Config-Value* is the name of the Microsoft Active Directory attribute you want to add. For example, BoxLogin. 5. Optionally, confirm the *Config-Value* is set. Type **docs:config *Config-Name***
The Box email address does not match any Microsoft Active Directory attribute.	Complete one of the following tasks: • Add an attribute to contain the Box email address and use the previous configuration. See the instructions above. • Enable the EnablePersonalBoxAccess config value to allow users to use personal Box email addresses without adding an attribute. **Warning:** If you use this method to allow users to use custom Box email addresses to access Box, users can copy documents from your organization's network to their private Box accounts. 1. On the computer hosting BEMS, open a command prompt and navigate to the client.bat file. By default, the file is located at <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<*version*>\bin. 2. Type **client.bat -u *domain name**username***. Press **Enter**. 3. Type the password for the BEMS administrator account. Press **Enter**. 4. Set the EnablePersonalBoxAccess to 1 to enable the attribute. Type **docs:config EnablePersonalBoxAccess 1**. 5. Optionally, confirm EnablePersonalBoxAccess is enabled. Type **docs:config EnablePersonalBoxAccess**.

Using the Docs Self-Service web console

Similar to the method for adding user-defined repositories on and from the device (see "Adding a New Data Source" in the respective BlackBerry Work Client User Guide for iOS or Android), authorized users can login to a Docs Self-Service web console from a browser on their office workstation or laptop to add user-defined File Share, Box, and SharePoint repositories. The self-service console is included in your BEMS installation and automatically configured with the Docs service in the BEMS Dashboard.

The web address is http://<*bems_fqdn*>:<*port*>/docsconsole. Contact your BEMS/BlackBerry Work administrator for the specific web address in your environment.

Log in to the Docs Self-Service web console

1. In your computer browser, open a browser and navigate to the Docs Self-Service console at **http://<*bems_fqdn*>:<*port*>/docsconsole**.
2. On the login webpage, type your username, password, and domain name.
3. Click **Add Repository** to define a new data source.
4. In the **Display Name** field, type a display name. This name is displayed in repository lists in the console and on your device.
5. In the **Storage Type** field, select a storage type. For example, File Share, SharePoint, or Box (iOS).
6. In the **Path** field, enter the path.
7. Click **Save**.

Remove a user-defined repository using Docs Self-Service

Before you begin: One or more user-defined repositories.

1. In your computer browser, open a browser and navigate to the Docs Self-Service console at **http://<*bems_fqdn*>:<*port*>/docsconsole**.
2. On the login webpage, type your username, password, and domain name.
3. Click ⊗ beside the repository you want to remove.

Add a CMIS storage service

11

BEMS is installed with support for a number of storage service providers: FileShare, SharePoint, and Box. You can also add storage services that utilize the Content Management Interoperability Services (CMIS) protocol, an open standard that allows different content management systems to inter-operate over the Internet. CMIS supports such storage services as Alfresco, Documentum, HP RM, IBM Filenet, etc.

1. In the **Good Enterprise Mobility Server Dashboard**, under **Good Services Configuration**, click **Docs**.
2. Click **Storages**. A list of storage providers is displayed.
3. Click **New Storage**.
4. In the **Storage name** field, type a name for the storage.
5. In the **Storage provider** drop-down list, select an authentication provider. For example, CMIS.
6. In the **Authentication Provider** drop-down list, select the provider.
7. To make the storage available on user devices, select the select the **Enable Storage** checkbox.

   Note: It may take up to an hour or a restart of the apps for storage changes to take effect on user devices. It may take up to five minutes for the changes to take effect on the server. Enabling and disabling storage providers on this page affects what storage resources are visible at any given time for users, but has no such impact on the server.

After you finish: Add repositories in the storage provider. For instructions, see Managing Repositories

Windows Folder Redirection (Native) 12

This feature gives administrators the ability to redirect the path of a folder to a new location, which can be on the local computer or a directory on a network file share. Users can work with documents on a server as if the documents were based on a local drive. The documents in the folder are available to the user from any computer on the network.

Folder Redirection is located under **Windows Settings** in the console tree when you edit a domain-based Group Policy using the Group Policy Management Console (GPMC). The path is <*Group Policy Object Name*>\User Configuration\Policies\Windows Settings\Folder Redirection.

Offline File technology (turned on by default) gives users access to the folder even when they are not connected to the network, and is especially useful on laptops and mobile devices. Offline folders do not, however, work out of the box with Samba network drives. See Offline Folders (Native) for details. Otherwise, Windows Folder Redirection can be enabled for any of the predefined folders in the Group Policy Management Editor.

In Windows Server 2008, a total of 13 different folders can be redirected.

- AppData (Roaming)
- Desktop
- Start Menu
- Documents
- Pictures
- Music
- Favorites
- Contacts
- Downloads
- Links
- Saved Games
- Searches
- Videos

As an administrator, you must create the root folder for the destination location. This folder can be created on a local or remote machine (NAS).

Note: All members of the group who have Windows Folder Redirection enabled must have full access to the root folder.

Enable folder redirection and configure access

When you enable folder redirection the user's folder will have exclusive user permissions. Other users cannot see the files. The user can update, add new, and delete files. When the user connects to the corporate network, the files are automatically synchronized with the redirected location.

If modifications are made on the file in both locations at the same time, an alert is issued, and the user is responsible for resolving the conflict; for example, keep the source, keep the destination, or keep both files).

If a user uploads a file through a mobile app directly to the share, the file is visible on the local computer in the Documents folder. Moreover, when the Docs service is configured with "User Private Shares" pointing to the redirected root folder—for example, C:\RedirectShare\— users can automatically use their own folders inside the mobile app from the "Home Directory" on their phone or tablet.

Note: Users with their home folder defined in Microsoft Active Directory, Folder Redirection works when the redirection path is the same as the user's home folder in Microsoft Active Directory.

1. Create a root folder (for example, RedirectShare) for the redirect destination.
2. In the **Group Policy Management Editor**, select a specific folder (for example, Documents) and add one or more rules to determine which users and user groups can redirect the selected folder to the root folder.
3. Set an environment variable **%USERNAME%** to the path [*Root*]\<*username*>\Documents\.

Local Folder Synchronization – Offline Folders (Native)

13

Users who work remotely on content creation and save files locally for offline access, can now access these files on-the-go from their mobile devices without having to open their local machine. The Docs service provides authorized users access to their Home Directory hosted on network-attached storage (NAS) shares and exposed through Microsoft Active Directory. This synchronization feature, synching folders on the user's remote laptop or desktop with their home directory, is only available on local machines running Microsoft Windows.

When you select a network file or folder to make it available offline, Windows automatically creates a copy of that file or folder on your computer. Thereafter, any time you reconnect to the network folder, Windows synchronizes these files with those in the network folder. You can also synchronize them manually any time you want. As pointed out above, this feature does not work out of the box with a Samba network drive, and workarounds are not currently supported by Microsoft. Otherwise, the feature can be enabled from Windows Explorer and used for any shared folder as pictured.

Now that the shared folder is available offline, it can be used offline. Users can even make a shortcut to the shared folder on their desktop for convenience. When working offline and changes are made to offline files in a network folder, Windows automatically synchronizes the changes the next time you connect to that network folder. You can also manually synchronize changes by clicking the Sync Center tool .

Additionally, there are more advanced synchronization scheduling controls available in the Windows Sync Center.

If the user is working offline while someone else changes a file in a shared network folder, Windows synchronizes those changes with the offline file on the local computer the next time it connects to that network folder. If a synchronization conflict occurs, for example, changes were made to both the network and offline versions of the file between syncups, Windows prompts the user to confirm which change takes precedence.

Files that were cached automatically are removed on a least-recently used basis once the maximum cache size is reached. Files cached manually are never removed from the local cache. When the total cache size limit is reached and all files that were cached automatically have already been removed, files cannot be made available offline until you specify a new limit or delete files from the local cache by using the Offline Files control panel applet.

The default size limit for the Offline Files cache is 25-percent of the total disk space of the drive where the cache is located. The cache size can be configured through the Group Policy by setting the limit on disk space used by Offline Files—go to Computer Configuration > Policies > Administrative Templates > Network > Offline Files—on each client separately.

Synchronization takes place a few minutes after the user logs in and connects/opens a shared network folder containing offline files and is schedule- or event-based. However, this must still be enabled manually by each user. Even so, through the Group Policy editor, the domain administrator can set various synchronization triggers; e.g., On Logon, On Logoff, Sync Interval, etc.

these settings are available in User Configuration\Administrative Templates\Network\Offline Files and in Computer Configuration\Administrative Templates\Network\Offline Files in the Group Policy Object Editor snap-in. For more information about policy settings, see the Explain tab on the Properties page of each policy.

Folder Redirection and Offline Folders, provide the following advantages compared to a proprietary laptop/desktop agent furnished by Good:

- IT does not have to manage and deploy another desktop agent
- Microsoft Folder Redirection is integrated with GPO and manages conflicts
- Existing compliance tools and processes govern the data.

Once the files are synchronized to the "Home Directory," IT administrators can make use of the Docs service feature in which Microsoft Active Directory attributes can be specified in the path to expose the user's "Home Directory" to the BlackBerry Work app running on provisioned mobile devices. It is also important to remember that for users who have their home folder defined in Microsoft Active Directory, Folder Redirection works when the folder redirection path is the same as the user's home folder in Microsoft Active Directory.

Configuring support for Microsoft SharePoint Online and Microsoft OneDrive for Business

14

Microsoft SharePoint Online locations can be added as repositories in the Docs service just like an on-premise Microsoft SharePoint site to support both admin-defined and user-defined data sources. This is also true for Microsoft OneDrive for Business (ODfB).

Microsoft SharePoint Online furnishes two different ways for on-premises Microsoft Active Directory users to authenticate and perform normal SharePoint operations. These include:

- DirSync with Password Hash: Users and their passwords on Microsoft Active Directory are synchronized with Microsoft Office 365. Users are presented with a login page where they can enter their credentials to access Microsoft SharePoint Online.

  Active Directory Federation Service (ADFS): ADFS serves as a Secure Token Service. Behind the scenes (in background), users are redirected to ADFS for authentication and are issued security tokens that are then used by Microsoft SharePoint Online to sign in. Microsoft SharePoint Online users do not need to enter credentials when accessing from the corporate network, which typically enables sign sign-on scenarios.

Both authentication mechanisms are supported by the Docs service and all preparations take place on the server side exclusively. No device changes are required. The only prerequisite is that Microsoft SharePoint Online is already deployed based on either of the authentication mechanisms—DirSync with Password Hash or ADFS.

Configure Microsoft SharePoint Online and Microsoft OneDrive for Business

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Settings**.
3. In the **SharePoint Online** section, in the **SharePoint Online Domain** field, type the FQDN for your primary Microsoft SharePoint Online domain. Then, separated by a comma, type your FQDN for Microsoft OneDrive for Business. For example, goodshare.sharepoint.com,goodshare-my.sharepoint.com.
4. Click **Save**.
5. Restart Good Technology Common Services.
6. Click **Repositories**.

7. Click **New Repository**.
8. In the **Display Name** field, type a name for the repository,
9. In the **Storage Type** drop-down list, click **SharePoint**.
10. In the **Path** field, type path for your primary Microsoft SharePoint Online site from Step 2
11. Click **Save**.
12. Optionally, click **New Repository** for Microsoft OneDrive for Business and repeat steps 8 to 11 using the path for the Microsoft OneDrive for Business.

    You can use the username wild card in the web address. For example, https://goodshare-my-sharepoint.com/personal<*username*>_goodshare_us.

    You can lookup the path web address by logging in to theMicrosoft SharePoint Online website and click the Microsoft OneDrive option. Copy the web address into the Path field.

13. Click **Save**. Both repositories are listed in the repository list.

Microsoft SharePoint Online authentication setup

15

For Kerberos constrained delegation (KCD), which allows for single sign-on credential-less access to network resources from devices, only Active Directory Federation Service (ADFS) authentication to Microsoft SharePoint Online is supported.

Note: Configure delegation using the BEMS service account (for example, BEMSAdmin). When adding Kerberos delegation constraints for Docs service users, add the ADFS server HTTP service. Do not add Microsoft SharePoint Online servers for delegation here.

For non-KCD configurations, where users enter their credentials on the device, both DirSync with Password Hash and ADFS authentication mechanisms to Microsoft SharePoint Online are supported. No extra authentication-related steps are required to use this configuration.

ADFS version and location

ADFS 2.0 is recommended. You can install ADFS on either Microsoft Windows 2008 R2 and Microsoft Windows 2012. The ADFS server is automatically identified by the Docs service based on theMicrosoft SharePoint Online location and does not need to be specified.

ADFS HTTPS certificate

If your ADFS server uses a self-signed certificate for HTTPS communication, the certificate must be added as a trusted CA on the computer hosting BEMS.

To add the certificate, navigate to the Microsoft IIS Manager on the computer hosting ADFS, then go to Server Certificates and export the certificate to a file. On the computer hosting BEMS, import this certificate into the trusted CA list.

Once you deploy Microsoft SharePoint Online, you're ready to configure the Docs service for your Microsoft SharePoint Online users.

Troubleshooting SharePoint Issues

BlackBerry Work Docs fails to find a Microsoft SharePoint view by name

Possible cause

Maximum HTTP URL length is set to short.

Possible solution

Increase the maxUrlLength setting.

1. In Microsoft IIS, under site or server, open **Configuration Editor**.
2. In the drop-down at the top, expand **system.web** and select **httpRuntime**.
3. Change the **maxUrlLength** property to 2048. By default, the maxUrlLength is 260 characters.

Configuring Microsoft Office Web Apps server for Docs service support

16

Microsoft Office Web Apps (OWAS) is an Office server product from Microsoft that delivers browser-based versions of Microsoft Word, Microsoft PowerPoint, Microsoft Excel, and Microsoft OneNote. A single Microsoft Office Web Apps server farm can support Docs service users who access Office files through Microsoft SharePoint and File Shares. The new stand-alone deployment model means that you can manage updates to your Microsoft Office Web Apps server farm independently of other Office Server products that are deployed in your organization.

Supported file types

Docs support for Microsoft Office Web Apps (OWAS) gives your users the ability to view and edit Office documents and convert them to PDF format in BlackBerry Work and other BlackBerry Dynamics-powered apps that use the Docs service. This is all done within the secure BlackBerry Dynamics container. The BlackBerry Work Docs component is used to browse and select the files. BlackBerry Access is used to view and edit the documents.

The following table lists the supported file types for Microsoft Word.

File format	View	Edit
Open XML (.docx)	√	√ iPad only
Binary (.doc)	√	—
Macro (.docm)	√	— Macros don't work
Templates (.dotm, .dotx)	√	—
Other file formats (.dot, .mht, .mhtml, htm, .html, .odt, .rtf, .txt, .xml, .wps, .wpd)	—	—

The following table lists the supported file types for Microsoft Excel.

File format	View	Edit
Open XML (.xlsx)	√	√

File format	View	Edit
Binary (.xlsb)	√	√
Binary (.xls)	—	—
Macro (.xlsm)	√	√ However, you are prompted to create a copy of the file that has the macros removed when you save the changes that you have made
Other file formats (.xltx, .xltm, .xlam, .xlm, .xla, .xlt, .xml, .xll, .xlw,ods, .prn, .txt, .csv, .mdb, .mde, .accdb, .accde, .dbc, .igy, .dqy, .rqy, .oqy, .cub, .uxdc, .dbf, .slk, .dif, .xlk, .bak, .xlb)	—	—

The following table lists the supported file types for Microsoft PowerPoint.

File format	View	Edit
Open XML (.pptx, .ppsx)	√	√ iPad only
Binary (.ppt, .pps)	√	√ PowerPoint Online or PowerPoint Web App converts the .ppt or .pps file to a .pptx or .ppsx file to allow you to edit the file, but you must save the file as a .pptx or .ppsx file to save your changes.
Macro (.pptm, .potm, .ppam, .potx, .ppsm)	√	—
Other file formats (.pot, .htm, .html, .mht, .mhtml, .txt, .rtf, .wpd, .wps, .ppa, .odp, .thmx)	—	—

The following table lists the supported file types for PDF and OpenDocument.

File format	View	Edit
PDF (.pdf)	√	—
OpenDocument Text (.odt)	√	—
OpenDocument Spreadsheet (.ods)	√	√
OpenDocument Presentation (.odp)	√	√

For more information on the file types supported with Microsoft Office Web Apps, visit support.microsoft.com and read article 2028380.

Supported files and storage types

Documents in a supported file format can reside on any of the following storage types:

- File Shares
- Microsoft SharePoint 2007, Microsoft SharePoint 2010, Microsoft SharePoint 2013, and Microsoft SharePoint 2016
- Microsoft SharePoint Online

Supported devices

- iOS devices
  - iPad: view and edit
  - iPhone: view only
- Android devices
  - Phones: view only
  - Tablets: view only

Configure the Docs service for Microsoft Office Web Apps access

Before you begin: A Microsoft Office Web Apps server is installed and configured in your environment.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Settings**.

3. Under **Office Web App Server**, in the **Office Web App Server URL** field, type the web address of the Microsoft Office Web Apps server.
4. Click **Save**.
5. On the **Office Web App Server** server, in the **Windows** folder, copy **Microsoft.CobaltCore.dll** file. By default, the file is located in <*drive*>:\Windows\Microsoft.Net\assembly\GAC_MSIL\Microsoft.CobaltCore\.
6. On the BEMS, browser to and paste the file into the lib folder at <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<*version*>\lib.
7. Restart the Good Technology Common Services.
8. On BEMS, export the SSL certificate to a file.
   a. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BEMS System Settings**, click **SSL Certificate**.
   b. Click **Download SSL Certificate**. By default, the BemsCert.cer file is saved to the Downloads folder.
9. On the **Office Web App Server** server, add the SSL certificate to the Trusted Root CA of the computer account.
   a. Open the Microsoft Management Console.
   b. Click **File** > **Add/Remove Snap-in**.
   c. In the **Available snap-ins** column, click **Certificates** > **Add**.
   d. Select **Computer account**. Click **Next**.
   e. Select **Local Computer**. Click **Finish**.
   f. Click **OK**.
   g. In the Microsoft Management Console, expand **Certificates (Local Computer).**
   h. Right-click **Trusted Root Certificate Authorities**. Select **All Tasks**.
   i. Click **Import**.
   j. In the **Certificate Import Wizard**, click **Next**.
   k. Browse to the SSL certificate file you exported in step 8.
10. Obtain the Microsoft Office Web Apps server SSL certificate.
11. Add the Microsoft Office Web Apps server SSL certificate to BEMS. For instructions, see Importing CA Certificates for BEMS.
12. Repeat steps 8 to 11 for each BEMS server in your environment.

Configuring resource based Kerberos constrained delegation for the Docs service

17

You can configure the Docs service to use resource based Kerberos constrained delegation (KCD) to access resources, such as Microsoft SharePoint servers and File Share servers, and remove the requirement for users to provide their network credentials to access resources within the domain, and between domains and forests. When you configure resource based KCD for your Docs service, the resource authorizes the service accounts that can delegate against the resource. If you need to enable KCD in your environment, it is recommended you enable resource based KCD, if your environment meets the minimum requirements. This is also recommended in environments that do not use multiple domains or forests. If your environment does not meet the requirements for resource based KCD, you can configure Kerberos constrained delegation (KCD).

Configuring the Docs service with resource based KCD allows users to access resources in the same domain or between domains and forests.

Configure resource based Kerberos constrained delegation

You can configure the Docs service with resource based Kerberos constrained delegation (KCD) to allows users to access resources in the same domain and between domains and forests.

Before you begin:

- All BEMS instances in your environment are hosted on a computer that is running Windows 2012 or later.
- Each domain in your environment has one or more Domain Controllers on a computer that is running Windows 2012 or later.
- The BEMS service account is a member of the local Administrators group and has the Act as part of the Operating System privilege.
- If you are configuring resource based KCD for Microsoft SharePoint, make sure that Microsoft SharePoint server uses Integrated Windows Authentication – Negotiate (Kerberos) for the authentication provider.
- You identified the file share servers and Microsoft SharePoint servers that the Docs service requires access to.

1. On the Domain Controller or another computer in your environment, open Windows PowerShell (run as administrator) and set up delegation.
   a. Import the ServerManager module. Type **Import-Module ServerManager**. Press **Enter**.

b. Install the Microsoft Active Directory module for Windows PowerShell and the Microsoft Active Directory Services. Type **Add-WindowsFeature RSAT-AD-PowerShell**. Press **Enter**.

c. Import the Microsoft Active Directory module. Type **import-module activedirectory**. Press **Enter**.

2. Find the application pool identity for the Microsoft SharePoint servers in your environment. The application pool identity is located in the Microsoft Internet Information Services (IIS) Manager, on the **Application Pools** screen.

3. If the Microsoft SharePoint web application is running on a non-default port (the default port is 80 and 443) or is not running under the network service, create SPNs. Complete one or more of the following tasks:

   Note: If you have multiple Microsoft SharePoint web applications, you must create an SPN for each web application that is available in the scenarios below.

Task	Steps
Create SPNs for a Microsoft SharePoint web application running on a non-default port and as a specific user	1. Type **setspn -S HTTP/<*Sharepoint server name*>:<*Sharepoint app port*> <*Sharepoint domain*>\<*Sharepoint app user*>**. Press **Enter**. • Where <*Sharepoint server name*> is the name of the computer hosting the Microsoft SharePoint web application. • Where <*Sharepoint app port*> is the port number of the Microsoft SharePoint web application server. • Where <*Sharepoint domain*> is the domain where the Microsoft SharePoint web application server is located. For example, www.example.com. • Where <*Sharepoint app user*> is the user or service account that is listed in the Identity column in step 2. If the service is set to run as a user, the identity column displays <*web application server name*>/<*username*>. If the service is set to run as a network, you will see Network service. 2. Type **setspn -S HTTP/<*Sharepoint server FQDN*>:<*Sharepoint app port*> <*Sharepoint domain*>\<*Sharepoint app user*>**. Press **Enter**. • Where *Sharepoint server FQDN* is the FQDN of the computer hosting the Microsoft SharePoint web application server.
Create SPNs for a Microsoft SharePoint web application running on a default port (80 or 443) and as a specific user	1. Type **setspn -S HTTP/<*Sharepoint server name*> <*Sharepoint domain*> \<*Sharepoint app user*>**. Press **Enter**. 2. Type **setspn -S HTTP/<*Sharepoint server FQDN*> <*Sharepoint domain*> \<*Sharepoint app user*>**. Press **Enter**.
Create SPNs for a Microsoft SharePoint web application running on a non-default	1. Type **setspn -S HTTP/<*Sharepoint server name*>:<*Sharepoint app port*> <*Sharepoint domain*>\<*Sharepoint server name*>**. Press **Enter**.

Task	Steps
port and under a network service	2. Type **setspn -S HTTP/**<***Sharepoint server FQDN***>**:**<***Sharepoint app port***> <***Sharepoint domain***>\<***Sharepoint server name***>. Press **Enter**.

4. Add the delegation to each file share server in your environment.

Task	Steps
Add the delegation for one computer hosting BEMS.	1. Type **$gems1** = **Get-ADComputer -Identity** <***GEMS-SERVER-NAME***>. Press **Enter**. 2. Type **Set-ADComputer** <***File server name***> **-PrincipalsAllowedToDelegateToAccount $gems**1. Press **Enter**.
Add the delegation for multiple computers hosting BEMS.	1. Type **$gems1** = **Get-ADComputer -Identity** <***GEMS-SERVER1-NAME***>. Press **Enter**. 2. Type **$gems2** = **Get-ADComputer -Identity** <***GEMS-SERVER1-NAME***>. Press **Enter**. For each additonal BEMS, increment the $gems# by one. 3. Type **Set-ADComputer** <***File server name***> **-PrincipalsAllowedToDelegateToAccount $gems1,$gems2**. Press **Enter**. For each additional BEMS, add a comma and $gems# incrementing the # by one.

5. If you configure the delegation for file share servers in a DFS configuration, add delegations to the name server and the file server. For domain based DFS, this requires adding delegations for all of the Domain Controllers in the domain. Type **Set-ADComputer** <***DC-SERVER-NAME***> **-PrincipalsAllowedToDelegateToAccount $gems1**. Press **Enter**.

   Where <*DC-SERVER-NAME*> is the name of the computer hosting the domain controller.

6. Add delegation to the Microsoft SharePoint servers in your environment. Complete one of the following actions:
   - If the application pool identity for Microsoft SharePoint application is Network Service, type **Get-ADComputer** <***Sharepoint server name***> **-Properties PrincipalsAllowedToDelegateToAccount**.
   - If the application pool identity for Microsoft SharePoint application is a specific domain user, type **Get-ADUser** <***Sharepoint app user***> **-Properties PrincipalsAllowedToDelegateToAccount**.

     Where *Sharepoint app user* is the user name that is listed in the Identity column in step 2.

7. Press **Enter**.

Verify the delegation is configured correctly

You can verify that the delegation property was set correctly.

1. On the Domain Controller or another computer in your environment, open Windows PowerShell (run as administrator).
2. Complete one of the following actions to verify the delegation:
    - If the delegation was set on the server name, type **Get-ADComputer** <***server_name***> **-Properties PrincipalsAllowedToDelegateToAccount**.
    - If the delegation was set on the username, type **Get-ADUser** <***user_name***> **-Properties PrincipalsAllowedToDelegateToAccount**.

Remove resource based Kerberos constrained delegation

1. Open the Windows PowerShell (run as administrator).
2. Complete one of the following tasks:
    - To remove the delegation from a server, type **Set-ADComputer** <***server_name***> **-PrincipalsAllowedToDelegateToAccount $null**.

      If you have multiple file share or Microsoft SharePoint servers in your environment, complete this step for each server.
    - To remove the delegation from a user, type **Set-ADUser** <***user_name***> **-PrincipalsAllowedToDelegateToAccount $null**.

      If you use different usernames for the Microsoft SharePoint and file share servers, complete this step for each username.
3. Press **Enter**.

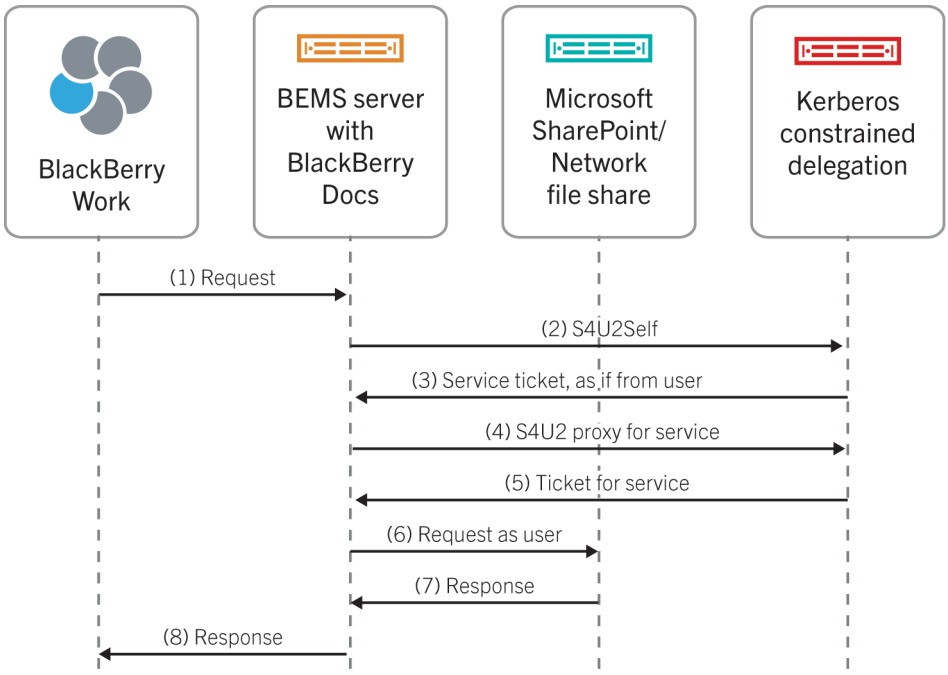
Configuring Kerberos constrained delegation for Docs

18

Configuring the Docs service to use Kerberos constrained delegation (KCD) for accessing resources such as Microsoft SharePoint and File Shares removes the requirement for end-users to provide their network credentials to access to network resources using the Docs service.

Before configuring the Docs service to use KCD, it is important to understand that configuring KCD for Docs service is independent of configuring BlackBerry Dynamics KCD. This means, for example, that if your mobile app (for example, BlackBerry Work) requires use of the Docs service exclusively, you only need to configure KCD for the Docs service.

For example, the following diagram charts a sample KCD call flow for BlackBerry Work.



All KCD transactions are between the Docs service account and the key distribution center (KDC) and respective resources. No KCD information is cached on the mobile app. The Docs service uses Microsoft's Service for User (S4U) specifications for KCD. For more information on S4U, visit the MSDN Library to see: https://msdn.microsoft.com/en-us/library/cc246071.aspx.

Configuring Kerberos constrained delegation for the Docs service

When you configure Kerberos constrained delegation (KCD) for Docs, you perform the following actions:

1. Find the SharePoint application pool identity and port.
2. Create any required Service Principle Names (SPNs).
3. Add Kerberos constrained delegation for Microsoft SharePoint servers.
4. Add Kerberos constrained delegation for file shares.
5. Turn on Kerberos constrained delegation on BEMS.

If you want to configure KCD for File Share repositories only, you can skip the Microsoft SharePoint configuration guidance that follows and proceed directly to Add Kerberos constrained delegation for file shares.

Find the SharePoint application pool identity and port

Before you begin: Make sure that you create a list of web applications that are going to be shared through the Docs service.

1. Open Windows Internet Information Services (IIS) Manager.

   Make sure that you record any additional port numbers that are assigned if a web application was extended to create alternate access mappings.

2. Find the Application Pool identity in the **Application Pools** list view or in **SharePoint Central Administration** > **Security** > **Configure service accounts**.

   In most instances, for Kerberos constrained deleagtion (KCD) to work properly, the application pool identity user must be the same for all application pools whose applications will be accessed by the Docs service. This means you cannot have different application pools running under different users.

3. In **SharePoint Central Administration**, on the **Web Applications** tab, find the port for each of the web applications listed. Look in the **Alternate Access Mappings** view as necessary.

4. In the **Sharepoint Central Administration**, open the **Application Management**, choose the web application and click **Authentication Providers** in the ribbon bar. Make sure that the authentication type for each web application is set to **Windows** and that **Negotiate (Kerberos)** is enabled under **IIS Authentication Settings**.

   In certain scenarios, switching to Negotiate (Kerberos) might require enabling Kernel-mode authentication in IIS for the corresponding IIS site. For more information, visit the MSDN Library to see Service Principal Name (SPN) checklist for Kerberos authentication with IIS 7.0/7.5.

Create Service Principal Names

Create a Service Principle Name (SPN) for each web application that needs to be shared as follows:

```
setspn -S HTTP/SPHOST:PORT <domain>\AppPoolUser
setspn -S HTTP/SPHOST.FQDN:PORT <domain>\AppPoolUser
setspn -S HTTP/SPHOST <domain>\AppPoolUser
setspn -S HTTP/SPHOST.FQDN <domain>\AppPoolUser
```

If the port is a default port, such as 80 or 443, omit the commands that include port above.

Note: Some of the lines only require a host name while others require a fully qualified host name. If the application pool identity is for a built-in user such as Network Service, then specify the host name as shown below instead of <*domain*>\AppPoolUser.

```
setspn -S HTTP/SPHOST:PORT <domain>\SPHOST
setspn -S HTTP/SPHOST.FQDN:PORT <domain>\SPHOST
setspn -S HTTP/SPHOST <domain>\SPHOST
setspn -S HTTP/SPHOST.FQDN <domain>\SPHOST
```

Note: If you use SSL, the SPN must refer to HTTP instead of HTTPS.

Add Kerberos constrained delegation in Microsoft Active Directory for Microsoft SharePoint

Note:

There is a limit of 1300 services that can be delegated to one account.

If you want to configure Kerberos contrained delegation (KCD) for File Share repositories only, do not complete this task.

1. Open Microsoft Active Directory Users and Computers.
2. In your domain, click **Users**.
3. Right-click the BEMS service account. For example BEMSAdmin. Click **Properties**.
4. In the Microsoft Active Directory account properties, on the **Delegation** tab, select the following options:
    - Trust this user for delegation to specified services only
    - Use any authentication protocol
5. Click **Add**.
6. Click **Users or Computers**.
7. In the **Enter the object names to select** field, type one of the following:
    - If the SharePoint web application is running under a domain user account, type the SharePoint Application Pool identity username.

- If SharePoint web application is running under the Network Service account, type the Microsoft SharePoint server name.

8. Click **OK**.
9. In the **Add Services** dialog box, select the HTTP service that corresponds to the SharePoint web applications running under the account specified in step 7.
10. Click **OK**.
11. Repeat Steps 4–9 for each application pool identity user and each Web Application identified.

Add Kerberos constrained delegation for file shares

The main difference between sharing files in File Share repositories, compared to sharing apps (for example, Microsoft SharePoint), is that here the delegation is to the computer hosting the BEMS instance account and not to the Docsservice process user, BEMSAdmin.

1. Open Microsoft Active Directory Users and Computers.
2. In your domain, click **Computers**.
3. Right-click the BEMS computer entry. Click **Properties**.
4. Click the **Delegation** tab.
5. Click **Add**, select **Users or Computers**, type in the name of the server whose file share needs access and click **OK**.
6. In the list of services, click **cifs**. Click **OK**.
7. Repeat Step 3 to 6 for each server that has file shares needing access.
8. Restart the BEMS server. Since Kerberos tokens are cached, restarting the BEMS server is the only way to make sure all delegation changes are received on the machines.

Turn on Kerberos constrained delegation on BEMS

When you configure Kerberos constrained delegation (KCD) for the Docs service, consider the following:

- Only Windows authentication in Microsoft SharePoint is supported. Forms-based and claims-based authentication are not supported.
- IP addresses are not allowed in the Microsoft SharePoint URLs and File Share paths that you configure in BEMS.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Settings**.
3. In the **Kerberos Contrained Delegation** section, select the **Enable Kerberos Constrained Delegation** checkbox.
4. Restart the Good Technology Common Services.

5. On BEMS instance, grant the **Act as part of the operating system** privilege to the BEMS server account (for example, GoodAdmin).
   a. Run the **Local Security Policy** administrative tool.
   b. In the left pane, expand **Local Policies**.
   c. Click **User Rights Agreement**.
   d. Configure the service account for the **Act as part of the operating system** permission.
6. Click **OK**.

Configuring BlackBerry Dynamics Launcher

19

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

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

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

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

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

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

The client entitlement app to use these services is Good Enterprise Services (AppID = com.good.gdserviceentitlement.enterprise).

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

Setting a customized icon for the BlackBerry Dynamics Launcher

You can specify a default customized icon for the BlackBerry Dynamics Launcher on users' devices. When you specify a customized icon, the icon replaces the BlackBerry Dynamics icon for all users managed by the BEMS instance.

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

- Less than 500kb.
- Named using the following format: <*file name*>_<*device_type*>_<*resolution*>.png. For example, Icon_iOS_2x.png.

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

  - Android devices: dpi, mdpi, hdpi, and xdpi
  - iOS devices: 1x, 2x, 3x, and so on

- Saved as a .png format

Specify a customized icon for the BlackBerry Dynamics Launcher

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

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry System Settings**, click **Launcher Branding**.
2. Select the **Show customized icon in launcher** checkbox.
3. Click the Device drop-down list, and select the device for which you want to specify the launcher icon. By default, Android is selected.
4. Under **Icon**, click **Choose File**.
5. Navigate to the icon file location. Click the file and then click **Open**.
6. Click **Save**.
7. Repeat steps steps 4 to 6 for each customized Android icon file resolution.
8. Complete steps 3 to 7 for customized iOS device icon files.

Remove a customized icon for the BlackBerry Dynamics Launcher

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

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry System Settings**, click **Launcher Branding**.
2. Click **Delete** beside the icon you want to remove.
3. Click **Save**.

Configuring Good Enterprise Services in Good Control

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

1. Verify Good Enterprise Services in Good Control.
2. Add BEMS to the Good Enterprise Services entitlement app.
3. Add the Good Enterprise Services entitlement app to an App Group.

For more information related to the advanced setup of multiple BEMS hosts with user affinity, see Appendix H: Microsoft Active Directory-based login for BEMS Dashboard and Web Console.

Verify Good Enterprise Services in Good Control

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

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

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

Adding BEMS to the Good Enterprise Services entitlement app

Before you begin: All BlackBerry Dynamics applications are associated with an application server in Good Control to enable communications between the client app and its application server.

1. In Good Control, under **Apps**, click **Manage Apps**.
2. Click **Good Enterprise Service**.
3. Click the **Good Dynamics** tab.
4. In the **Server** section, click **Edit**.
5. In the **Host Name** field, type the FQDN of the BEMS machine.
6. In the **Port** field, type 8443.
7. In the **Priority** field, specify the priority.
8. Specify the **Primary GP Cluster** and **Secondary GP Cluster** as required.
9. In the **Actions** column click  and repeat steps 5 to 10 for each BEMS host you are deploying.
10. Click **Save**.

Adding the Good Enterprise Services entitlement app to an app group

You add the Good Enterprise Services entitlement app to an app group in Good Control, for example the Everyone group, to entitle the services to users which belong to the group.

1. In Good Control, under **Apps**, click **App Groups**.
2. Beside a group you want to edit, click  .
3. Click  .
4. Under **Good**, select the **Good Enterprise Services - All**.
5. Click **OK**.
6. Repeat steps 2 to 5 to add the services entitlement app to another group.

Maintaining BEMS cluster identification in Good Control

20

Make sure that BlackBerry Connect servers listed in the Good Control application configuration for Connect identifies computers hosting BEMS in that cluster.

If you add a server to the cluster, correlate the timing of both the server's installation with updating the Good Control application configuration for BlackBerry Work, to include the additional server after it has been installed and is up and running.

If you temporarily remove a server from the cluster for maintenance, it is not necessary to change the Good Control application configuration for BEMS. The BlackBerry Work client will detect that the server is offline and automatically connects to another computer hosting BEMS in the cluster.

If you permanently remove a server from the cluster, first shut down the BEMS instance, then remove it from the Good Control application configuration.

Device provisioning and activation

21

Devices are activated using activation keys. Users invited to install and activate BlackBerry Connect on their device, require an access key. The access key must be entered when the user opens BlackBerry Connect for the first time on a given device. The access key is a 15-character alphanumeric code sent to the user's (registered) company email address and has the following properties:

- It can be used only once and is consumed immediately upon the activation of an application.
- It is not application-exclusive. For example, a user who has been sent four access keys can use them to activate any four applications to which the user is entitled.
- It does not support reactivation. However, if a user is issued multiple access keys, the user can use them to activate the same application multiple times. For example,
    - If the client software is uninstalled, then reinstalled on the same device, a new access key is required.
    - If a new or factory-reset device is in use, or a device emulator is in use and its state is not persisted, a new access key is required.
- It can be configured to expire after a specified period of time.

In Good Control, configure the access key to expire after a specified amount of time

1. In Good Control, under **Policies**, click **Policy Sets**.
2. Click the **Security Policies** tab.
3. In the **Provisioning Policies** section, select the **Access Keys expire** checkbox. Select the number of days after which access keys expire if not consumed.
4. Click **Update**.

In Good Control, grant access to your enterprise users

1. Assign the default policy set or create a new policy set in accordance with your enterprise's user access protocols. The default policy set is automatically applied to all new users.

For each user, the policy currently applied is located at the top of the user's account page. To apply a different policy set, hover your cursor over it and select from the available policy sets in the listbox. It should be noted that the user must be granted access to the app to activate it. This is done by assigning the user to an App Group that includes the app (Good Work) for which the user is being permitted access.

2. In Good Control, under **Users**, click **Users and Groups**.
3. On the **Users** tab, select the checkbox for the user that you want to provision, in the **User Actions** drop-down list, click **Edit User**.
4. Click the **Access Keys** tab
5. Click **New Access Key**.

   The access key is sent to the user's registered enterprise email address, one email message per key. Hashes of the access keys are also copied to the BlackBerry Dynamics NOC for validation.

   After the user receives the email message containing the access key and downloaded and installed the BlackBerry Dynamics client application on the device, they can activate the application until its Good Control-specified expiration date. At application start-up, the BlackBerry Dynamics user activation interface opens and the user must enter the access key and their enterprise email address so that the BlackBerry Dynamics Client Library can transmit the access key to the BlackBerry Dynamics NOC.

   For more information about additional provisioning and activation options available in Good Control, see Easy Activation Feature Overview Guide.

Monitoring the status of BEMS and users

22

You can use the BEMS Lookout tool to view the status of the BEMS node and scan the logs for information including the following:

- The state of devices and users.
- Notification success and failure
- The notifications received by a user during a specified time range

You can also use monitoring probes to report on the health metrics for the Push Notifications service. For example, number of successful and failed push notifications. You can run the Lookout tool on log files you saved locally in a folder or on a shared drive. The analysis tool is included in your BEMS 2.4 or later installation package and supports analyzing logs from BEMS 2.1.5 or later.

Install the BEMS Lookout tool

Before you begin: Install Python 2.7 on the computer that you use to analyse the BEMS logs. You can download it from Python 2.7 at www.python.org/downloads.

1. Update the PATH system variable.
   a. On the computer that you use to run the Lookout tool, right-click **Computer** or **This PC**. Click **Properties**.
   b. Click **Advanced system settings**.
   c. Click the **Advanced** tab.
   d. Click **Environment Variables**.
   e. In the **System variables** list, click **Path**. Click **Edit**.
   f. In the **Variable value** field, add **;C:\Python27;C:\Python27\Scripts**.
   g. Click **OK**. Click **OK** again.
2. Optionally, enable BEMS monitoring tools.
   a. On the computer that hosts BEMS, open the **Apache Karaf Web Console**. Open a browser window and navigate to **https://<*BEMS instance hostname*>:8443/system/console/configMgr**.
   b. Scroll to and click **Good Technology Probe Query Servlet**.
   c. In the **default realm** field, type **gems-ad**.

d. In the **default role** field, type **admin**.

e. Click **Save**.

f. Verify the monitoring probes are successfully enabled. In a browser navigate to **https://<*BEMS FQDN*>:8443/monitor**. Review the monitor content. If you are prompted to download the monitor.json file, download it to review the content. To view the data provided by each monitoring probe, see Monitoring probes.

3. On the computer that hosts BEMS, navigate to the BEMS Lookout tool. By default, the BEMS Lookout tool is located in the BEMS installation folder at <*drive*>:\GoodEnterpriseMobilityServer<*version*>\GoodEnterpriseMobilityServer\bems-lookout.
4. Extract the **bems-lookout<*version*>tools.zip** file.
5. Double-click **setup.bat** to install the python libraries on the computer.
6. In a text editor, open **Config.cfg**.
    - **ServerBaseUrls**: Optionally, specify the BEMS https web addresses you want to connect to and include in your analysis. If you want to run the Lookout tool on multiple BEMS instances, separate the instances using a comma, no space.
    - **MonitorCredentials**: If you configured **ServerBaseURLs**, you must include the user credentials specified during BEMS monitoring setup. For example, gemsadmin:<*password*>.
    - **ServerLogDirectories**: Specify the location of the logs for each computer that hosts a BEMS instance in the BEMS cluster. You must include the BEMS instance name and location of the log files. For example, if the log files for BEMS1 are available on a network share and BEMS2 are located in C:\blackberry, and you analyze the logs on BEMS2 you specify <*bemshost1*>:\\<*bemshost1*>\<*bemslogs share*>,<*bemshost2*>:C:\blackberry\bemslogs.

      Note: You can list the BEMS log locations in any order.
    - **DataDir**: Create a folder to where the processed data is saved. For example, create a folder called 'bem-lookout-data'. Update the DataDir property to DataDir=C:\blackberry\bems-lookout-data.
    - **LogSyncIntervalSec**: Optionally, specify the interval time, in seconds, that the analysis tool scans the log directory for new logs. By default, the LogSyncIntervalSec is set to onetime. If logs are not available, you can set the LogSyncIntervalSec=none to only view the user state.
    - **MaxLogScanAgeDays**: Optionally, specify the oldest date that you want to synchronize the logs. By default, the MaxLogScanAgeDays is 14 days.
7. Save the **Config.cfg** file.

After you finish:

- Optionally, enable monitoring probes to view additional information for the the health of your BEMS server and users
- Run the BEMS Lookout tool to analyze the BEMS logs.

Monitoring probes

The following table describes the monitoring probes you can use to view additonal information for the the health of your BEMS server and users. You can use monitoring probes to view information for a BEMS instance locally or from a remote computer.

Note: To use monitoring probes in your environment, you must enable them. For instructions, see Install the BEMS Lookout tool

Probe name	cURL Command	Output description
Push Notification Counter	Type **curl -k -i -X GET \ -H "Content-Type:application/json" \ -H "Authorization:Basic ZG9tYWluXHVzZXI6cGFzc3dvcmQ=" \ 'https://<*BEMS instance name*> :8443/monitor/push.notifications'**	**SuccessfulPushes** This probe specifies the number of push notifications, per push notification type (for example, APNS, GNP, and GCM) that have the instance sent for users supported by this instance. You want to see the number increase over short intervals of time. If it stops rising then BEMS is not sending any push notifications.
Total user count	Type **curl -k -i -X GET \ -H "Content-Type:application/json" \ -H "Authorization:Basic ZG9tYWluXHVzZXI6cGFzc3dvcmQ=" \ 'https://<*BEMS instance name*>:8443/monitor/mail.users/UsersCount'**	**UsersCount** This probe specifies the total number of users across the BEMS cluster which successfully registered a device and are successfully auto discovered by BEMS. The UsersCount does not reflect the number of devices receiving push notifications.
Stale user count	type **curl -k -i -X GET \ -H "Content-Type:application/json" \ -H "Authorization:Basic ZG9tYWluXHVzZXI6cGFzc3dvcmQ=" \ 'https://<*BEMS instance name*>:8443/monitor/mail.users/StaleUsersCount'**	**StaleUsersCount** This probe specifies the total number of users across the BEMS cluster which successfully registered a device, but for which BEMS is no longer sending push notifications because the device hasn't registered in the past 72 hours.
EWS user count	Type **curl -k -i -X GET \ -H "Content-Type:application/json" \ -H "Authorization:Basic ZG9tYWluXHVzZXI6cGFzc3dvcmQ=" \ 'https://<*BEMS instance name*>:8443/monitor/mail.ewslistener/EWSUserStats'**	**EWSConnectedUserCount** This probe specifies the number of users on the Microsoft Exchange Web Services instance, for which BEMS connects to the Microsoft Exchange Server, and is attempting to monitor the users' mailboxes. This EWSConnectedUserCount reflects the number of users most likely to be receiving push notifications unless BEMS is experiencing errors with its Microsoft

Probe name	cURL Command	Output description
		Exchange Web Services connections to the Microsoft Exchange Server. The EWSConnectedUserCount should be equal across all Microsoft Exchange Web Services instances in a cluster. If this count drops to 0 then the Microsoft Exchange Web Services instance is not servicing any user mailboxes.

Run the BEMS Lookout tool

Before you begin:

- Install Python 2.7 on the computer that you use to analyse the BEMS logs. You can download it from Python 2.7 at www.python.org/downloads.
- Install the BEMS Lookout tool.

1. On the computer that you installed the BEMS Lookout tool, navigate to the bems-lookout-<*version*>.tools folder. By default, the folder is located at: <drive>:\Downloads\GoodEnterpriseMobilityServer.<*version*>\GoodEnterpriseMobilityServer\bems-lookout\bems-lookout-<*version*>.tools-all\bems-lookout-<*version*>.tools
2. Start the log analysis, double-click **start.bat**. The BEMS Lookout tool writes the log files it generates to the DataDir parameter that you specified when you installed the BEMS Lookout tool.

After you finish: The BEMS Lookout tool log analysis results are saved to a database in the DataDir folder. To view the analysis results, open a browser and go to **http://localhost:5000**.

Removing the BEMS software

23

When you stop a BEMS instance, it will not be used by your high availability implementation, and all users that are serviced by the discontinued instance are reallocated to other servers automatically as soon as the discontinued instance goes down. This also applies to BlackBerry Connect server instances.

When you uninstall a BEMS or Connect instance, you perform the following actions:

1. Remove the BEMS server references for BlackBerry Work
2. Remove the BEMS Connect server references for BlackBerry Connect

Remove the BEMS server references for BlackBerry Work

1. On the computer that hosts the BEMS server, navigate to the BEMS installation folder. By default, the BEMS installation folder is located at <*BEMS_install_location*>\GoodEnterpriseMobilityServerSetup.<*version*>.exe.
2. Double-click **GoodEnterpriseMobilityServer.<*version number*>.exe**.
3. Select **Uninstall** and follow the wizard's onscreen instructions.
4. In Good Control, under **Apps**, click **Manage Apps**.
5. Click **BlackBerry Work**.
6. Click the **BlackBerry Dynamics** tab.
7. In the **Server** section, click **Edit**.
8. Click the BEMS server you want to remove. Click  .
9. Click **Save**.

Remove the BEMS Connect server references for BlackBerry Connect

1. Uninstall the BEMS instance on the host machine.
2. In Good Control, under **Apps**, click **Manage Apps**.

3. Click **Good Connect**.
4. Click the **BlackBerry Dynamics** tab.
5. In the **Server** section, click **Edit**.
6. Click the BEMS server you want to remove. Click  .
7. Click **Save**.

Appendix A: Preinstallation checklists 24

The following BEMS pre-installation checklists for the respective services cited are recommended for environments:

- BlackBerry Push Notifications
- BlackBerry Connect and BlackBerry Presence
- BlackBerry Docs

You can download the BEMS software from the Admins for Enterprise software portal.

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

After completing the preinstallation checklists, see the supplemental publication SSL/TLS Certificate Check for BEMS and BlackBerry Work for more information about importing and exporting required security certificates to and from the relevant keystores on BEMS and BlackBerry Work client devices for authenticating with BlackBerry Dynamics, Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, and Microsoft Office Web Apps server (OWAS).

BlackBerry Push Notifications

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

Complete	Requirement
Registration	
☐	Register with the Enterprise software portal.
☐	Request the BlackBerry Work app from the Marketplace for Enterprise Software portal.
Network	
☐	The following ports are open for BEMS: Inbound TCP ports • 61617 to and from computers hosting BEMS in the same cluster (bidirectional) • 61616 to and from computers hosting BEMS in the same cluster (bidirectional) • 8443 from the Good Proxy server (required for Presence and Push Notifications); add port 8181 if SSL is not going to be used

Complete	Requirement
	Outbound TCP ports • 443 to BlackBerry Dynamics NOC/APNS • 443 to Firebase Cloud Messaging (FCM) • 443 to Microsoft Exchange Server • 17080 to the Good Proxy server (17433 for SSL) • 61617 to and from computers hosting BEMS in the same cluster (bidirectional) • 61616 to and from computers hosting BEMS in the same cluster (bidirectional)
Active Directory and Exchange	
☐	Verify the supported version of Microsoft Exchange.
☐	Create a Microsoft Active Directory account for the BEMS service account. For password considerations, see Creating a Microsoft Active Directory account for the BEMS service account.
☐	Create a Microsoft Exchange mailbox for the BlackBerryAdmin account.
☐	Grant Application Impersonation Permissions to the BlackBerryAdmin account in Microsoft Exchange. For instructions, see Grant application impersonation permission to the BEMS service account
☐	Make sure that your Microsoft Exchange Autodiscover is set up correctly. For more information on how to to use third-party tools to test autodiscover, visit support.blackberry.com/kb to read article 40351.
☐	Make sure that Microsoft Exchange EAS is enabled on port 443, and that connections are permitted for the Good Proxy server.
.NET FRAMEWORK	
☐	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.
BEMS	
☐	Verify that your environment is running BlackBerry Dynamics servers that support BEMS. **Important**: BlackBerry Dynamics must already be installed and operational before installing BEMS.

Complete	Requirement
☐	Verify that the computer hosting BEMS is running an operating system that supports BEMS.
☐	Verify that you have the required hardware to host BEMS. For more information about hardware requirements, see BlackBerry Dynamics Servers and BlackBerry Enterprise Mobility Server Plannning conntent.
☐	Make sure that the BlackBerryAdmin service account is a local administrator on the server.
☐	Ensure that the server's date and time are set correctly.
☐	Ensure that the server has been joined to the domain.
☐	Make sure that Windows Firewall is OFF.
☐	Disable antivirus programs before you install or upgrade the BEMS software Exclude the BEMS directory from virus scanning
☐	Install JRE 8 (latest update release).
☐	Make sure you set the JAVA_HOME environment variable.
☐	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 Exchange (EWS). For more information on how to use third-party tools to test connectivity, visit support.blackberry.com/kb to read article 40351.
Database	
☐	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.
☐	Create a database for the BlackBerry Push Notifications (PNS) service and name it "BEMSDB."
☐	Make sure that the Microsoft SQL Server account or the BEMS Windows service account has db_owner privileges to the BEMSDB.

BlackBerry Connect and BlackBerry Presence

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

Note: BlackBerry Presence is available only for Microsoft Lync and Skype for Business implementations.

Complete	Requirement
Registration	
☐	Register with the Enterprise software portal.
☐	Request the BlackBerry Connect app from the Marketplace for Enterprise Software portal.
Network - Microsoft Lync Server and Skype for Business	
☐	Ensure the following ports are open for BEMS: Inbound TCP Ports • 8080/8082 from the Good Proxy server • 8443 from the Good Proxy server (for BlackBerry Presence) • 49555 from the Microsoft Lync Server and Skype for Business server (for BlackBerry Connect) • 49777 from the Microsoft Lync Server and Skype for Business server (for BlackBerry Presence) Outbound TCP Ports • 443 to the BlackBerry Dynamics NOC • 206.124.114.0/24 • 206.124.121.0/24 • 206.124.122.0/24 • 5061 to the Microsoft Lync Server server and Skype for Business • 17080 to the Good Proxy server • 17433 to the Good Proxy server • 1433 to the Microsoft SQL Server (default) • 1434 UDP to the Microsoft Lync database (for initial setup only) • 49777 – 57500 TCP: Random port in this range to the Microsoft Lync database (for initial setup only)

Complete	Requirement
☐	If BEMS requires a proxy server for external access, record it here: • Proxy server make and model: _____ • Method: _____
Network - Cisco Jabber	
☐	Ensure the following ports are open for BEMS: Inbound TCP Ports • 8080/8082 from the Good Proxy server Outbound TCP Ports • 443 to the BlackBerry Dynamics NOC • 206.124.114.0/24 • 206.124.121.0/24 • 206.124.122.0/24 • 8443 to the Cisco User Data Service • 5222 to the Cisco Jabber XMPP Service • 17080 to the Good Proxy server • 17433 to the Good Proxy server • 1433 to the Microsoft SQL Server server (default)
☐	If BEMS requires a proxy server for external access, record it here: • Proxy server make and model: _____ • Method: _____
Microsoft Active Directory - Microsoft Lync Server	
☐	Create an Microsoft Active Directory service account for the BEMS software (can be the same account used for BlackBerry Dynamics).
☐	Verify that the BEMS service account has RTCUniversalReadOnlyAdmins permission during the BEMS installation. This permission is granted via Microsoft Active Directory.
☐	Create a Trusted Application Pool, trusted application, and trusted application endpoint for BEMS via the Microsoft Lync Shell Console. **Note:** The user creating the Trusted Application Pool must have RTCUniversalServerAdmins and Domain Admins permissions.

Complete	Requirement
	For more information about preparing the first computer hosting BEMS, see Prepare the initial computer hosting BEMS.
Microsoft Active Directory - Cisco Jabber	
☐	Create an Microsoft Active Directory service account for the BEMS software (can be the same account used for BlackBerry Dynamics)
BEMS - Microsoft Lync Server and Skype for Business	
☐	Verify that your environment is running BlackBerry Dynamics servers that support BEMS. **Important**: BlackBerry Dynamics must already be installed and operational before installing BEMS.
☐	Verify that you have a supported instant messaging server.
☐	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 rights.
☐	Make sure that the server's date and time are set correctly.
☐	Make sure that the server is joined to the domain.
☐	Make sure that Windows PowerShell (x86) is installed: • For Microsoft Lync Server 2010, Microsoft Lync Server 2013, and Skype for Business install Windows PowerShell 3.0 RTM • Open “Windows PowerShell (x86)” and run the following command to enable execution of remote signed scripts: `Set-ExecutionPolicy -Scope CurrentUser RemoteSigned`
☐	Make sure that the Microsoft Unified Communications Managed API is installed. 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.
☐	Request and install an SSL certificate on BEMS. For more information, see SSL certificate requirements for Microsoft Lync Server and Presence.
☐	Disable all antivirus programs and backup software before you install or upgrade the BEMS software. Exclude the BEMS directory from virus scanning.

Complete	Requirement
☐	Install JRE 8 (latest update version).
☐	Make sure you set the JAVA_HOME environment variable.
BEMS - Cisco Jabber	
☐	Verify that your environment is running BlackBerry Dynamics servers that support BEMS. **Important**: BlackBerry Dynamics must already be installed and operational before installing BEMS.
☐	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 rights.
☐	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. Exclude the BEMS directory from virus scanning.
☐	Install JRE 8 (latest update version).
☐	Make sure you set the JAVA_HOME environment variable.
Database	
☐	Verify your environment is running a supported database server.
☐	Create a database for the BlackBerry Connect service and name it "BEMS-Connect." This must be done prior to installing BEMS. For more information about database requirements, see BlackBerry Connect service database requirements.
☐	Make sure that the BEMS service account has db_owner permission for the Connect database.

BlackBerry Docs

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

Complete	Requirement
Registration	
☐	Register with the Enterprise software portal.
☐	Request the BlackBerry Work app from the Marketplace for Enterprise Software portal.
☐	Log in to https://account.good.com/#/a/organization//entitlements and confirm that you have the *Feature - Docs Service Entitlement* app.
Network	
☐	Make sure the following ports are open for BEMS: Inbound TCP ports • 8443 from the Good Proxy server Outbound TCP ports • 80 or 443 to SharePoint • 80 or 443 to Microsoft Office Web Apps server • 17080 or 17433 to the Good Proxy server • 1433 to the SQL Server (default) • 445, 139 to CIFS share • 389 or 636 to LDAP Outbound UDP ports • 137–138 to CIFS share
☐	If BEMS requires a proxy server for external access, record the following information: • Proxy server make and model: _____ • Authentication method: _____
Active Directory	

Complete	Requirement
☐	Create an Microsoft Active Directory service account for the BEMS software (this can be the same account that was used for BlackBerry Dynamics).
Microsoft .NET Framework	
☐	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.
BEMS	
☐	Verify that your environment is running BlackBerry Dynamics servers that support BEMS. **Important**: BlackBerry Dynamics must already be installed and operational before installing BEMS.
☐	Verify that the computer hosting BEMS is running an operating system that supports BEMS.
☐	Verify that you have the required hardware to host BEMS. For more information about hardware requirements, see BlackBerry Dynamics Servers and BlackBerry Enterprise Mobility Server Plannning conntent.
☐	Make sure that the server's time and date are set correctly.
☐	Make sure that the server is joined to the domain.
☐	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.
☐	If you are using resource based Kerberos constrained delegation or Kerberos contrained delegation (KCD), 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 rights.
☐	Make sure that Windows Firewall is OFF.
☐	Disable all antivirus programs and backup software before you install or upgrade the BEMS software. Exclude the BEMS directory from virus scanning.
☐	Make sure you install the correct Java version.

Complete	Requirement
☐	Make sure you set the JAVA_HOME environment variable.
Database	
☐	Verify your environment is running a supported database server.
☐	Create a database for the BlackBerry Docs service and name it "BEMS-Docs."
☐	Make sure the BEMS service account has db_owner permissions for the BlackBerry Docs database.

Appendix B – Understanding the BEMS-Connect configuration file

25

Configuration settings can be manually updated in the BEMS Connect configuration file (GoodConnectServer.exe.config) located in <*drive*>\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Connect. However, best practice for updating the file should use the BEMS admin console.

Note: After updating the configuration parameters, you must restart the BEMS machine for the changes to take effect.

Parameter name	Required	Description	Default setting
ACK_TIME_WAIT	—	Time (in milliseconds) that the BlackBerry Connect server waits for acknowledgment from client for a message received before sending message failed to deliver.	90 000
ACTIVE_DIRECTORY_CACHE_REFRESH_SECS	√	The number of seconds the BlackBerry Connect server waits before synchronizing with the Microsoft Active Directory (any value smaller than 7200 is disregarded in favor of 7200 seconds).	86,400 (24 hours)
ACTIVE_DIRECTORY_SEARCH_RESULT_MAX	√	The upper limit on the number of hits from a search of the company directory.	150
AD_USERS_SOURCE	—	Parameter indicates if the Connect service should connect to Microsoft Active Directory Global Catalog servers or use LDAP to a local Domain Controller for loading SIP-enabled users. This value can be “GC” or “LDAP”. By default, the value is LDAP if the value is empty.	
AD_USERS_SOURCE_DOMAIN	√ If users source is GC	The Active Directory Domain in the Global Catalog to query. This value should be in an LDAP format; for example, DC=EXAMPLE,DC=COM.	
APN_ALERT	√	Apple push notification message string that notifies a user that there are unread messages.	“You have <*number*> unread messages.”
APN_BADGE	√	Determines whether or not to use the badge graphic for Apple push notifications.	True

Parameter name	Required	Description	Default setting
APN_SLEEP_TIME	√	The number of milliseconds the BlackBerry Connect server waits in between queued Apple push notifications.	100
APN_SOUND	√	Play sound when an Apple device receives a push notification.	
BASE_URL	√	Web address for the Connect service which takes one of the following values: • http://*:8080/ • https://*:8082/	http://*:8080/
BUILD_VERSION	√	The version number of the BlackBerry Connect server build.	Auto-populated
DB_AUTHTYPE	√	USE_INTEGRATEDAUTH when the specifying Windows integrated authentication, or Microsoft SQL Server authentication is used.	
DB_INIT_CATALOG	—	SQL Server database name; only valid if DB_TYPE=SQLSERVER **Note:** Do not change this value. It is set by the installer.	GoodConnect
DB_PURGE_HOURS	—	Any IMs from invitations are obfuscated. In addition to obfuscation, the integer value representing the maximum age, in hours, of missed messages and invitations before they are automatically deleted (purged) is set with DB_PURGE_HOURS. For example, <add key="DB_PURGE_HOURS" value="72" /> If Connect is started 7/8/2015 @ 12:31pm, then on 7/9/2015 @ 12:31pm a process removes all invitations and all missed messages older than 72 hours. Connect continues to run every 24 hours thereafter.	0
DB_RECONNECT_TRY_NUM	√	Number of times the Connect server tries reconnecting to the database after a failure to connect to database.	3
DB_RECONNECT_WAITTIME_SEC	√	Number of seconds the Connect server waits before trying to reconnecting to database.	300
DB_SESSION_TIMEOUT_SECS	√	Time limit for search Lync/OCS database as defined by LYNC_DB_CONNECTIONSTRING.	300
DB_TYPE	√	SQLSERVER or ORACLE depending on what database is used.	

Parameter name	Required	Description	Default setting
DISABLE_MESSAGEUPDATE	—	Disable message not delivered errors which may potentially be due client and network latencies.	False
ENABLE_SOURCE_NETWORK	—	Labels address book contacts as "external" if they do not belong to your organization. These are federated contacts. A federated contact is a member of a company whose Office Communications server is federated (connected) with your company's Office Communications server.	False
EWS_HISTORY_INTERVAL_MINUTES	—	Defines the number of interval in minutes the BlackBerry Connect server waits before writing to Conversation history. 0 means that conversation history is written only after conversation has been terminated.	5
EWS_HOST	—	FQDN of the Microsoft Exchange Server to which the BlackBerry Connect server writes conversation histories.	
EWS_VERSION	—	Version of Microsoft Exchange Server 0 = Microsoft Exchange Server 2007 SP1 1 = Microsoft Exchange Server 2010 2 = Microsoft Exchange Server 2010 SP1 3 = Microsoft Exchange Server 2010 SP2 or SP3 4 = Microsoft Exchange Server 2013 5 = Microsoft Exchange Server 2016	2
GASLAMP_USERNAME	√	Windows service account	
GD_APN_HTTP_URL	√	Web Service web address for BlackBerry Dynamics Apple Push Notifications Service (APNS).	
GD_APN_PROXY_AUTH_DOMAIN	—	Web Proxy Domain	Deprecated
GD_APN_PROXY_AUTH_PASSWORD	—	Web Proxy Password	Deprecated
GD_APN_PROXY_AUTH_USERNAME	—	Web Proxy Username	Deprecated
GD_APN_PROXY_HTTP_HOST	—	Web Proxy Host	

Parameter name	Required	Description	Default setting
GD_APN_PROXY_HTTP_PORT	—	Web Proxy Port	

GD_APN_PROXY_TYPE	—	Web Proxy Authentication Mechanisms. Acceptable values are:
		`"" (empty string for no proxy)`
		`"Basic No Auth"`
		`"Basic"`
		`"Digest"`
			""

GD_APNS_BLACKLIST_RETRY_NO	√	Specifies the number retries after the server receives APNS response where the token is blacklisted	3
GD_URL	√	Complete web address of the Good Proxy server, with protocol, fully qualified domain name, and port. For example: https://gp.myCompany.com:17433.	
LONG_INVITATION_TIME_DELAY	—	Time (in milliseconds) that a Connect client waits for invitation received to confirm or ignore a request to a conversation.	60 000
LYNC_DB_CONNECTIONSTRING	—	The Microsoft SQL Server connection string for the Microsoft SQL Server/OCS database	
OCS_SERVER	√	The FQDN of the Microsoft Lync Front-End server or Front-End server pool.	
RESTRICT_CERT_BY_FRIENDLY_NAME	—	Allows naming of certificate so that the BlackBerry Connect can load correct certificate; the certificate friendly name must match the name specified here.	
SEND_TIME_WAIT	—	Time (in milliseconds) the BlackBerry Connect server waits after sending message before reporting message failed to deliver.	120 000
SESSION_TIMEOUT_SECS	√	The number of seconds a client is allowed to remain idle **Note:** The minimum SESSION_TIMEOUT_SECS is 600, even if you put in 60 seconds or 1 second. This was done to mitigate stress related race conditions.	86,400 (24 hours)
UCMA_APPLICATION_NAME	√	Name of application as defined through the installation provisioning process.	Generated during application provisioning

Parameter name	Required	Description	Default setting
UCMA_APPLICATION_PORT	√	The fixed port used by the BlackBerry Connect server to receive messages from the enterprise IM server.	49555
UCMA_GRUU	√	GRUU = Globally Routable User-Agent URI that uniquely defines the Session Initiation Protocol (SIP) URI for the application.	Generated during application provisioning

Appendix C – Java Memory Settings

26

By default, the Java settings for BEMS are located in the configuration file Good Server Distribution\gems-karaf-<*version*>\etc \GoodServerDistribution-wrapper.conf.

You can review or modify the default Java settings used by BEMS. However, as a general rule, you won't need to make changes to these settings.

The default memory settings for BEMS can be viewed at:

Initial memory allocation:

- # Initial Java Heap Size (in MB)

```
wrapper.java.initmemory=4096
```

- # Maximum Java Heap Size (in MB)

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

Appendix D – Setting up IIS on the BEMS

27

SSL offloading takes all the processing of SSL encryption and decryption off the main Web server and moves it to the computer that hosts BEMS.

1. Download and install the IIS Application Request Routing extension.
2. When installation completes, click **Start** > **IIS Manager**.
3. Under **Connections**, select **Server** > **Server Certificates**, then double-click **Import** to import a trusted third-party certificate (the .PFX file received from your CA).
4. After the certificate is added, click **Server** under **Connections**, double-click **Application Request Routing**, and click **Server Proxy Settings** under **Actions**.
5. Check **Enable proxy**, then click **Apply**.
6. Next, click **Server** under **Connection**, double-click **URL Rewrite**, then click **Add Rule(s)** under **Actions**.
7. Select **Blank Rule** and click **OK**.
8. On the **Edit Inbound Rule** screen, in the **Name** field, type a name for the rule.
9. In the **Match URL** section, in the **Requested URL** drop-down list, select Matches the Pattern.
10. In the **Using** drop-down list, select **Regular Expressions**.
11. In the **Patterns** drop-down list, select **pushnotify/pushchannels**.
12. Under **Conditions**, click **Add**.
13. In the **Add Conditon** dialog box, complete the following actions:
    - In the **Condition input** field, type {**REQUEST_METHOD**}.
    - In the **Check if input strings** drop-down list, select **Matches the Pattern**.
    - In the **Patterns** field, type **POST**.
14. Click **OK**.
15. Under **Action**, in the **Action type** drop-down list, click **Rewrite**.
16. In the **Rewrite URL** field, type **http://localhost:8181/{R:0}**.
17. Click **Apply**.
18. Verify that you can access BEMS under its secure HTTPS port.
    In a browser, type **https://localhost:8443/dashboard**.

19. After the certificate is added, under click **Connections**, click **Server**.
20. Double-click **Application Request Routing**.
21. Under **Actions** click **Server Proxy Settings**.
22. Select the **Enable proxy** checkbox.
23. Click **Apply**.
24. Under **Connection**, click **Server**.
25. Double-click **URL Rewrite**.
26. Under **Actions**, click **Add Rule(s)**.
27. Click **Blank Rule**. Click OK.
28. On the **Edit Inbound Rule** screen, enter a Name for the rule. For exampe, "bems".
29. In the **Match URL** section, in the **Requested URL** drop-down list, select **Matches the Pattern**.
30. In the **Using** drop-down list, select **Regular Expressions**.
31. In the **Patterns** drop-down list, select **pushnotify/pushchannels**.
32. Expand **Conditions**. Click **Add**.

Appendix E – BEMS Windows Event Log Messages

28

Message	Component	Level	Context
Error Node exceeded capacity (100%). <*number of users including users over exceeded capacity*>/<*number of users for maximum capacity*>	autodiscover/ ewslistener	Error	This error occurs when the BEMS instance reaches maximum user capacity. BEMS features might not work as expected for any new users added to the BEMS instance. For example, notifications.
Warn Node close to exceed capacity (80%). <*number of users*>/<*number of users for maximum capacity*>	autodiscover/ ewslistener	Warning	This warning occurs when the BEMS instance reaches 80% of user capacity or if one BEMS instance is working at overcapacity and one BEMS instance is working under capacity. BEMS automatically reassigns users between the two BEMS instances.
Error communicating with Good Proxy Server - HTTP code {}, Message {}	server-core/gd-core	Error	Could not connect to Good Proxy server while verifying authorization token (during Push Registration from G3 Mail context)
Failed to retrieve the list of Good Proxy servers - code {} - Reason {}	server-core/gd-core	Error	Used for high availability and load balancing of requests to Good Proxy server. The list of known Good Proxy servers are maintained in memory and requests are load-balanced through this list.
Failed to retrieve the list of Good Proxy servers	server-core/gd-core	Error	Used for high availability and load balancing of requests to Good Proxy server. The list of known Good Proxy servers are maintained in memory and requests are load-balanced through this list.
Incorrect Good Proxy Server configuration	server-core/gd-spring	Error	Communicate with Good Proxy server to verify Authorization token using HTTP(s) protocol. If URL is syntactically wrong or configuration error then error is logged in event log.
Autodiscover failed for {} users with exception {}	server-notifications/ autodiscover	Warn	Failed to retrieve user's settings through autodiscover. Needs administrator attention to fix the issue. The user will not receive notifications

Message	Component	Level	Context
			until issue is resolved. This is a batch request and the log only prints the number of users that failed auto discover.
Invalid syntax for property {}, must be a valid URL	server-notifications/ autodiscover	Error	Server is configured with an invalid URL used for bypassing the steps to find the autodiscover end point. BEMS ignores this URL and follows the regular steps to perform autodiscover.
User {} being quarantined after {} attempts to perform autodiscover	server-notifications/ autodiscover	Warn	BEMS can not autodiscover the user's settings for configured number of attempts. The user mentioned is marked as 'QUARANTINED' and does not receive notifications. The status can be reset through karaf command (user:reset).
No response from server while performing autodiscover for user {}	server-notifications/ autodiscover	Warn	Autodiscover failed for the user mentioned.
Autodiscover failed for user {}, error code: {}, Detail: {}	server-notifications/ autodiscover	Warn	Autodiscover failed for the user mentioned.
Failed to retrieve user settings while performing autodiscover for user {}	server-notifications/ autodiscover	Warn	Autodiscover failed for the user mentioned.
No valid EWS URL setting configured for the user {}	server-notifications/ autodiscover	Warn	Autodiscover failed for the user mentioned.
Error communicating with Database server - {error msg}	server-notifications/ autodiscover	Error	BEMS failed to connect to SQL database. Needs immediate attention.
Database Error - {error msg}	server-notifications/ autodiscover	Error	BEMS failed to connect to SQL database. Needs immediate attention.
Lost connection with exchange server. Last known error {}	server-notifications/ ewslistener	Erro	EWSListener: Lost connection with exchange server. This might be due to Exchange server \Autodiscover service down.
Error subscribing user {} with exchange server {}	server-notifications/ ewslistener	Error	Subscribe to the user email address with exchange server to track modifications of user mailbox.

Message	Component	Level	Context
User {} marked for reautodiscover	server-notifications/ ewslistener	Info	Does a database call to mark the user for reautodiscovery. This task is done every *n* interval of time.
Error communicating with Database server - {error details}	server-notifications/ pushnotifydbmanager	Error	Bootstrap database connection.
{} is no longer the master (producer) since database server time {}	servernotifications/ pushnotifyha-dbwatcher	Error	High availability System: Check whether the node itself is Producer or not. Prints the error in event log when the server has lost ownership of the high availability system (not master any more).
{} is the master (producer) since database server time {}	servernotifications/ pushnotifyha-dbwatcher	Info	High availability System: Check whether the node itself is Producer or not. If it was not master before; the fail-over is happening.
Detected Server {} is inactive. Users will be load balanced to other active servers	servernotifications/ pushnotifyha-dbwatcher	Error	High availability System: If server is detected as inactive\heartbeat fails, the users of the bad server are reassigned to other active server.
Error communicating with Database server - {error details}	servernotifications/ pushnotifyprefs	Error	Database error due to server down\login error, etc.
{ Good Dynamic Proxy Server connection error details }	server-console/config	Error	Connect BlackBerry Dynamics Module – Test from dashboard with GP down, connection failure error.
Connection to Good Dynamic Proxy Server is successful	server-console/config	Info	Connect BlackBerry Dynamics – Test from dashboard when GP is up and running, successful test.
Connection Successful, Server: -{}: Database : {}	server-console/config	Info	Mail – DB – Test database configurations from dashboard. Connection successful.
Exception during connection test - {}	server-console/config	Error	Mail – DB – Test database configurations from dashboard. Connection issues due to bad password or user or host info.
Invalid configuration properties- {}	server-console/config	Error	Mail – DB – Test database configurations from dashboard. Validation of database configuration values.

Message	Component	Level	Context
{ Good Dynamic Proxy Server connection error details }	server-console/config	Error	Presence BlackBerry Dynamics – Test from dashboard with Good Proxy down, connection failure error.
Connection to Good Dynamic Proxy Server is successful	server-console/config	Info	Presence BlackBerry Dynamics – Test from dashboard when Good Proxy is up and running, successful test.
Lync Presence Provider Ping failed with error status {} and reason - {}	server-presence/ presencebundle	Error	Connection to Presence server. If response received, log the reason for failure.
Lync Presence Provider Ping failed with exception {}: {} - set status {}	server-presence/ presencebundle	Error	Connection to Presence server. Most likely connection refused because down
Lync Presence Provider Ping failed, cause unknown	server-presence/ presencebundle	Error	Connection to Presence server.
Presence Service failed to reset LPP, interrupted with error: {}	server-presence/ presencebundle	Error	Reset all contacts presence status.
Presence Service failed to reset LPP, timed out with error: {}	server-presence/ presencebundle	Error	Reset all contacts presence status. Timeout error.
Failed to reset LPP, {} with error: {}	server-presence/ presencebundle	Error	Reset all contacts presence status.
Presence Service started	server-presence/ presencebundle	Info	Presence service started.
Presence Service stopped	server-presence/ presencebundle	Info	Presence service stopped.
Bad Lync Presence Provider Subscription URI: {}	server-presence/ presencebundle	Error	Presence service provider subscription URI.
Bad Lync Presence Provider Ping URI: {} Ping	server-presence/ presencebundle	Error	Presence service provider subscription URI.
Redis Cache & Queue services are not available at the moment.	server-presence/ presencebundle	Error	When cache provider is set to Redis and Redis service is unavilable.

Message	Component	Level	Context
GNP Relay Service not available	server-presence/ presencebundle	Warn	GNP service which sends GNP notification is not available or down.

Appendix F – File types supported by the BlackBerry Docs service

29

The following file types and extensions are currently supported by the BlackBerry Docs service and as mail attachments:

.goodsharefile	.tiff	.utf16-plain-text,
.doc, Docx	.apple.pict	.rtf
wordprocessingml.document	.compuserve.gif	.html
powerpoint.ppt, PPTx	.png	.xml
excel.xls, XLSX	.quicktime-image	.xhtml
spreadsheetml.sheet,	.bmp	.htm
adobe.pdf	.camera-raw-image	.data
apple.rtfd,	.svg-image,	.content
apple.webarchive	.text	.zip
.image	.plain-text	
.jpeg	.utf8-plain-text	

The following media file types are supported on iOS devices only:

.3gp	.caf	.au
.mp3	.aac	.snd
.mp4	.adts	.sd2
.m4a	.aif	.mov
.m4v	.aiff	
.wav	.aifc	

Appendix G – Advanced BlackBerry Dynamics Launcher setup

30

BlackBerry Dynamics Launcher relies on the services identified in Configuring the BlackBerry Dynamics Launcher with BlackBerry Enterprise Services. In a basic setup, a BlackBerry Dynamics Launcher search for a provider of the services produces a single result for all services (com.good.gdservice-entitlement.enterprise). In setups that require user affinity or where there's a large list of BEMS instances deployed, each with different purposes, strict adherence to the basic setup approach is insufficient.

Deploying multiple BEMS instances

Environments containing multiple BEMS hosts with different servers tied to different purposes will need new, organization-level App IDs created for the appropriate services; after which, these services will then bind to the new App IDs, which will require updated server information so they point to the correct computer hosting the BEMS instance. Finally, these App IDs need to be configured as allowed apps for select users via App Groups.

To illustrate by example, consider a fictional company that wants to deploy 25 BEMS hosts, six of which will be used for BlackBerry Presence, with three others used for both BlackBerry Directory Lookup and Good Follow-Me services. Hence, the following steps would need to be performed via Good Control.

When BlackBerry Dynamics Launcher opens using the following configuration, it searches for providers of the three services. For Presence, it will find com.xyzcorp.enterprise-services.presence, then read the provider's configured servers list, using it to set up communication with the BlackBerry Presence server. The same behavior applies to the other two services. BlackBerry Dynamics Launcher is agnostic with respect to the providers of each service; i.e., whether they are the same machine or different.

1. Create a couple of organization-level App IDs: **com.xyzcorp.gdservice-entitlement.presence** and **com.xyzcorp.gdservice-entitlement.directory-followme**.
2. Make **com.xyzcorp.gdservice-entitlement.presence** a provider of the enterprise BlackBerry Presence service and **com.xyzcorp.gdservice-entitlement.directory-followme** a provider of the enterprise BlackBerry Directory Lookup and Good Follow-Me services. Notwithstanding the different App IDs, each would use the existing published Good Enterprise Services; they would not create their own.
3. Under the application details of **com.xyzcorp.gdservice-entitlement.presence**, set up the 6 BEMS hosts. Only the server list needs to be configured; the application configuration is left blank. For the application details of **com.xyzcorp.gdservice-entitlement.directory-followme**, populate the three severs to be used for BlackBerry Directory Lookup and Good Follow-Me. Again, leave the application configuration section blank.
4. Add **com.xyzcorp.gdservice-entitlement.presence** and **com.xyzcorp.gdservice-entitlement.directoryfollowme** to the appropriate application group(s).

5. Make sure that **com.good.gdservice-entitlement.enterprise** is NOT listed as an allowed application in the "Everyone" App Group.

Configuring User Affinity

For most other apps, user affinity is done via the security policy configuration of that app. BlackBerry Work, for example, has a section for entering affinity servers. Users are divided into different security policies as a means of determining which server affinity to use. With BlackBerry Dynamics Launcher, the same end-goal is accomplished by dividing users into different application groups.

For purpose of simplicity, assume a company plans to deploy all three of the above services on a BEMS host but these servers will be geolocated across the world and will have different and/or unique sets of users connecting to them. For example, lets say there's a company with three different offices located in San Francisco, London, and Tokyo. Ideally, you would configure Good Control in the following manner:

1. Create three (3) organization-level App IDs: **com.xyzcorp.gdservice-entitlement.enterprise.svl**, **com.xyzcorp.gdservice-entitlement.enterprise.ldn**, and **com.xyzcorp.gdserviceentitlement.enterprise.tyo**.
2. In Good Control, go to **Manage Apps** > **Add App** > **GD App ID and Version Only**.
3. Populate the server information for the new application IDs in Step 1 with the appropriate server clusters for each affinity. For example, com.xyzcorp.gdservice-entitlement.enterprise.svl would have its servers be strictly those located in Sunnyvale. Do the following:
    1. Go to **Manage Apps** > newly created App ID > **Good Dynamics** > **Server-Edit**
    2. Configure all the servers for this particular location
    3. Repeat Steps a–b for each app that were created in Step 1.
4. Assign each of the app IDs as providers of the three enterprise services listed under basic setup, as follows:
    1. Go to **Manage Apps** > newly created App ID > **Good Dynamics** > **Version-Edit**
    2. Click **Edit** for your version, then click the **Bind Service** button. Add all three services (Presence, Directory, FollowMe)
    3. Repeat Step a–b for each app created in Step 1.
5. Create a different **App Group** for each affinity.
6. Make sure that com.good.gdservice-entitlement.enterprise is NOT listed as an allowed application in the "Everyone" App Group.
7. Assign each new App ID as an allowed application to the respective application group. Since users can be part of multiple application groups, it would be ideal that these new affinity groups be strictly limited to allowed apps for that affinity.
8. Add users to the appropriate App Groups.

Additional Considerations

Since it is possible to mix and match multiple BEMS and user affinities, when desired, in deployments where there is a different Good Control server for different affinities, advanced setup may be unnecessary. This is because server configurations aren't shared across Good Control servers. The major thing to watch out for when performing custom setup is to ensure that a user will find only one provider of a particular service. If BlackBerry Dynamics Launcher detects multiple providers of a service, it will choose one at random (and likely remain with that choice if nothing changes). In setups where organization-level App IDs are created for complex server mapping, such a scenario could happen in the following ways:

1. com.good.gdservice-entitlement.enterprise is populated with server information and not removed from the "Everyone" application group.
2. Multiple organization-level App IDs are created that become providers of the same service and a user is granted access to them.
3. A user is added to more than one affinity App Group.

From the client perspective, the best way to debug this is by enabling detailed logging and looking through the logs to determine if more than one provider has been found.

Troubleshooting Launcher Performance

During Good Launcher setup in Good Control, your primary concern is making sure the configured services are visible to Good Launcher. If you use the Good Enterprise Services App ID com.good.gd-serviceentitlement. enterprise and it is incorrectly configured, the following log lines could appear.

```
No FollowMe service available
Unable to find Presence service provider
Unable to find Directory service provider
```

One of two things could be causing this:

- App IDs that are providers of server-side services will not show up for an app if there no servers are specified for this particular App ID.
- Although users can be allowed access to an ID on an individual basis, assigning a user to an application group is typically more efficient; the paritucular user in question may not belong to an App Group with access to this App ID.

Verify that servers are specified for this App ID

In Good Launcher, under **Apps**, click **Manage Applications**, select com.good.gdservice-entitlement.enterprise. Click the **BlackBerry Dynamics** tab, and add the pertinent FQDNs to the BEMS server cluster. For instructions, see Adding BEMS to the Good Enterprise Services entitlement app

Verify that the user is entitled to this App ID

Find the App Groups to which this user belongs and check to see that the Good Enterprise Services entitlement ID is set as an allowed application to at least one of the groups.

If the setup is correct and none of the log messages above show up, make sure detailed logging is enabled and check for the following log line:

```
Discovered <PROVIDERS COUNT> service providers for service: <SERVICE NAME> (using
first in list)
```

Here, <PROVIDER COUNT> should always be 1. If this number is greater than 1, it is because more than one app became a provider of one of the three enterprise services. If this provider happens to be an actual app that is installed on the device, it will show up as a provider, despite not listing any servers. Unfortunately, Launcher's logging doesn't list this case so it may be a challenge to track down the rogue provider. Future versions of BlackBerry Dynamics Launcher will address this issue.

```
Discovered <SERVER COUNT> servers for service provider: <SERVICE PROVIDER NAME>
```

Here, verify that the <SERVICE PROVIDER NAME> is the correct or intended provider. For setups using the Good Enterprise Services entitlement ID, the name should be BlackBerry Enterprise Mobility Server Entitlement.

If remedial action is taken to specify servers for this App ID or to add this user to an entitled App Group, BlackBerry Dynamics Launcher should now be attempting to connect to the appropriate BEMS host. Again, with detailed logging enabled, you should see the following:

```
Directory info request: <REQUEST URL>\n<REQUEST HEADERS> (directory info)
Presence subscribe request: <REQUEST URL>\n<REQUEST HEADERS>\n<JSON BODY> (presence)
```

If a connection error occurs, it could be for either of two reasons:

- The https connection could not be established
- The server returned with an error response.

If the former (a), the following log lines will appear:

```
Error in getting directory info (<ERROR CODE>): <ERROR REASON> (directory info)
Error in subscribing to presence (<ERROR CODE>): <ERROR REASON> (presence)
Connection error when trying to retrieve from FollowMe store: <ERROR REASON> (followme)
```

These log entries don't require detailed logging to be enabled. In such cases, first verify that the user is connected to the web, that the required BEMS hosts are each online, and that the server URL(s) specified for the provider(s) of the BlackBerry Dynamics Launcher services are correct.

For cases where the server returns an error code, this is likely no longer an issue with BlackBerry Dynamics Launcher, but something for the BEMS engineering support team to take a look at.

Appendix H: Microsoft Active Directory-based login for BEMS Dashboard and Web Console

31

As of BEMS version 1.4, both the Dashboard and Web Console support Microsoft Active Directory-based login. However, for versions of BEMS numbered 1.3.x and earlier, it is a recommended practice to change the administrator's password for the BEMS Dashboard UID/PWD, in accordance with your IT policy.

Change the GEMS Dashboard and Web Console login password

Complete the following to change the administration password in GEMS version 1.3.x and earlier:

1. In your favorite text editor, open <*GEMS Machine Path*>\Good Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<*version*>\etc\users.properties.
2. Change the current password from admin (the SHA-1 Hash below) to something else, after which, this will be the password for the GEMS Web. `Console.admin={CRYPT}a0089182becd921781d5ba1e58fa4d129b24060f{CRYPT}, _g_:admingroup ð admin=<new_password>,_g_:admingroup`. You can enter a plain text value. It will automatically be replaced with a salted SHA-256 Hash the next time an admin user logs in.
3. Save your changes.
4. Confirm the change by restarting the Good Technology Common Services and login to the GEMS Web Console by going to http://<*fqdn_of_ your_gems_host*>:8443/system/console/configMgr and using the new/changed password.

Appendix I – Migrating your Good Share database to BEMS-Docs

32

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 andGood 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 Good Control application policy for BlackBerry Work. Any Open-in lists created in Good Share must now be added in Good 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 J: AlwaysOn support for SQL Server 2012 and 2014

33

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. 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, see the Microsoft Documentation to read Overview of Always On Availabilty Groups.

Steps to setup SQL Server for AlwaysOn availability

When you setup SQL Server 2012 and SQL Server 2014, you perform the following actions:

Step	Action
1	Create an AlwaysOn availability group.
2	Configure SQL Server for AlwaysOn availability.
3	Install the BEMS software.
4	Configure the BEMS services databases for AlwaysOn availability.
5	Configure AlwaysOn availability group failover for single and multi-subnets for the following services: • 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 Upgrading the schema for 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. If necessary, click **Service Account** and enter the BEMS service account credentials.
3. Click **Database**.
4. In the **Server** field, enter the FQDN of the AlwaysOn Listener.
5. In the **Database** field, enter the name of the database that is added to the AlwaysOn Availability Group.
6. Click **Test** to test the connection.
7. Click **Save**.
8. Repeat steps 1 to 7 for the Connect and Docs services.

Enable 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, see the Microsoft Documentation to read Listeners, clients and failover.

1. On each computer that hosts BEMS, open the **Apache Karaf Web Console**. Open a browser window and navigate to **https://<*BEMS instance hostname*>:8443/system/console/configMgr**.
2. Scroll to and click **com.good.server.core.datasource**.

3. In the **jdbc.url** field, add the following property to the end of the connection string: **MultiSubnetFailover=true**. For example, **Jdbc:sqlserver://<*Listener value*>;databaseName=<*database name*>;integratedSecurity=true;MultiSubnetFailover=true;**.
4. Click **Save**.

Enable AlwaysOn availability group failover to subnets for the Connect service

You can enable availability group failovers to different subnets by setting MultiSubnetFailover to true for the Connect service. 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.

1. On each computer that hosts BEMS, in a text editor, open the GoodConnectServer.exe.config file. By default, the file is located in <*drive*>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\BlackBerry Connect\.
2. Search for the following configuration string: <**property name="connection.connection_string"**>.
3. Create the connection string for **MultiSubnetFailover=true**. For example, **Server=<*Listener value*>;Initial Catalog=<*database name*>;integratedSecurity=SSPI;MultiSubnetFailover=true;**.
4. Save the file.
5. Restart the Good Technology Connect service.

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 Upgrading the schema for BEMS.

Glossary

34

BEMS	BlackBerry Enterprise Mobility Server
CAS	Client Access Server
CSR	certificate signing request
DFS	distributed file system
FCM	Firebase Cloud Messaging
FQDN	fully qualified domain name
GCM	Google Cloud Messaging
GPO	Group Policy Object
IIS	Internet Information Services
MTLS	Mutual Transport Layer Security
NTLM	NT LAN Manager
SPN	Service Principal Name
SSL	Secure Sockets Layer

Legal

35

©2017 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.

Apache is a trademark of The Apache Software Foundation. Apple, iPad, and iPhone are trademarks of Apple Inc.Box is including without limitation, either a trademark, service mark or registered trademark of Box, Inc. Cisco Jabber is a trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Google, Android, Firebaseand Google Chrome are trademarks of Google Inc. iOS is a trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. Java is a trademark of Oracle and/or its affiliates. Kerberos is a trademark of the Massachusetts Institute of Technology. Mozilla Firefox is a trademark of Mozilla Foundation. Microsoft, Active Directory, ActiveSync, Excel, Internet Explorer, Lync, Office 365, Outlook, PowerPoint,SQL Server, SharePoint, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Skype is a trademark of Skype Corporation. 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, MERCHANTABLE 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