BlackBerry Enterprise Mobility Server

Configuring the BlackBerry Connect service

3.4

Contents

BlackBerry Connect service

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

Steps to configure the Connect service

When you configure the Connect service, you perform the following actions. If you installed the Connect service on multiple computers, complete this task on each computer that hosts the Connect service.

Step	Action
1	Configure the Connect service in the BEMS Dashboard.
2	Configure the Connect service for SSL communications using BlackBerry Proxy or Good Proxy.
3	Optionally, enable the Connect service to use a global catalog.
4	Add the computer, or computers if the Connect service is installed on multiple computers to the entitlement. See the instructions for your environment, • In a BlackBerry UEM environment, see "Configure BlackBerry Connect connection settings in BlackBerry UEM" in the BlackBerry Connect Administration content. • In a Good Control environment, see "Configure BlackBerry Connect connection settings in Good Control" in the BlackBerry Connect Administration content.

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, if you have an on-premises Microsoft Lync Server or Skype for Business server 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" in the Installation content.

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
- Configure Microsoft Lync Server 2013 or Skype for Business for the Connect service or Configure the BEMS-Connect service for Cisco Unified Communications Manager IM and Presence
- Optionally, Microsoft Exchange Server
- Optionally, Web proxy

Configure the Microsoft SQL Server database for the Connect service

Complete this task the first time that you configure the Connect service to specify the Microsoft SQL Server location and database for the Connect service.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Connect**.
2. Click **Service Account**, enter the BEMS service account credentials, and click **Save**.
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 Connect service uses the Windows credentials access the Microsoft SQL Server database.
   - If you select **SQL Server Login**, type the username and password used to access the Microsoft SQL Server database.
6. If your organization uses AlwaysOn support for SQL Server, in the **Additional Properties** field, type `MultiSubnetFailover=true`.
7. Click **Test** to verify the connection with the database.
8. Click **Save**.

Configure BEMS connectivity with BlackBerry Dynamics

The BlackBerry Dynamics server information in the following instructions refers to the FQDN of the server that hosts the BlackBerry Proxy or Good Proxy service. Complete this task to specify which BlackBerry Proxy or Good Proxy that the Connect service should use to complete processes (for example, authentication requests). You can specify the BlackBerry Proxy or Good Proxy server that the Connect service contacts first. When you specify the BlackBerry Proxy or Good Proxy, it forces BEMS to always communicate with this BlackBerry Proxy or Good Proxy server first. The Connect service uses the BlackBerry Proxy or Good Proxy server to create a list of BlackBerry Proxy or Good Proxy servers to use. If the BlackBerry Proxy or Good Proxy server that you specified in the BEMS Dashboard fails, then the Connect service contacts the next primary BlackBerry Proxy or Good Proxy server in the list.

In a BlackBerry UEM environment, the BlackBerry Proxy service is installed on on-premises BlackBerry UEM servers that have BlackBerry Connectivity Node. The BlackBerry Connectivity Node is required for some BlackBerry UEM Cloud deployments when they link a company directory to the BlackBerry UEM Cloud tenant and to offer on-premises connectivity to BlackBerry Dynamics users activated using the BlackBerry UEM Cloud. For more information about the BlackBerry Connectivity Node, see the BlackBerry UEM Planning content.

In a Good Control environment, the Good Proxy can be installed on the same server as Good Control or a different server that doesn't run Good Control. For more information about the Good Proxy, see the Good Control installation content.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Connect**.
2. Click **Service Account**, enter the BEMS service account credentials, and click **Save**.
3. Click **BlackBerry Dynamics**.
4. In the **Hostname** field, type the FQDN of the server hosting the BlackBerry Proxy or Good Proxy service.
5. In the **Port** field, the port number is prepopulated based on the communication type that you select.
   - If you select HTTP, the Port field prepopulates to 17080.
   - If you select HTTPS, the Port field prepopulates to 17433.

   Note: If you select HTTPS, you must import the trusted certificate to the Windows keystore. For instructions, see "Import the Good Proxy or BlackBerry Proxy CA certificate to the BEMS Windows keystore" in the BEMS-Core Configuration content.
6. Click **Test** to verify the connection to the BlackBerry Proxy or Good Proxy server.
7. Click **Save**.

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

You can configure your environment to work with Microsoft Lync Server and Skype for Business.

Before you begin:

- If your environment uses multiple Skype for Business on-premises servers using trusted application mode or non-trusted application mode, have the Skype for Business servers load balanced with a load balance server. For more information about load balancing requirements, visit https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/load-balancing.
- If your environment uses Skype for Business in non-trusted application mode, verify that you completed the prerequisite for the LyncDiscoverInternal DNS record. For more information about preinstallation requirements, see "BlackBerry Connect and BlackBerry Presence" in the BEMS installation content.

- If your environment uses Skype for Business in non-trusted application mode, import the certificate chain trust into the BEMS Java keystore to trust the HTTPS connections to LyncDiscoverInternal.example.com and the Skype Front End pool. For instructions on how to import the certificate chain, see "Import the CA certificate into the Java certificate store" in the BEMS-Core configuration content.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Connect**.
2. Click **Service Account**, enter the BEMS service account credentials, and click **Save**.
3. Click **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. Complete one of the following tasks:

Instant messaging server in environment	Tasks
Microsoft Lync Server 2013	**a.** 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 set up correctly or the service account does not have permissions to query these settings.
Skype for Business on-premises using trusted application mode **Note:** Using this configuration, the Connect service is trusted by Skype for Business and can impersonate a user. End user authentication is not required on the device to access BlackBerry Connect.	**a.** Select the **Skype for Business On-Premises** check box. **b.** Select **Trusted Application Mode**. **c.** Beside the **Application ID** dropdown list, click **Browse**. This step can take up to a minute to complete. **d.** In the **Application ID** drop-down list, select the app ID. For example, ***<appid_connect.mycompany.com>***. If the drop-down list is empty, either the BEMS <*instant messaging server type*> topology is not set up correctly or the service account does not have permissions to query these settings. **e.** If you enable persistent chat in your Skype for Business 2015 environment, in the **Persistent Chat Default Category** field, enter the default category. For more information on enabling persistent chat, see the BlackBerry Connect Administration content.

Instant messaging server in environment	Tasks
Skype for Business on-premises using non-trusted application mode **Note:** Using this configuration, the Connect service is not trusted by Skype for Business and cannot impersonate a user. End user authentication on the device is required to access BlackBerry Connect.	**a.** Select the **Skype for Business On-Premises** check box. **b.** Select **Non-trusted Application Mode**. **c.** Complete one or both of the following actions: • Select the **Auto discover servers** checkbox for BEMS to use the existing DNS records of LyncDiscoverInternal to discover the Skype for Business servers in the environment. For more information about preinstallation requirements, see "BlackBerry Connect and BlackBerry Presence" in the BEMS installation content. • Enter the default Skype for Business on-premises FQDN or the complete URL to the Skype for Business server for BEMS to use if autodiscovery is not enabled or fails. For example, http(s)://<*FQDN_of_the Skype_front_end_pool*>/Autodiscover/AutodiscoverService.svc/root/oauth/user. **Note:** The certificate chain trust must be imported into the BEMS Java keystore to trust the HTTPS connections to LyncDiscoverInternal.example.com and the Skype Front End pool. For instructions on how to import the certificate chain, see "Import the CA certificate into the Java certificate store" in the BEMS-Core configuration content.

5. Verify that the Azure information is accurate and log in to the user account:
   - If you configure the environment to use Skype for Business On-Premises using non-trusted application mode
     a. Click **Test**.
     b. Enter a user email address and password.
     c. Click **Test**.
6. Click **Save**.

After you finish:

For more information about available settings in the BEMS-Connect configuration files, see Appendix: Understanding the BEMS-Connect configuration file.

Changing users' SMTP addresses

BEMS supports changing users' SMTP addresses without requiring the user to provision their BlackBerry Connect app. Previously, if a user changed their primary email address they needed to reprovision their BlackBerry Connect app if they were unable to log in to the app, if they missed message notifications, or the presence status didn't update for other users. BEMS now detects the primary SMTP address change and updates the BEMS database with the new SMTP address automatically.

Configuring the BEMS-Presence and BEMS-Connect services in a multi-cluster Cisco Unified Communications Manager for IM and Presence environment

You can configure the BEMS-Presence and BEMS-Connect services for users that are located in multi-cluster 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 multi-cluster 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 a multicluster Cisco Unified Communications Manager IM and Presence environments for BlackBerry Connect and BlackBerry Presence services

When you configure a multicluster Cisco Unified Communications Manager IM and Presence environment 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 Publisher in each CUCM cluster in a multi-cluster environment. 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. The AXL application user must be a user that is in a group that is assigned the Standard AXL API Access role. For more information, see your Cisco documentation. For BlackBerry Presence • Application user and password. For instructions, see "Create an Application User" in the Installation content. • UDS Username (Dummy user). For instructions, see "Create a Dummy User" in the Installation content.

Step	Action
3	Download the required certificates from each cluster. • Tomcat.der • Cup.der • Cup-xmpp.pem and Cup-xmpp-ECDSA.pem • Cup-ECDSA.der and Tomcat-ECDSA.der • 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 CA certificate into the Java certificate store" in the BEMS-Core configuration content.
5	Configure the BlackBerry Connect service.
6	Configure the BlackBerry Presence service.

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 and Cup-xmpp-ECDSA.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.
- Cup-ECDSA.der and Tomcat-ECDSA.der
  - 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 and cup-xmpp-ECDSA certificate as a .pem file.
9. Download the following .der files:
   - cup certificate
   - Cup-ECDSA
   - Tomcat-ECDSA

After you finish: Import these certificates into the BEMS Java keystore. For instructions, see "Import the CA certificate into the Java certificate store" in the BEMS Core configuration content.

Configure the BEMS-Connect service for Cisco Unified Communications Manager IM and Presence

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 Application user username** and **AXL Application password**. The AXL Application user must be in a group that is assigned the Standard AXL API Access role. For more information, see your Cisco documentation.
   - 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. In the **Cisco Unified Communications Manager IM and Presence XMPP client service port** field, enter the outbound port that points to the Cisco Jabber XMPP Service. By default this 5222.
10. Start the Good Technology Connect service.

Configure BEMS to access on-premises Microsoft Exchange Server conversation histories

Note: Complete this task only if your environment includes an on-premises Microsoft Exchange Server. If your environment uses Microsoft Exchange Online, complete the instructions in Configure BEMS to access Microsoft Exchange Online conversation histories. Enable this feature to imitate a user's desktop client experience when they save the history of a BlackBerry Connect chat to their Microsoft Exchange Server mailbox.

You can enable the conversation history to allow users to access conversations that are saved in the Conversation History folder of the user's Microsoft Exchange mailbox. Saving the conversation history is

- Supported in a Skype for Business on-premises where users have mailboxes on an on-premises Microsoft Exchange Server environments.
- Not supported in an on-premises Skype for Business environment where users have mailboxes on Microsoft Office 365.

Before you begin:

- Enable Autodiscovery on the Microsoft Exchange Server. For instructions, see your Microsoft Exchange Server documentation.
- Integrate the Microsoft Lync Server or Skype for Business integration with the Microsoft Exchange Server. For instructions, see your Microsoft Exchange Server and Microsoft Lync Server or Skype for Business documentation.
- Install the Microsoft Exchange Server SSL certificates on the computer that hosts the Connect service. If you do not correctly install the SSL certificate on the computer that hosts the Connect service, the history logging to the Microsoft Exchange Server will fail. For instructions, see your Microsoft Exchange Server documentation.
- Verify that conversation history is enabled on the enterprise Microsoft Lync Server 2013 or Skype for Business for which you configure BlackBerry Connect. For information about the supported instant messaging servers, see the BEMS Compatibility Matrix.
- Verify that the Microsoft Lync Server or Skype for Business topology for BEMS is prepared. For instructions, see "Preparing the Microsoft Lync Server and Skype for Business topology for BEMS" in the Installation content.
- Grant application impersonation permission to the BEMS service account on the Microsoft Exchange Server.

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. Grant the account application impersonation permissions to the BEMS service account. For instructions, Grant application impersonation permissions to the BEMS service account.
5. Click **Test**.
6. Click **Save**.

Grant application impersonation permissions to the BEMS service account

Complete this task only if your environment has an on-premises Microsoft Exchange Server. For the Connect service to save instant messaging chats to the Microsoft Exchange Server Conversation History, the Connect service account must have impersonation permissions. Complete this task if you use a different service account for Connect.

Execute the following Microsoft Exchange Management Shell command to apply Application Impersonation permissions to the Connect service account. This task enables application impersonation for all users to the Connect service account.

1. On the Microsoft Exchange Server open the Microsoft Exchange Management Shell.
2. Type `New-ManagementRoleAssignment -Name:<ImpersonationAssignmentName> -Role:ApplicationImpersonation -User:<ConnectServiceAccount>` (for example, `New-ManagementRoleAssignment -Name:BlackBerryAppImpersonation -Role:ApplicationImpersonation -User ConnectAdmin`).

Configure BEMS to access Microsoft Exchange Online conversation histories

Note: Complete this task only if your environment includes a Microsoft Exchange Online. If your environment uses an on-premises Microsoft Exchange Server, complete the instructions in "Obtain an Azure app ID for the BEMS-Docs component service" in the Configuring BlackBerry Docs content.

If you configure the Connect service, you can enable the conversation history to allow users to access conversations that are saved in the Conversation History folder of the user's Microsoft Exchange mailbox. Saving the conversational history is

- Supported in a Skype for Business on-premises environment where users have mailboxes on an on-premises Microsoft Exchange Server.
- Supported in an on-premises Skype for Business environment where users have mailboxes on Microsoft Office 365.

Configure the web proxy for the Connect service

Complete this task if your organization uses a web proxy server to connect to the Internet. It is recommended to use the same web proxy server in the Connect component as in the BEMS-Core component. When you configure the web proxy, the BEMS Connect configuration file (GoodConnectServer.exe.config) updates the GD_APN_PROXY_HTTP_HOST and GD_APN_PROXY_HTTP_PORT parameters. For more information about the BEMS Connect configuration file, see Understanding the BEMS-Connect configuration file.

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**.

Sending files in one-to-one chats

Users can send and receive files in one-to-one chats when you configure the Connect service with one of the following instant messaging servers and users are running Connect 3.5 or later:

- Skype for Business 2015 or 2019 on-premises using trusted application mode
- Microsoft Lync Server 2013

For more information about restricting the files that users can send in chats, 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 2015, you can enable it in your BEMS environment.

Note: Persistent chat is not supported in Skype for Business 2019 environments.

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

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

Optionally, you can configure the Connect service to always use a BlackBerry Proxy or Good Proxy that you specified in the BlackBerry Dynamics settings instead of the temporary list that is generated regularly. For more information, see Configure BEMS connectivity with BlackBerry Dynamics. The Connect service contacts the BlackBerry Proxy or Good Proxy in the generated temporary list to verify authentication of users' Connect clients. By default, this feature is disabled.

Before you begin:

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

1. 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\Good Connect\`.
2. Add the following key and value to the file: type `<add key="ENABLE_CONFIGURED_GP_PIN" value="true" />`.
3. Save the file.
4. 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. If you installed the Connect service on multiple computers, complete this task on each computer that hosts the service.

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 SSL certificate requirements for Microsoft Lync Server and Skype for Business in the Installation content.

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. In the **<appSettings>** section, 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.

Configure the Connect service to receive SSL communications for a new installation

By default, SSL is enabled when you install the Connect service and runs securely using SSL/TLS (HTTPS) to communicate with the BlackBerry Connect app over port 8082. By default, the BEMS installer generates a secure certificate that is bound to port 8082. Optionally, you can choose to manually create a secure certificate that you must import to BEMS and bind to port 8082 or another available port. If you upgrade from BEMS 2.10 or earlier, see Options to configure the Connect service to receive SSL communications from an upgraded BEMS instance for available options.

If you installed the Connect service on multiple computers, complete this task on each computer that hosts the Connect service.

For SSL support, you perform one of the following actions based on your environment

- Use the default BEMS-Connect SSL certificate that is generated by the BEMS installer and the default port number. In this scenario, you must Assign the BEMS-Connect SSL certificate to users.
- Use the default BEMS-Connect SSL certificate that is generated by the BEMS installer, but your environment requires that you use a different port number. In this scenario, you must complete the following steps:
  1. Unbind the SSL certificate from port 8082.
  2. Bind the SSL certificate to the Connect service SSL port.
  3. Update the port number to enable SSL for BEMS Common and Connect service.
  4. Assign the BEMS SSL certificate to users.
  5. Configure the BlackBerry Connect app to send requests over SSL. For more information, see 'Configuring BlackBerry Connect app settings' in the BlackBerry Connect administration content.
- Use your own SSL certificate and the default port number. In this scenario you must complete the following steps:
  1. Create a CSR request.
  2. Submit a CSR request to a certificate authority. You must install the certificate on the server that generated the CSR.
  3. Import the signed certificate to the computer that hosts the Connect service.
  4. Import the certificate into the Java keystore. For more information, see 'Keystore commands' in the BEMS-Core configuration content.
  5. Bind the SSL certificate to the Connect service SSL port
  6. Add the certificate friendly name to the BlackBerry Connect server configuration file.
  7. Assign the BEMS-Connect SSL certificate to users
  8. Configure the BlackBerry Connect app to send requests over SSL. For more information, see 'Configuring BlackBerry Connect app settings' in the BlackBerry Connect administration content.

Options to configure the Connect service to receive SSL communications from an upgraded BEMS instance

If you upgraded from BEMS version 2.10 or earlier, select one of the following scenarios:

- You want to upgrade your BEMS instance, don't have the Connect service configured for secure connections, and don't require secure connections. In this scenario, you are not required to complete any additional upgrade steps.
- You want to upgrade my BEMS instance and am already using secure connections and want to keep this configuration. In this scenario, you are not required to complete any additional upgrade steps.

- You want to configure a non-secure connection environment to a secure connection environment. In this scenario, you must choose one of the following options:
  - Configure BEMS-Connect to use a secure connection using the default installation SSL certificate generated by the BEMS installer
  - Configure BEMS-Connect to use a secure connection using your own SSL certificate

Configure BEMS-Connect to use a secure connection using the default installation SSL certificate generated by the BEMS installer

Complete the tasks for your environment.

Task	Steps
If you have a BlackBerry UEM environment	**a.** Bind the SSL certificate to the Connect service SSL port. **b.** Enable SSL communications. **c.** Configure the BlackBerry Connect app to send requests over SSL. **d.** Assign the BEMS-Connect SSL certificate to users.
If you have a Good Control environment	**a.** Bind the SSL certificate to the Connect service SSL port. **b.** Enable SSL communications. **c.** Configure Good Control to send requests over SSL. For more information, see 'Configuring BlackBerry Connect app settings' in the BlackBerry Connect administration content. **d.** Configure the Connect service to use SSL with the Good Proxy. For more information, see 'Configuring HTTPS for BEMS to the BlackBerry Proxy or Good Proxy server' in the BEMS-Core configuration content. **e.** Assign the BEMS-Connect SSL certificate to users.

Configure BEMS-Connect to use a secure connection using your own SSL certificate

1. Create a CSR request.
2. Submit a CSR request to a certificate authority. You must install the certificate on the server that generated the CSR.
3. Import the signed certificate to the computer that hosts the Connect service.
4. Import the certificate into the Java keystore. For more information, see 'Keystore commands' in the BEMS-Core configuration content.
5. Bind the SSL certificate to the Connect service SSL port.
6. Enable SSL communications.
7. Assign the BEMS-Connect SSL certificate to users.
8. Configure the Connect service to use SSL with the Good Proxy. For more information, see 'Configuring HTTPS for BEMS to the BlackBerry Proxy or Good Proxy server' in the BEMS-Core configuration content.

Create a CSR request

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. In the **Certificates snap-in wizard**, select **Computer account**. Click **Next**.
7. On the **Computer > Select Computer** screen, select **Local Computer**. Click **Finish**.
8. Click **OK**.
9. In the Microsoft Management Console, expand **Certificates (Local Computer)**.
10. Right-click **Personal** and click **All Tasks > Advanced Operations > Create Custom Request**.
11. In the **Certificate Enrollment** wizard, click **Next**.
12. On the **Select Certificate Enrollment Policy** screen, select **Proceed without enrollment policy**. Click **Next**.
13. On the **Custom request** screen, select the following settings:
    - In the **Template** field, select **(No template) Legacy key**
    - In the **Request format** option, select **PKCS #10**
14. Click **Next**.
15. On the **Certificate Information** screen, expand **Details** for the custom request.
16. Click **Properties**.
17. Click the **Subject** tab.
18. On the **Subject** tab, in the **Subject name** section, complete the following actions:
    a) In 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**.
19. In the **Alternative name** section, add two values by completing the following actions:
    a) In 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**.
20. On the **Extensions** tab, complete the following actions:
    a) In the **Extended Key Usage (application policies)** drop-down list, in the **Available options** column, click **Server Authentication**.
    b) Click **Add**.
21. On the **Private Key** tab, complete the following actions:
    a) In the **Cryptographic Service Provider** drop-down list, in the **Select cryptographic service provider(CSP)** section, clear all the check boxes.
    b) Select the **Microsoft RSA SChannel Crytographic Provider (Encryption)** check box.
    c) In the **Key size** field, type `2048`.
    d) In the **Key options** drop-down list, in the **Key type** drop-down list, select **Exchange**.
22. Click **Apply**.
23. Click **OK**.
24. Click **Next**.
25. Enter a name for the certificate request and save it to your desktop.

26. In the **File format** section, select **Base 64**.
27. Click **Finish**.

After you finish:

1. Submit the certificate request that you created to the certificate authority to obtain a certificate.
2. Import the signed certificate to the computer that hosts the Connect service

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

Make sure that you install the certificate on the server that generated the CSR.

1. If necessary, open the Microsoft Management Console (MMC).
2. Expand **Certificates (Local Computer)**.
3. Right-click **Personal** and click **All Tasks > Import**.
4. Click **Next**.
5. Navigate to the certificate file that you obtained from the certificate authority.
6. Click **Next**.
7. On the **File to Import** screen, select the file and click **Open**
8. Click **Next**.
9. In the **Certificate Store** screen, click **Browse** and click **Trusted Root Certification Authorities**.
10. Click **Next**.
11. Click **Finish**.

After you finish: 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.

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. If required, login to the computer that hosts the Connect service with the service account.
3. Open a command prompt (run as administrator).
4. Check that a certificate is not already bound to port 8082. Type `netsh http show sslcert`. If you use a new certificate, document the hash information for port 8082. The certificate hash is used in step 4.

   If a certificate is bound to port 8082 or a port that you want to use, 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` or the port that you want to bind the certificate to.

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

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

After you finish:

1. Enable SSL communications.
2. Configure your environment to send requests over SSL. For more information, see 'Configuring BlackBerry Connect connection settings' in the BlackBerry Connect administration content.

Enable SSL communications

You must enable SSL in two locations; the BlackBerry Connect server configuration file and the BEMS Common to Connect communications.

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

1. Enable SSL communications in the Connect service.
   a) 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\`.
   b) In a text editor (run as administrator), edit the **GoodConnectServer.exe.config** file.
   c) Locate the BASE_URL line (for example, `<add key="BASE_URL" value="http://*:8080/"/>`).
   d) Change the line to `<add key="BASE_URL" value="https://*:8082/"/>`. If required, update the port to the port that you are using.
   e) Save your changes.
   f) Restart the Good Technology Connect service.
2. Enable SSL for BEMS Common to Connect communications
   a) On the computer that hosts BEMS, open the Apache Karaf Web Console. Open a browser window and navigate to `https://<fqdn_of_the_bems_host>:8443/system/console/configMgr`.
   b) Scroll to and click **com.good.gcs.connect.adapter.core.config.CoreSettingsImpl.name**.
   c) In the **com.good.gcs.connect.adapter.core.config.CoreSettingsImpl.connect.websocket.uri.name** field, verify that URI is `wss://localhost:8082/ AdapterNotifyService/Notify/ws`. If necessary, change the port to the port you want to use.
   d) Click **Save**.

After you finish:

Configure your environment to send requests over SSL. For more information, see 'Configuring BlackBerry Connect connection settings' in the BlackBerry Connect administration content.

Configure the BlackBerry Connect app to send requests over SSL

Before you begin: If you configured the BlackBerry Connect app configuration to use the default port of 8080, you can update the app configuration to use the SSL port information.

Complete the instructions in the *Configure BlackBerry Connect app settings* in the BlackBerry Connect Administration content. For the Connect Server Hosts field, make sure you type the FQDN of the computers that host the BlackBerry Connect server and use the SSL port 8082. For example, if you have multiple servers,

separate the names using commas, no spaces. For example, https://domain01.example.com:8082,https://domain02.example.com:8082,https://domain03.example.com:8082.

Assign the BEMS-Connect SSL certificate to users

By default, BEMS-Connect uses a self-signed certificate that is generated by the BEMS installer.

1. Complete one of the following tasks:
   - If you use the default SSL certificate generated by the BEMS installer,
     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.
   - If you use your own SSL certificate,export the SSL certificate chain from the Microsoft Management Console (MMC). If you don't know which certificate chain to download, in a command prompt type `netsh http show sslcert` to confirm the certificate hash, then use the MMC to locate the certificate where the certificate thumbprint is the same as the certificate hash.
     a. Open the Microsoft Management Console (MMC).
     b. Click **Console Root**.
     c. Click **File > Add/Remove Snap-in**.
     d. In the **Available snap-ins** column, click **Certificates > Add**.
     e. In the **Certificates snap-in wizard**, select **Computer account**. Click **Next**.
     f. On the **Computer > Select** Computer screen, select **Local Computer**. Click **Finish**.
     g. Click **OK**.
     h. In the **MMC**, expand **Certificates (Local Computer) > Personal** .
     i. Double-click the SSL certificate.
     j. Click **Certification Path**.
     k. Click the root certificate. The root certificate is the first item in the Certificate hierarchy.
     l. Click **View Certificate**.
     m. Click the **Details** tab.
     n. Click **Copy to File**.
     o. Click **Next**.
     p. Enter name for the certificate and export it to your desktop.
     q. Click **Save**.
     r. Click **Finish**.
     s. Click **OK**.
2. Complete one of the following:
   - In BlackBerry UEM environment, create a CA certificate profile for the BEMS Self-Signed certificate, or create individual CA certificate profiles for the CA Root certificate and any CA Intermediate certificates. Assign the profiles to users or user groups. For instructions on creating a CA certificate profile and assigning it to users or user groups, see the BlackBerry UEM administration content.
   - In a Good Control environment, complete the following
     a. Under **Settings**, click **Server Certificates**.
     b. On the **Trusted Authorities** tab, click the Add icon and navigate to the certificate and upload it.
     c. Click **Apply**. Good Control automatically distributes the CA certificate to all BlackBerry Dynamics apps, including BlackBerry Connect.

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. In the BEMS Dashboard, configure each new Connect instance to point to the same BlackBerry Proxy or Good Proxy server.
3. Perform one of the following actions:

Environment	Tasks
If you have a BlackBerry UEM environment	**a.** In the BlackBerry UEM console, add the new computer hosting the Connect service instance to BlackBerry UEM. **b.** Add each new computer hosting the Connect instance to the BlackBerry Connect app settings.
If you have a Good Control environment	**a.** Whitelist each new Connect server host and port in Good Control. **b.** Configure each new Connect instance in Good Control for the BlackBerry Connect app.

Disaster recovery

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

Troubleshooting the Connect service

The Connect log files contain critical information for the instant messaging server that is used in your environment and are required when troubleshooting Connect issues. For information about the location of the log files and the information each Connectlog file logs, see the Monitoring and reporting content.

Next steps

After you complete the tasks to configure the Connect service, see to the following guides to configure the necessary services and install and configure BlackBerry Dynamics apps:

- The BlackBerry Connect app: The BlackBerry Connect app provides secure instant messaging calendar, company directory look-up, and user presence information to iOS and Android devices. For more information about managing BlackBerry Connect, see the BlackBerry Connect Administration content.
- BlackBerry Docs service: This service lets your BlackBerry Dynamics app users access, synchronize, and share documents 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 Mail (BlackBerry Push Notifications) service: This service accepts push registration requests from iOS and Android devices, and then communicates with the on-premises Microsoft Exchange Server or Microsoft Office 365 using it's Microsoft Exchange Web Services protocol to monitor the user's enterprise mailbox for changes.
- BlackBerry Presence service: This service provides real-time presence status to BlackBerry Work, BlackBerry Dynamics Launcher, and third-party BlackBerry Dynamics apps.

Appendix: Understanding the BEMS-Connect configuration file

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. If you manually update the configuration file, complete this task on each computer that hosts the Connect service.

Note: Stop the Good Technology Connect service before you update the configuration file, make your changes, and start the service on BEMS 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.	50
AD_USERS_SOURCE	—	Parameter indicates if the Connect service should connect to Microsoft Active Directory Global Catalog servers or use the distinguished name 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 can be the distinguished name of the domain or the fully qualified domain name; for example, DC=EXAMPLE,DC=COM or EXAMPLE.COM, respectively.	
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/	https://*:8082/
BUILD_VERSION	√	The version number of the BlackBerry Connect server build.	Auto-populated
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

Parameter name	Required	Description	Default setting
DISABLE_MESSAGEUPDATE	—	Disable message not delivered errors which may potentially be due client and network latencies.	False
DISABLE_SSL_CERT_CHECKING	—	Disables certificate validation when the Connect service connects to the Notifications service. For example, <add key="DISABLE_SSL_CERT_CHECKING" value="true" />	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 Microsoft Lync Server or Skype for Business server is federated (connected) with your company's Microsoft Lync Server or Skype for Business server.	False
ENABLE_PERSISTENT_CHAT	—	Enables persistent chat features in BEMS, enabling users to create and participate in group discussions. Requires that the feature is enabled in Microsoft Lync Server 2013 or Skype for Business 2015 server. For more information about enabling persistent chat, see the BlackBerry Connect Administration content.	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

Parameter name	Required	Description	Default setting
EWS_HISTORY_FOLDER_NAME	—	Name of the folder in users' Microsoft Exchange mailbox where conversations are saved and accessible by the users. For more information about enabling conversation history, see Configure BEMS to access on-premises Microsoft Exchange Server conversation histories. For information on changing the Conversation History folder name to a localized name (for example, Historique des conversations), visit http://support.blackberry.com/community to read article 71402.	
EWS_HOST	—	FQDN of the Microsoft Exchange Server to which the BlackBerry Connect server writes conversation histories.	
EWS_VERSION	—	EWS_Version parameter number and corresponding Microsoft Exchange Server version • 1 = Microsoft Exchange Server 2010 • 2 = Microsoft Exchange Server 2010 SP1 • 3 = Microsoft Exchange Server 2010 SP2 • 4 = Microsoft Exchange Server 2010 SP3 • 5 = Microsoft Exchange Server 2013 • 6 = Microsoft Exchange Server 2016 and Microsoft Exchange Server 2019 • 100 = Microsoft Exchange Online	2
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

Parameter name	Required	Description	Default setting
GD_APN_PROXY_AUTH _USERNAME	—	Web Proxy Username	Deprecated
GD_APN_PROXY_HTTP_HOST	—	Web Proxy Host	
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://example.com:17433.	
IS_ON_PREM_ENABLED	—	This setting specifies that the Connect service is configured to work with Skype for Business on-premise.	False
IS_TRUSTED_APP_MODE	—	This setting specifies that the Connect service is configured to work with Skype for Business on-premises and uses trusted application mode to obtain user information.	True
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_SERVER	√	The FQDN of the Microsoft Lync Front-End server or Front-End server pool.	LYNC FQDN
LYNC_PORT		The port number of the Microsoft Lync Front-End server or Front-End server pool.	5061

Parameter name	Required	Description	Default setting
PCHAT_DEFAULT_CATEGORY_ID	—	Specifies the default persistent chat category for users. For more information about enabling persistent chat, see the BlackBerry Connect Administration content.	
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
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: Global catalog for Connect and Presence

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.

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.

In addition to configuring the Connect and Presence services to use the global catalog, you must replicate some additional Microsoft Lync Server or Skype for Business attributes to the global catalog. You must perform this set up only once, whether the global catalog is used for one or both services. Some environments might require some Active Directory attributes to be correctly replicated to the global catalog in the other domains. For more information about enabling replication of user attributes to the global catalog server, visit support.blackberry.com/community to read article 46152.

Enable the Connect service to use a global catalog

The instructions in this topic use the environment example.com to configure the Connect service to use a global catalog. If you installed the Connect service on multiple servers, complete this task on each computer that is running the Connect service.

1. 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.
2. In the <appSettings> section of the file, locate the following values:
   - <addkey = "AD_USERS_SOURCE" value= "" />
   - <addkey = "AD_USERS_SOURCE_DOMAIN" value="" />
3. Update the values as required for your environment. For example, to configure the Connect service to access Active Directory domains outside of the local domain that the BEMS is located in, complete the following steps:
   a) In the value double quotation marks of the <addkey = "AD_USERS_SOURCE" value= "" /> key, enter `GC`.
   b) In the value double quotation marks of the <addkey = "AD_USERS_SOURCE_DOMAIN" value="" /> key, enter `DC=EXAMPLE,DC=COM` or the fully qualified domain name `EXAMPLE.COM`. Make sure that you use the distinguished name of the domain. For more information, see Appendix: Understanding the BEMS-Connect configuration file.

   The following example shows the GoodConnectServer.config file configured to access a global catalog:

```
.
.
<!-- valid values are: GC - Global Catalog; LDAP - Active Directory (default)
 -->
<add key="AD_USERS_SOURCE" value="GC" />
```

```
<!-- valid values are: "DC=GOOD,DC=COM" - GC/AD at good.com (example only,
 change to your domain); No value attribute (default) - Domain the Good
 Connect resides; -->
<add key="AD_USERS_SOURCE_DOMAIN" value="DC=EXAMPLE,DC=COM" />
.
.
```

4. In the Windows Manager, restart the Good Technology Connect service.

Revert the Connect service settings to use the local Active Directory

If you configured the Connect service to use a global catalog, you can modify the GoodConnectServer.exe.config file to have the Connect service use the local Active Directory domain that the BEMS is located in. In the following example, the Connect service was configured to use the global catalog in the example.com environment. If you installed the Connect service on multiple servers, complete this task on each computer that is running the Connect service.

1. 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.
2. In the <appSettings> section of the file, locate the following values:
   - <addkey = "AD_USERS_SOURCE" value= "GC" />
   - <addkey = "AD_USERS_SOURCE_DOMAIN" value="DC=EXAMPLE,DC=COM" />
3. Remove the specified values from the double quotation marks. The following example shows the GoodConnectServer.exe.config file configured to use the local Active Directory domain where the BEMS is located:

```
.
.
<!-- valid values are: GC - Global Catalog; LDAP - Active Directory (default)
 -->
<add key="AD_USERS_SOURCE" value="" />
<!-- valid values are: "DC=GOOD,DC=COM" - GC/AD at good.com (example only,
 change to your domain); No value attribute (default) - Domain the Good Connect
 resides; -->
<add key="AD_USERS_SOURCE_DOMAIN" value="" />
.
.
```

4. In the Windows Manager, restart the Good Technology Connect service.

Enable Microsoft Lync Server or Skype for Business related attributes in the global catalog

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 following attributes:
    - msRTCSIP-PrimaryUserAddress
    - msRTCSIP-UserEnabled
    - msRTCSIP-DeploymentLocator
    - telephoneNumber
    - displayname
    - title
    - mobile
    - givenName
    - sn
    - sAMAccountName

Appendix: Updating the Connect and Presence services using Lync Director

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 service to use a Lync Director

1. On the BEMS host, stop the **Good Technology Connect** service.
2. Update the BlackBerry Connect configuration file. By default, the GoodConnectServer.exe.config file is located in `<drive>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Connect`.
   a) On the BEMS host, navigate to the GoodConnectServer.exe.config file.
   b) In a text editor, open the GoodConnectServer.exe.config file.
   c) Locate the LYNC_SERVER key and update the value with the FQDN of the Director pool that you want to use.
3. On the BEMS host, start the Good Technology Connect service.

Legal notice

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

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

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

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

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

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

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

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

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

Published in Canada