



# **BlackBerry Enterprise Mobility Server**

## **Configuring the BlackBerry Presence service**

3.4



# Contents

- BlackBerry Presence service.....5**
- Configuring the BlackBerry Presence service.....6**
- Configuring the BlackBerry Presence service in the BEMS Dashboard.....7**
  - Logging in to the Presence service..... 7
  - Configure the BlackBerry Presence service settings..... 7
    - Allow Presence subscriptions to users in specified domains.....8
    - Remove a domain and restrict users from requesting subscription requests..... 8
  - Configure Microsoft Lync Server 2013 or Skype for Business for the Presence service.....9
  - Configure Jabber for the Presence service..... 11
  - Manually configure the Presence service for multiple application endpoints..... 11
  - Using friendly names for certificates in Presence..... 12
    - Change the certificate friendly name description..... 13
    - Add the certificate friendly name to the Presence server configuration file..... 13
  - Configuring the BEMS-Presence and BEMS-Connect services in a multi-cluster Cisco Unified Communications Manager for IM and Presence environment..... 14
    - Steps to configure a multicluster Cisco Unified Communications Manager IM and Presence environments for BlackBerry Connect and BlackBerry Presence services..... 14
    - Download certificates from the Cisco Unified Communications Manager and Cisco IM and Presence servers into the BEMS Java keystore..... 15
- Configuring the Presence service for high availability..... 17**
- Disaster recovery..... 18**
- Troubleshooting the Presence service..... 19**
- Next steps.....20**
- Appendix: Updating the Connect and Presence services using Lync Director... 21**
  - Specify the Presence service to use a Lync Director.....21
- Appendix: Global catalog for Connect and Presence..... 22**
  - Enable the Presence service to use a global catalog with Microsoft Lync Server or Skype for Business.....22
  - Revert the Presence service settings to use the local Active Directory.....23
  - Enable Microsoft Lync Server or Skype for Business related attributes in the global catalog..... 23

**Legal notice..... 25**

# BlackBerry Presence service

You can configure the Presence service to provide real-time presence status to BlackBerry Work app users, the BlackBerry Dynamics Launcher, and third-party BlackBerry Dynamics apps.

# 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 one of the following actions.

- If your environment includes a Microsoft Lync Server or Skype for Business:
  - [Configure BlackBerry Presence in the BEMS Dashboard.](#)
  - [Manually configure the Presence service for multiple application endpoints.](#)
  - Optionally, [enable the Presence service to use a global catalog.](#)
  - Optionally, [configure the Presence service for high availability.](#)
  - Optionally, [configure the Presence service for disaster recovery.](#)
- If your environment includes a Cisco Unified Communications Manager (Cisco Jabber):
  - [Configure BlackBerry Presence in the BEMS Dashboard.](#)
  - [Configure Jabber for the Presence service](#)
  - Optionally, [configure the Presence service for high availability](#)
  - Optionally, [configure the Presence service for disaster recovery.](#)
  - Add the computer, or computers if the Presence service is installed on separate computers to the entitlement. For instructions, see "[Configure BlackBerry Work connection settings](#)" in the BlackBerry Work administration content.

# Configuring the BlackBerry Presence service in the BEMS Dashboard

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

- If not completed when you configured the BEMS-Core settings, [configure BlackBerry Dynamics in the BEMS-Core configuration content](#).
- If your environment uses Skype for Business, [log in with the service account credentials](#).
- Optionally, [configure the BlackBerry Presence service settings](#).
- [Configure Microsoft Lync Server 2013 or Skype for Business for the Presence service](#).
- [Configure Jabber for the 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.

## Configure the BlackBerry Presence service settings

You can specify the basic and common settings for the BlackBerry Presence service or keep the default settings. These settings are irrespective of the instant messaging server you use in your environment.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Presence**.
2. If your environment uses a Microsoft Lync Server or Skype for Business, click **Service Account** and type the login credentials for the Good Technology Presence 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. For example, if user A opens BlackBerry Work to view an email from user B, BlackBerry Work contacts the Presence service for user B's presence status. If user A then doesn't view user B's contact information in the Inbox, contacts, or calendar for longer than the expiration time, BlackBerry Work must contact the Presence service again for updated user B presence status. By default, this is 180 seconds. If you experience issues with the Presence status not displaying, increase the subscription expiration time (for example, 1000 seconds). Increasing the expiration time allows the subscriptions to remain active for a longer time.
5. Optionally, select the **Enable domain whitelisting** checkbox. For more information, see [Allow Presence subscriptions to users in specified domains](#).
  - a) In the **Domains whitelist** dialog box, click  .

b) In the **Domains whitelist** text box, type the email domains for which you want to allow presence subscriptions. When adding multiple domains, you can add the domains using one or more of the following formats to separate the domains.

- Comma
- Semi-colon
- Space
- New line

For example, example.com, example1.com, and so forth.

c) Click .

6. Click **Test**.

7. Click **Save**.

### **Allow Presence subscriptions to users in specified domains**

Your organization can use whitelisting to control which users in internal and federated Microsoft Lync Server 2013, Skype for Business, or Cisco Unified Communications Manager environments can be subscribed to. By allowing specific email domains to be subscribed to, you can improve the performance of the Presence service and exclude domains that are not part of the internal or federated domains. You can also limit presence subscriptions to specific internal and federated domains. By default, the whitelisting feature is disabled and all internal and external email domain subscriptions are attempted. When this feature is configured, you can manage the allowed list from all BEMS servers that host the Presence service.

When your organization enables whitelisting, contacts in an email domain that is not listed are restricted and no presence subscriptions are attempted to that domain. Consider the following scenarios when you enable domain white listing:

- If you enable domain whitelisting, but do not specify one or more email domains, all email domains are restricted from requesting Presence subscriptions.
- If you enable domain whitelisting and specify one or more email domains, only contacts in the specified email domains are included in the subscription request to the instant messaging server. If a contact is not a user in the whitelisted email domains, the user presence is not displayed.
- If you do not enable domain whitelisting, then contacts in any email domain are included in the subscription request to the instance messaging server.

### **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**.



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

Environments configured to use Microsoft Lync Server 2013, or Skype for Business on-premises that are using trusted application mode use the Unified Communications Managed API (UCMA) software for the Presence service to communicate with the instant messaging server. Environments configured to use Skype for Business on-premises that are using non-trusted application mode use Unified Communications Web API (UCWA) software for the Presence service to communicate with the instant messaging server.

## Before you begin:

- If your environment uses Skype for Business on-premises using non-trusted application mode, make sure that the Skype for Business on-premises root CA certificate is imported. For instructions, see "[Import the CA certificate into the Java certificate store](#)" in the [BEMS-Core configuration content](#).
  - If your environment uses Skype for Business on-premises using non-trusted application mode the Good Technology Presence service is not used.
  - 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 balancer. For more information about load balancing requirements, visit <https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/load-balancing>.
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 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. Complete one of the following tasks:

Instant messaging server in environment	Task
Microsoft Lync Server 2013	<ol style="list-style-type: none"> <li>a. In the <b>Application ID</b> drop-down list, select <b>&lt;appid_connect.mycompany.com&gt;</b>.  If the drop-down list is empty, either the BEMS <i>&lt;instant messaging server type&gt;</i> topology is not set up correctly or the service account does not have permissions to query these settings.</li> <li>b. In the <b>Application Endpoint</b> drop-down list, select the corresponding application endpoint.</li> </ol>

Instant messaging server in environment	Task
<p>Skype for Business on-premises using trusted application mode</p> <p><b>Note:</b> Using this configuration, the Presence service is trusted by Skype for Business and can impersonate a user. End user authentication is not required on the device to view the presence status.</p>	<ol style="list-style-type: none"> <li>a. Select the <b>Skype for Business On-Premises</b> check box.</li> <li>b. Select <b>Trusted Application Mode</b>.</li> <li>c. Beside the <b>Application ID</b> drop-down list, click <b>Browse</b>. This step can take up to a minute to complete.</li> <li>d. In the <b>Application ID</b> drop-down list, select the app ID for Presence to use the correct configuration information registered with the Skype topology. For example, <b>&lt;appid_connect.mycompany.com&gt;</b>.  If the drop-down list is empty, either the BEMS <i>&lt;instant messaging server type&gt;</i> topology is not set up correctly or the service account does not have permissions to query these settings.</li> <li>e. In the <b>Application Endpoint</b> drop-down list, select the appropriate endpoint for the Presence service to use when subscribing to a user's presence status in the Skype topology.</li> </ol>
<p>Skype for Business on-premises using non-trusted application mode</p> <p><b>Note:</b> Using this configuration, the</p> <ul style="list-style-type: none"> <li>• Presence service is not trusted by Skype for Business and cannot impersonate a user. End user authentication on the device is required.</li> <li>• Presence service passes through the web proxy if it is defined but doesn't use the bypass list even if the Skype for Business servers are added to the bypass proxy list. In some cases, authentication to Skype for Business might fail. For more information on configuring the web proxy, see <a href="#">"Configure a web proxy server" in the BEMS-Core configuration content</a>.</li> </ul>	<ol style="list-style-type: none"> <li>a. Select the <b>Skype for Business On-Premises</b> check box.</li> <li>b. Select <b>Non-trusted Application Mode</b>.</li> <li>c. Complete one or both of the following actions: <ul style="list-style-type: none"> <li>• Select the <b>Auto discover servers</b> checkbox to have BEMS discover the Skype for Business servers in the environment.</li> <li>• 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, <code>http(s)://&lt;FQDN_of_the_Skype_front_end_pool&gt;/Autodiscover/AutodiscoverService.svc/root/oauth/user</code>.</li> </ul> </li> </ol>

5. Verify the Azure information is valid and log in to the user account:
  - If you configure the environment to use Skype for Business on-premises:
    - a. Enter a user email address and password.
    - b. Click **Test**.
6. Click **Save**.
7. Complete one of the following actions:
  - If you configured the Presence service for Microsoft Lync Server 2013, or Skype for Business on-premises using trusted application mode, start the Good Technology Presence service. Make sure that you save the configuration in the Dashboard prior to starting the service.
  - If you configured the Presence service for Skype for Business on-premises using non-trusted application mode only, you do not need to start the Good Technology Presence service. Skype for Business on-premises using non-trusted application mode don't require the Presence service to view users' presence

status. If you try to start the service, the following error message is displayed. **Windows could not start the Good Technology Presence service on Local Computer. Error 5: Access denied.**

- If you configured the Presence service for Skype for Business on-premises using non-trusted application mode only, restart the Good Technology Common Services to enable the BEMS cache to use memory instead of Redis.

## Configure Jabber for the Presence service

Complete this task only if you have a Cisco CM IM and Presence server in your environment to provide user presence status to BlackBerry Work users in a Cisco topology.

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 end user. This is the user you created in "[Create a Dummy User](#)" in the [Installation content](#). If you install multiple BEMS instances, you must use the same user account for each instance.
8. 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`.
9. 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`.
10. 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.
11. In the **Application Password** field, enter the password of the application user.
12. Click **Test** to verify the fields are completed. The test does not verify that the information in the fields are accurate.
13. 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. Cisco Jabber, and Skype for Business on-premises using non-trusted application mode do not support multiple application endpoints.

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

**Before you begin:** You must have a 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](#)" in the [Installation content](#).
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 assigning the next 2000 subscriptions to the next endpoint.

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

## Using friendly names for certificates in Presence

**Note:** Friendly names for certificates only apply to environments that use a Microsoft Lync Server or Skype for Business on-premises using trusted application mode.

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 not have one, create and enroll a certificate.
2. Change the certificate friendly name 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 ["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 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. Locate the existing entry for `<add key="RESTRICT_CERT_BY_FRIENDLY_NAME" value=" " />` and enter the certificate friendly name in the value property. For example: `<add key="RESTRICT_CERT_BY_FRIENDLY_NAME" value="<cert_friendly_name>" />`. The key value is case sensitive.
3. Save your changes.
4. Start the Good Technology Presence service.

# 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	<p>Make sure your multi-cluster environment has the following configured:</p> <ul style="list-style-type: none"><li>• DNS SRV records for Cisco Jabber Service Discovery. For instructions, see "Service Discovery" in the <a href="#">Cisco Jabber Planning Guide</a> for your version of Cisco Jabber.</li><li>• Cisco Intercluster Lookup Service (ILS) between the CUCM clusters in your environment. For instructions, see "Intercluster Lookup Service" in the <a href="#">Cisco Unified Communications Manager Features and Services Guide</a> for your version of Cisco Unified Communications Manager.</li><li>• Intercluster Peering between the CIMP clusters in your environment. For instructions, see "Intercluster Peer Configuration" in the <a href="#">Cisco Unified Communications Manager Configuration and Administration Guide</a> for your version of the Cisco Unified Communications Manager.</li></ul>
2	<p>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.</p> <p>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.</p> <p>For BlackBerry Presence</p> <ul style="list-style-type: none"><li>• Application user and password. For instructions, see "<a href="#">Create an Application User</a>" in the <a href="#">Installation content</a>.</li><li>• UDS Username (Dummy user). For instructions, see "<a href="#">Create a Dummy User</a>" in the <a href="#">Installation content</a>.</li></ul>

Step	Action
3	<p>Download the required certificates from each cluster.</p> <ul style="list-style-type: none"> <li>• Tomcat.der</li> <li>• Cup.der</li> <li>• Cup-xmpp.pem and Cup-xmpp-ECDSA.pem</li> <li>• Cup-ECDSA.der and Tomcat-ECDSA.der</li> <li>• CUCM SSL certificate. Visit the <a href="#">Cisco Devnet</a> to see <a href="#">Download the Cisco Unified CM SSL Certificate</a></li> </ul>
4	<p>Import the certificates into the Java keystore. For instructions, see "Import the CA certificate into the Java certificate store" in the <a href="#">BEMS-Core configuration content</a>.</p>
5	<p>Configure the BlackBerry Connect service.</p>
6	<p>Configure the BlackBerry Presence service.</p>

### 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](#).



# 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 BlackBerry Proxy or Good Proxy server.](#)
2. Perform one of the following actions:

Environment	Tasks
If you have a BlackBerry UEM environment	<ol style="list-style-type: none"><li>a. <a href="#">Add the new computer hosting the Presence service instance to BlackBerry UEM.</a></li><li>b. <a href="#">If you installed the Presence service on a separate computer, configure each computer with the Presence service instance for the BlackBerry Presence Service (com.blackberry.gd-service.entitlement.presence) app.</a></li></ol>
If you have a Good Control environment	<ol style="list-style-type: none"><li>a. <a href="#">Whitelist each new Presence server host and port in Good Control.</a></li><li>b. <a href="#">If you installed the Presence service on a separate computer, configure each computer with the Presence service instance for the BlackBerry Presence Service (com.blackberry.gd-service.entitlement.presence) app.</a></li></ol>

# 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 Presence service

The Presence log files contain presence information that is logged to the same log files as the Push Notifications (Mail) logs and saved to the bemslogs folder. The log files are required when you troubleshoot Presence issues. For information about the Presence log files, see the BEMS [Monitoring and reporting content](#).

# Next steps

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

- [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 its Microsoft Exchange Web Services protocol to monitor the user's enterprise mailbox for changes.
- BlackBerry Work app: The BlackBerry Work app integrates all your business collaboration and keeps the organization's data secure. The app allows users to stay on top of business email and calendar, view online presence, manage contacts and easily work on documents. For more information, [see the BlackBerry Work Administration content for your environment](#).
- [BlackBerry Docs service](#): This service lets your BlackBerry Dynamics app users access, synchronize, and share documents using their work file server, SharePoint, Box, and content management systems supporting CMIS, without the need for VPN software, firewall reconfiguration, or duplicate data stores.
- [BlackBerry Connect service](#): This service provides secure instant messaging, company directory lookup, and user presence information to iOS and Android devices.
- 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, [BlackBerry Connect administration content](#).

# 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 Presence service to use a Lync Director

1. On the BEMS host, stop the Good Technology Presence service.
2. Update the BlackBerry Presence configuration file. By default, the LyncPresenceProviderService.exe.config file is located in `<drive>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Presence`.
  - a) On the BEMS host, navigate to the LyncPresenceProviderService.exe.config file.
  - b) In a text editor, open the LyncPresenceProviderService.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 Presence service.

# 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](http://support.blackberry.com/community) to read article 46152.

## Enable the Presence service to use a global catalog with Microsoft Lync Server or Skype for Business

The instructions in this topic use the environment example.com to configure the Presence service to use a global catalog and applies to an environment that is configured for on-premises Microsoft Lync Server 2013 or Skype for Business on-premises servers using trusted application mode. If you installed the Connect service on multiple servers, complete this task on each computer that is running the Presence service.

1. In a text editor, open the LyncPresenceProviderService.exe.config file. By default, the file is located in `<drive>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Presence` 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, if your environment (example.com) requires access to a global catalog, 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 the distinguished domain name using `DC=EXAMPLE,DC=COM` or the fully qualified domain name using `EXAMPLE.COM`. Make sure that you use the distinguished name of the domain. For more information, see [Understanding the BEMS-Connect configuration file](#).

The following example shows the LyncPresenceProviderService.exe.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
Presence resides; -->
<add key="AD_USERS_SOURCE_DOMAIN" value="DC=EXAMPLE,DC=COM" />
.
.

```

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

## Revert the Presence service settings to use the local Active Directory

If you configured the Presence service to use a global catalog, you can modify the `LyncPresenceProviderService.exe.config` file to have the Presence service use the local Active Directory domain that the BEMS is located in. In the following example, the Presence 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 Presence service.

1. In a text editor, open the `LyncPresenceProviderService.exe.config` file. By default, the file is located in `<drive>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Presence` 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 `LyncPresenceProviderService.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 Presence 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



# Legal notice

©2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

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

Published in Canada