



BlackBerry Enterprise Mobility Server

Configuring the BlackBerry Docs service

3.7

Contents

- BlackBerry Docs service..... 5**
- Steps to configure the Docs service..... 6**
 - Configure the database for the BlackBerry Docs service..... 6
 - Configure a web proxy server for the Docs service..... 7
 - Configure the Docs security settings..... 7
 - Configuring Microsoft Office Web Apps and Office Online Server for Docs service support..... 8
 - Configuring Kerberos constrained delegation for Docs..... 9
 - Configuring resource based Kerberos constrained delegation for the Docs service..... 13
 - Obtain an Entra app ID for the BEMS-Docs component service..... 16
 - Storage services..... 18
 - Authentication providers..... 19
 - Add a storage service..... 19
 - Microsoft SharePoint Online authentication setup..... 20
 - Managing Repositories..... 21
 - Repositories..... 22
 - Enable modern authentication for Microsoft SharePoint Online..... 22
 - Configuring repositories..... 23
 - Admin-defined shares..... 23
 - Configuring Docs for Rights Management Services..... 32
 - Using the Docs Self-Service web console..... 35
 - Configuring support for Microsoft SharePoint Online and Microsoft OneDrive for Business..... 35
 - Auditing the Docs service..... 37
 - In a BlackBerry UEM environment, add an app server hosting the BEMS-Docs service to a BlackBerry Dynamics connectivity profile..... 37
 - Configuring Good Control for Docs service..... 38
 - Entitle users, configure the Docs service entitlement..... 38
 - Configure the Docs service entitlement, add BEMS to Good Control..... 38
 - Publish the Docs app to users..... 38
 - Enable server affinity for Docs in BlackBerry Work..... 39
- Configuring the Docs instance for high availability.....40**
- Disaster recovery..... 41**
- Next steps.....42**
- Appendix: File types supported by the BlackBerry Docs service..... 43**
 - Supported files and storage types..... 43

| | |
|---|-----------|
| Windows Folder Redirection (Native)..... | 45 |
| Enable folder redirection and configure access..... | 45 |
| Local Folder Synchronization – Offline Folders (Native)..... | 47 |
| Supported Microsoft Office Web Apps and Office Online Server file types..... | 49 |
| Legal notice..... | 51 |

BlackBerry Docs service

The Docs service supports the ability to add or delete access to storage providers and their repositories. The Docs 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. You can configure and maintain folder and file repositories and user access policies for mobile app users of the BlackBerry Docs service. The BEMS Dashboard supports and manages the following repositories:

- Microsoft SharePoint
- Microsoft SharePoint Online
- File Share
- Box
- CMIS-supported content management systems
- OneDrive for Business

Steps to configure the Docs service

BlackBerry Dynamics servers must be operating before the Docs service can be configured for BlackBerry Dynamics.

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

| Step | Action |
|------|---------------------------------------|
| 1 | Configure the Database. |
| 2 | Configure the Web Proxy. |
| 3 | Configure the Docs security settings. |
| 4 | Configure storages. |
| 5 | Configure repositories. |
| 6 | Auditing the Docs service. |

Configure the database for the BlackBerry Docs service

In configuring your Microsoft SQL Server database for BEMS-Docs, you have a choice of using either Windows Authentication or SQL Authentication for granting access to the database by BEMS. Perform the steps below for either Windows Authentication or SQL Authentication.

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

Configure a web proxy server for the Docs service

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

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

Configure the Docs security settings

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

Before you begin: Verify that one or more of the following are configured in your environment:

- Kerberos constrained delegation for the BlackBerry Docs service is configured in your environment. For instructions, see [Configuring Kerberos constrained delegation for the Docs service](#).
 - Resource-based Kerberos constrained delegation for the BlackBerry Docs service is configured in your environment. For instructions, see [Configuring resource based Kerberos constrained delegation for the Docs service](#).
 - Your environment is configured to use Entra-IP, have the following information. For instructions, see [Obtain an Entra app ID for the BEMS-Docs component service](#).
 - Entra Tenant Name
 - BEMS Service Entra Application ID
 - BEMS Service Entra Application Key
 - Optionally, you can configure BEMS to allow users to authenticate to Microsoft SharePoint Online with an email address that is different from the email address that was used to install and activate BlackBerry Work. For instructions, see [Enable the use of an alternate email address to authenticate to BEMS-Docs](#).
1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
 2. Click **Settings**.
 3. Select the **Enable Kerberos Constrained Delegation** checkbox to allow Docs to use Kerberos constrained delegation.
 4. Separated by a comma, enter each of the Microsoft SharePoint Online domains you plan to make available. For more information, see [Configuring support for Microsoft SharePoint Online and Microsoft OneDrive for Business](#).
 5. Enter the URL for your approved Office Web App or Office Online Server.

6. Provide your Microsoft Active Directory user domains (separated by commas), then enter the corresponding **LDAP Port**. LDAP (Lightweight Directory Access Protocol) is used to look up users and their membership in user groups.
7. Optionally, specify the timeout before the BEMS connection attempt to the LDAP server times out. In the **LDAP Connection Timeout** field, increase or decrease the value, in seconds, as required. The default value is 30 seconds. You can specify between zero and 300 seconds.
8. Optionally, specify the timeout before the BEMS search for users and their membership in user groups times out. In the **LDAP Search Timeout** field, increase or decrease the value, in seconds, as required. The default value is 30 seconds. You can specify between zero and 300 seconds.
9. Select the **Use SSL for LDAP** checkbox for secure communication with your Microsoft Active Directory servers.
10. Add the **Workspaces Public Key**. Adding the public key allows BEMS and the BlackBerry Workspaces server to communicate with each other. For more information about locating the public key, contact BlackBerry Technical Support Services.
11. Select the **Enable Azure Information Protections** check box to allow Docs to authenticate to Entra-IP. Complete the **Azure registration** fields to authenticate Docs to Entra-IP to allow the Docs to decrypt protected documents and confirm the rights any given user has on a document. For instructions about obtaining the Azure registration fields, see [Obtain an Entra app ID for the BEMS-Docs component service](#).
12. Click **Save**.
13. Restart the Good Technology Common Services service for the changes to take effect.

Configuring Microsoft Office Web Apps and Office Online Server for Docs service support

Microsoft Office Web Apps and Office Online Server is an Office server product from Microsoft that delivers browser-based versions of Microsoft Word, Microsoft PowerPoint, Microsoft Excel, and Microsoft OneNote. A single Microsoft Office Web Apps or Office Online Server can support Docs service users who access Office files through Microsoft SharePoint and File Shares. The new stand-alone deployment model means that you can manage updates to your Microsoft Office Web Apps, web apps, or Office Online Server independently of other Office Server products that are deployed in your organization. For information on supported file types, see [Supported Microsoft Office Web Apps and Office Online Server file types](#).

Configure the Docs service for Microsoft Office Web Apps and Office Online Server access

Before you begin:

- A Microsoft Office Web Apps or Office Online Server is installed and configured in your environment.
 - Verify that you have the Microsoft Office Web Apps or Office Online Server URL, and custom port if required. BEMS automatically adds `/hosting/discovery` to the web address when BEMS performs a service discovery and adding it to the web address is not required.
 - Add a registry key to enable strong cryptography on the Office Online Server. If this key is not added to the registry, users can't view or edit Microsoft Office Web Apps or Office Online Server files in BlackBerry Access and the Office Online Server log files log the error message **Could not create SSL/TLS secure channel**. For instructions, see the Known issues section of the [BEMS on-premises Release Notes content](#).
1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
 2. Click **Settings**.
 3. Under **Office Web App Server**, in the **Office Web App Server URL** field, type the web address of the Microsoft Office Web Apps or Office Online Server. For example, `https://officewebapps.example.com` or `https://officewebapps.example.com:1234` if a custom port is used.
 4. Click **Save**.
 5. On the **Office Web App Server** server, in the **Windows** folder, copy **Microsoft.CobaltCore.dll** file. By default, the file is located in `<drive>:\Windows\Microsoft .Net\assembly\GAC_MSIL\Microsoft.CobaltCore\`.

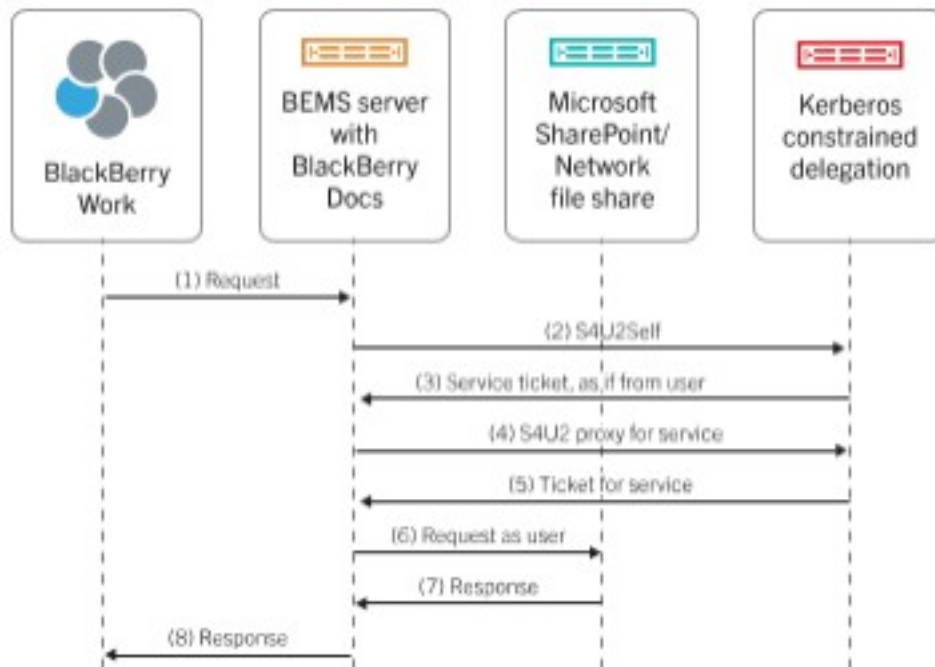
6. On the BEMS, browser to and paste the file into the lib folder at <drive>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<version>\lib.
7. Restart the Good Technology Common Services service.
8. On BEMS, export the SSL certificate to a file.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

Configuring Kerberos constrained delegation for Docs

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

Before configuring the Docs service to use KCD, it is important to understand that configuring KCD for Docs service is independent of configuring BlackBerry Dynamics KCD. This means, for example, that if your mobile app (for example, BlackBerry Work) requires use of the Docs service exclusively, you only need to configure KCD for the Docs service. It is recommended to configure the Docs service to use resource based Kerberos constrained delegation to access resources and remove the requirement for users to provide their network credentials to access resources within the domain, and between domains and forests. For more information on resource based Kerberos constrained delegation, see [Configuring resource based Kerberos constrained delegation for the Docs service](#).

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



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

Configuring Kerberos constrained delegation for the Docs service

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

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

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

Find the SharePoint application pool identity and port

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

1. Open Windows Internet Information Services (IIS) Manager.
Make sure that you record any additional port numbers that are assigned if a web application was extended to create alternate access mappings.
2. Find the Application Pool identity in the **Application Pools** list view or in **SharePoint Central Administration > Security > Configure service accounts**.
In most instances, for Kerberos constrained delegation (KCD) to work properly, the application pool identity user must be the same for all application pools whose applications will be accessed by the Docs service. This means you cannot have different application pools running under different users.

3. In **SharePoint Central Administration**, on the **Web Applications** tab, find the port for each of the web applications listed. Look in the **Alternate Access Mappings** view as necessary.
4. In the **Sharepoint Central Administration**, open the **Application Management**, choose the web application and click **Authentication Providers** in the ribbon bar. Make sure that the authentication type for each web application is set to **Windows** and that **Negotiate (Kerberos)** is enabled under **IIS Authentication Settings**.
In certain scenarios, switching to Negotiate (Kerberos) might require enabling Kernel-mode authentication in IIS for the corresponding IIS site. For more information, visit the [MSDN Library](#) to see [Service Principal Name \(SPN\) checklist for Kerberos authentication with IIS 7.0/7.5](#).

Create Service Principal Names

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

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

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

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

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

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

Add Kerberos constrained delegation in Microsoft Active Directory for Microsoft SharePoint

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

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

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

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

Add Kerberos constrained delegation for file shares

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

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

Turn on Kerberos constrained delegation

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

- Only Windows authentication in Microsoft SharePoint is supported. Forms-based and claims-based authentication are not supported.
 - IP addresses are not allowed in the Microsoft SharePoint URLs and File Share paths that you configure in BEMS.
1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
 2. Click **Settings**.
 3. In the **Kerberos Constrained Delegation** section, select the **Enable Kerberos Constrained Delegation** checkbox.
 4. Click **Save**.
 5. Restart the Good Technology Common Services service.
 6. On the computer hosting the BEMS-Docs service, grant the **Act as part of the operating system** privilege to the BEMS server account (for example, GoodAdmin).
 - a) Run the **Local Security Policy** administrative tool.
 - b) In the left pane, expand **Local Policies**.
 - c) Click **User Rights Agreement**.
 - d) Configure the service account for the **Act as part of the operating system** permission.
 7. Click **OK**.

Configuring resource based Kerberos constrained delegation for the Docs service

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

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

When you configure resource based Kerberos constrained delegation, you perform the following actions:

1. [Configure resource based Kerberos constrained delegation](#)
2. Optionally, [Verify the delegation is configured correctly](#)
3. [Turn on resource based Kerberos constrained delegation](#)

Configure resource based Kerberos constrained delegation

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

Before you begin:

- Each domain in your environment has one or more Domain Controllers on a computer that is running Windows 2012 or later.
 - The BEMS service account is a member of the local Administrators group and has the Act as part of the Operating System privilege.
 - If you are configuring resource based KCD for Microsoft SharePoint, make sure that Microsoft SharePoint server uses Integrated Windows Authentication – Negotiate (Kerberos) for the authentication provider.
 - You identified the file share servers and Microsoft SharePoint servers that the Docs service requires access to.
1. On the Domain Controller or another computer in your environment, open Windows PowerShell (run as administrator) and set up delegation.
 - a) Import the ServerManager module. Type `Import-Module ServerManager`. Press **Enter**.
 - b) Install the Microsoft Active Directory module for Windows PowerShell and the Microsoft Active Directory Services. Type `Add-WindowsFeature RSAT-AD-PowerShell`. Press **Enter**.
 - c) Import the Microsoft Active Directory module. Type `import-module activedirectory`. Press **Enter**.
 2. Find the application pool identity for the Microsoft SharePoint servers in your environment. The application pool identity is located in the Microsoft Internet Information Services (IIS) Manager, on the **Application Pools** screen.
 3. If the Microsoft SharePoint web application is running on a non-default port (the default ports are 80 and 443) or is not running under the network service, create SPNs. Complete one or more of the following tasks:

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

| Task | Steps |
|---|--|
| Create SPNs for a Microsoft SharePoint web application running on a non-default port and as a specific user | <ol style="list-style-type: none"> Type <code>setspn -S HTTP/<Sharepoint server name>:<Sharepoint app port> <Sharepoint domain>\<Sharepoint app user></code>. Press Enter. <ul style="list-style-type: none"> Where <i><Sharepoint server name></i> is the name of the computer hosting the Microsoft SharePoint web application. Where <i><Sharepoint app port></i> is the port number of the Microsoft SharePoint web application server. Where <i><Sharepoint domain></i> is the domain where the Microsoft SharePoint web application server is located. For example, <i>www.example.com</i>. Where <i><Sharepoint app user></i> is the user or service account that is listed in the Identity column in step 2. If the service is set to run as a user, the identity column displays <i><web application server name>/<username></i>. If the service is set to run as a network, you will see Network service. Type <code>setspn -S HTTP/<Sharepoint server FQDN>:<Sharepoint app port> <Sharepoint domain>\<Sharepoint app user></code>. Press Enter. <ul style="list-style-type: none"> Where <i>Sharepoint server FQDN</i> is the FQDN of the computer hosting the Microsoft SharePoint web application server. |
| Create SPNs for a Microsoft SharePoint web application running on a default port (80 or 443) and as a specific user | <ol style="list-style-type: none"> Type <code>setspn -S HTTP/<Sharepoint server name> <Sharepoint domain>\<Sharepoint app user></code>. Press Enter. Type <code>setspn -S HTTP/<Sharepoint server FQDN> <Sharepoint domain>\<Sharepoint app user></code>. Press Enter. |
| Create SPNs for a Microsoft SharePoint web application running on a non-default port and under a network service | <ol style="list-style-type: none"> Type <code>setspn -S HTTP/<Sharepoint server name>:<Sharepoint app port> <Sharepoint domain>\<Sharepoint server name></code>. Press Enter. Type <code>setspn -S HTTP/<Sharepoint server FQDN>:<Sharepoint app port> <Sharepoint domain>\<Sharepoint server name></code>. Press Enter. |

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

| Task | Steps |
|---|--|
| Add the delegation for one computer hosting BEMS. | <ol style="list-style-type: none"> Type <code>\$gems1 = Get-ADComputer -Identity <GEMS-SERVER-NAME></code>. Press Enter. Type <code>Set-ADComputer <File server name> -PrincipalsAllowedToDelegateToAccount \$gems1</code>. Press Enter. |

| Task | Steps |
|---|--|
| Add the delegation for multiple computers hosting BEMS. | <p>a. Type <code>\$gems1 = Get-ADComputer -Identity <GEMS-SERVER1-NAME></code>. Press Enter.</p> <p>b. Type <code>\$gems2 = Get-ADComputer -Identity <GEMS-SERVER2-NAME></code>. Press Enter.</p> <p>For each additional BEMS, increment the <code>\$gems#</code> by one.</p> <p>c. Type <code>Set-ADComputer <File server name> -PrincipalsAllowedToDelegateToAccount \$gems1,\$gems2</code>. Press Enter.</p> <p>For each additional BEMS, add a comma and <code>\$gems#</code> incrementing the <code>#</code> by one.</p> |

5. If you configure the delegation for file share servers in a DFS configuration, add delegations to the name server and the file server. For domain based DFS, this requires adding delegations for all of the Domain Controllers in the domain. Type `Set-ADComputer <DC-SERVER-NAME> -PrincipalsAllowedToDelegateToAccount $gems1`. Press **Enter**.
 - Where `<DC-SERVER-NAME>` is the name of the computer hosting the domain controller.
 - Where `$gems1` is created in step 4 above.
6. Add delegation to the Microsoft SharePoint servers in your environment. Complete one of the following actions:
 - If the application pool identity for Microsoft SharePoint application is Network Service, type `Get-ADComputer <Sharepoint server name> -Properties PrincipalsAllowedToDelegateToAccount`.
 - If the application pool identity for Microsoft SharePoint application is a specific domain user, type `Get-ADUser <Sharepoint app user> -Properties PrincipalsAllowedToDelegateToAccount`.

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

Verify the delegation is configured correctly

You can verify that the delegation property was set correctly.

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

Turn on resource based Kerberos constrained delegation

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

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

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Settings**.
3. In the **Kerberos Constrained Delegation** section, select the **Enable Kerberos Constrained Delegation** checkbox.
4. Click **Save**.
5. Restart the Good Technology Common Services service.
6. On the computer hosting the BEMS-Docs service, grant the **Act as part of the operating system** privilege to the BEMS server account (for example, GoodAdmin).
 - a) Run the **Local Security Policy** administrative tool.
 - b) In the left pane, expand **Local Policies**.
 - c) Click **User Rights Agreement**.
 - d) Configure the service account for the **Act as part of the operating system** permission.
7. Click **OK**.

Remove resource based Kerberos constrained delegation

1. Open the Windows PowerShell (run as administrator).
2. Complete one of the following tasks:
 - To remove the delegation from a server, type `Set-ADComputer <server_name> -PrincipalsAllowedToDelegateToAccount $null`.
If you have multiple file share or Microsoft SharePoint servers in your environment, complete this step for each server.
 - To remove the delegation from a user, type `Set-ADUser <user_name> -PrincipalsAllowedToDelegateToAccount $null`.
If you use different usernames for the Microsoft SharePoint and file share servers, complete this step for each username.
3. Press **Enter**.

Obtain an Entra app ID for the BEMS-Docs component service

When your environment is configured for Microsoft SharePoint Online, Microsoft OneDrive for Business, or Microsoft Entra ID-IP you must register the BEMS component services in Entra. You can register one or more of the services in Entra. In this task, the Docs services and Microsoft Entra ID-IP are registered in Entra.

Before you begin: To grant permissions, you must use an account with tenant administrator permissions.

1. Sign in to portal.azure.com.
2. In the left column, click **Microsoft Entra ID**.
3. Click **App registrations**.
4. Click **New registration**.
5. In the **Name** field, enter a name for the app. For example, AzureAppIDforBEMS.
6. Select a supported account type.
7. In the **Redirect URI** drop-down list, select **Web** and enter `https://localhost:8443`.
8. Click **Register**.
9. Record the **Application (client) ID**. This is used as the **BEMS Service Azure Application ID** value for the Docs > Settings service in the BEMS dashboard.
10. In the **Manage** section, click **API permissions**.
11. Click **Add a permission**.

12. Complete one or more of the following tasks:

| Service | Permissions |
|--|---|
| If you configure BEMS-Docs to use Microsoft SharePoint Online or Microsoft OneDrive for Business | <p>a. Search for and click SharePoint.</p> <p>b. Set the following permissions:</p> <ul style="list-style-type: none"> In application permissions, clear all of the permissions. <ol style="list-style-type: none"> Click Application permissions. Click expand all. Make sure that all options are cleared. In Delegated permissions, click AllSites and select the AllSites.Manage checkbox to grant Read and write items and lists in all site collections. Make sure that all other options are cleared. <p>c. Click Add permissions.</p> |
| If you use Microsoft Entra ID-IP | <p>a. Click Microsoft Graph. If Microsoft Graph is not listed, add Microsoft Graph.</p> <p>b. Set the following permissions:</p> <ul style="list-style-type: none"> In application permissions, select the Read directory data checkbox (Directory > Directory.Read.All). In delegated permissions, select the Read directory data checkbox (Directory > Directory.Read.All). <p>c. Click Update permissions.</p> <p>d. Add a permission.</p> <p>e. In the Select an API section, click Azure Rights Management Services. Set the following permissions:</p> <ul style="list-style-type: none"> In application permissions, select all of the permissions. <ol style="list-style-type: none"> Click Application permissions. Make sure that all Content options are selected. In delegated permissions, select the user_impersonation checkbox. <p>f. Click Add permissions.</p> <p>g. Click Add a permission.</p> <p>h. In the Select an API section, click APIs my organization uses.</p> <p>i. Search for and click Microsoft Information Protection Sync Service. Set the following permission:</p> <ul style="list-style-type: none"> In delegated permissions, select the Read all unified policies a user has access to checkbox (UnifiedPolicy > UnifiedPolicy.User.Read). <p>j. Click Add permissions.</p> |

13. Wait a few minutes, then click **Grant admin consent**. Click **Yes**.

Important: This step requires tenant administrator privileges.

14. To allow autodiscovery to function as expected, set the authentication permissions. Complete the following steps:

- In the **Manage** section, click **Authentication**.
- Under the **Allow public client flows** section, select **Yes** to **Enable the following mobile and desktop flows**.
- Click **Save**.

15. Define the scope and trust for this API. In the **Manage** section, click **Expose an API**. Complete the following tasks.

| Task | Steps |
|--------------------------|--|
| Add a scope | <p>The scope restricts access to data and functionality protected by the API.</p> <ol style="list-style-type: none"> Click Add a scope. Click Save and continue. Complete the following fields and settings: <ul style="list-style-type: none"> Scope name: Provide a unique name for the scope. Who can consent: Click Admins and user. Admin consent display name: Enter a descriptive name. Admin consent description: Enter a description for the scope. State: Click Enabled. By default, the state is enabled. Click Add Scope. |
| Add a client application | <p>Authorizing a client application indicates that the API trusts the application and users shouldn't be prompted for consent.</p> <ol style="list-style-type: none"> Click Add a client application. In the Client ID field, enter the client ID that you recorded in step 9 above. Select the Authorized scopes checkbox to specify the token type that is returned by the service. Click Add application. |

16. In the **Manage** section, click **Certificates & secrets** and add a client secret. Complete the following steps:

- Click **New client secret**.
- In the **Description** field, enter a key description up to a maximum of 16 characters including spaces.
- Set an expiration date (for example, In 1 year, In 2 years, Never expires).
- Click **Add**.
- Copy the key **Value**.

Important: The Value is available only when you create it. You cannot access it after you leave the page. This is used as the **BEMS Service Application Key** in the BEMS-Docs service in the BEMS Dashboard.

Storage services

BEMS is installed with support for several storage service providers, including File Share, Microsoft SharePoint, Microsoft SharePoint Online, and Box.

You can also add a new storage service if you need to use a service that is not displayed, or your environment requires customized storage service settings. The following table lists the available storage providers and when they should be used.

| Storage provider | Description |
|------------------|--|
| Box | By default, BEMS allows corporate box.com cloud storage users to view the Box repositories using BlackBerry Work Docs. If you delete the predefined Box storage, the hidden authentication parameters are also removed. For more information about determining if you are using a non-default Box storage and how to re-add the default Box storage, visit support.blackberry.com/community to read article 48469. |

| Storage provider | Description |
|------------------|--|
| CMIS | You can add storage services that utilize the Content Management Interoperability Services (CMIS) protocol, an open standard that allows different content management systems to inter-operate over the Internet. Note: Only Microsoft Active Directory users are supported for CMIS. This requires that the content management system is connected to a Microsoft Active Directory for user authentication for Docs to support it. |
| FileShare | This storage provider allows BEMS to communicate with the FileShare server. If your environment is configured for a specific version of SMB or CIFS protocol to access a File Share, BEMS must be installed on a compatible Windows operating system. Refer to your Microsoft documentation for more information on compatibility. |
| SharePoint | If your environment uses a supported version of Microsoft SharePoint or Microsoft SharePoint Online, this storage provider allows BEMS to determine the appropriate storage provider to use to communicate with your version of SharePoint. |

For more information about supported versions of Microsoft SharePoint, see the [BEMS Compatibility Matrix](#).

Authentication providers

The following table lists the available authentication providers and the storage provider that each can be used for. For instructions on adding storage services, see [Add a storage service](#) and [Enable modern authentication for Microsoft SharePoint Online](#)

| Authentication Provider | Storage provider |
|---|-----------------------|
| Windows - Explicit Credentials | FileShare, SharePoint |
| Windows - Kerberos Constrained Delegation | FileShare, SharePoint |
| OAuth2 | Box |
| Explicit Credentials | Workspaces |
| Modern | SharePoint Online |

Add a storage service

BEMS is installed with support for a number of storage service providers. Complete this task when you need to use a service that is not displayed, or your environment requires customized storage service settings.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Storages**. A list of storage providers is displayed.
3. Click **New Storage**.
4. In the **Storage name** field, type a name for the storage.
5. In the **Storage provider** drop-down list, select a service provider. For more information about storage services and when each storage provider should be used, see [Storage services](#).
6. In the **Authentication Provider** drop-down list, select an authentication provider. For information about authentication providers and the storage provider that each can be used for, see [Authentication providers](#).

7. To make the storage available on user devices, select the **Enable Storage** checkbox.

It may take up to an hour or a restart of the apps for storage changes to take effect on user devices. It may take up to five minutes for the changes to take effect on the server. Enabling and disabling storage providers on this page affects what storage resources are visible at any given time for users, but has no such impact on the server. If this option is not selected, users can't access the fileshare and receive the following error message on the device: **Data sources could not be retrieved. Unable to connect to the server.**

After you finish: Add repositories in the storage provider. For instructions, see [Managing Repositories](#)

Microsoft SharePoint Online authentication setup

The following instructions do not apply when you configure Microsoft SharePoint Online using Modern Authentication. For Kerberos constrained delegation (KCD), which allows for single sign-on credential-less access to network resources from devices, only Active Directory Federation Service (ADFS) authentication to Microsoft SharePoint Online is supported.

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

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

ADFS version and location

Refer to the version of Microsoft Windows that is installed in your environment to verify which version of ADFS is required. The ADFS server is automatically identified by the Docs service based on the Microsoft SharePoint Online location and does not need to be specified.

ADFS HTTPS certificate

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

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

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

Enable the use of an alternate email address to authenticate to BEMS-Docs

You can configure BEMS to allow users to authenticate to Microsoft SharePoint Online with an email address that is different from the email address that was used to install and activate BlackBerry Work. Complete this task only if your environment is configured to use one of the following:

- If your environment is configured to use Windows authentication, you can configure BEMS to use the UserPrincipalName (UPN), email address or any other Active Directory attribute to authenticate to Microsoft SharePoint Online. By default, the UserPrincipalName attribute is used.
- If your environment uses modern authentication, you can configure BEMS to disable validating the email address when users authenticate to Microsoft SharePoint Online or the environment uses Entra-IP.

1. Sign in to the computer that is running the BEMS-Docs service.

2. In a browser, open the BEMS Karaf Console Configuration web site. Type `https://localhost:8443/system/console/configMgr` and login as administrator with the appropriate Microsoft Active Directory credentials.
3. On the menu, click **Main > Gogo**.
4. In the command, type one of the following commands:

| Task | Attribute | Description |
|---|---|---|
| Authenticate to Microsoft SharePoint Online using mail | <code>docs:config</code> <code>SAMLUsernameAttribute</code> <code>mail</code> | Allows users to use their email address to authenticate to Microsoft SharePoint Online instead of the user's userPrincipalName. To use the users' UPN again to authenticate, type <code>docs:config</code> <code>SAMLUsernameAttribute</code> <code>UserPrincipalName</code> |
| Disable user validation when authenticating to one of the following: <ul style="list-style-type: none"> • Microsoft SharePoint Online configured for modern authentication • Entra-IP | <code>docs:config</code> <code>modernauth.uservalidatio</code> <code>1</code> | Disables validation of the user's email address. |

5. Close the browser.

Managing Repositories

BEMS has the following repository storage providers:

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

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

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

Repositories

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

Before you configure your repositories, configure the [Docs Security Settings](#). After the the repositories are configured, entitle your users so that they can access the repositories you add and define from their devices. For more information about setting up and maintaining your enterprise shares in BEMS and the associated user access, see [Managing Repositories](#).

Enable modern authentication for Microsoft SharePoint Online

You can also enable modern authentication for Microsoft SharePoint Online when you have Microsoft SharePoint configured in your environment.

Before you begin: If you enable modern authentication, configured the Entra registration in the **Docs > Settings** screen. For more information, see [Configure the Docs security settings](#).

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Storages**.
3. Click the storage name **SharePoint Online**.
4. If this is a new installation, the following settings are selected by default:
 - **Authentication Provider** drop-down list: **Modern**. For information about authentication providers and the storage provider that each can be used for, see '[Authentication providers](#)' in the [BlackBerry Docs Service Configuration content](#).
 - **Use Azure registration from Settings** check box is selected. SharePoint uses the Entra registration settings that are specified in the **Docs > Settings** screen. For more information, see [Configure the Docs security settings](#).
5. If you upgraded from BEMS 2.10 or earlier and modern authentication was configured, no additional actions are required. Optionally, select the **Use Azure registration from Settings** check box for SharePoint to use the Entra registration settings that are specified in the **Docs > Settings** screen. For more information, see [Configure the Docs security settings](#).
6. To make the storage available on user devices, select the select the **Enable Storage** checkbox.

Note: It may take up to an hour or a restart of the apps for storage changes to take effect on users' devices. It may take up to five minutes for the changes to take effect on the server. Enabling and disabling storage providers on this page affects what storage resources are visible at any given time for users, but it has no such impact on the server. If this option is not selected, users can't access the fileshare and receive the following error message on the device: **Data sources could not be retrieved. Unable to connect to the server.**

After you finish:

Add repositories in the storage added. For instructions, see [Managing Repositories](#)

Configuring repositories

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

| Tabs | Description |
|---------------|--|
| Admin defined | Allows you to create and manage repositories, add and remove users and user groups, and assign users and user groups file access and use permissions. |
| User defined | Allows you to add and remove users and user groups, enable and disable user and user group the ability to create user-defined repositories, and grant and rescind permissions to perform a range of file-related actions on their user-defined repositories. |
| Users | Allows you to search for a user in a Microsoft Active Directory domain to view the repositories permitted by path or override, and who defined the share (for example, administrator or user). |

Admin-defined shares

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

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

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

Granting user access permissions


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

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

| Permission | Permissions Attributes | Default setting |
|---------------|---|-----------------|
| List (Browse) | View and browse repository content (for example, subfolders and files) in a displayed list, and sort lists by Name, Date, Size, or Kind | Enabled |
| Delete Files | Remove files from the repository | Enabled |

| Permission | Permissions Attributes | Default setting |
|-----------------------|--|------------------------------|
| Read (Download) | Download repository files to the user's device and open them to read | Enabled |
| Write (Upload) | Upload files (new/modified) from user's device to the repository for storage | Enabled |
| Cache (Offline Files) | Temporarily store a cache of repository files on the device for offline access. You can designate files and folders to synchronize to users' BlackBerry Work Docs app Offline folder. | Enabled |
| Open In | Open a file in a format-compatible app on the device | Enabled |
| Create Folder | Add new folders to the repository | Enabled |
| Copy/Paste | Copy repository file content and paste it into a different file or app | Enabled |
| Check In/Check Out | When a file is checked out, the user can edit, close, reopen, and work with the file offline. Other users cannot change the file or see changes until it is checked back in | Enabled (SharePoint only) |
| Generate Shared Link | Users can generate a link to a file and folder and send the link to recipients The Generate Shared Link requires an updated BlackBerry Work app. | Enabled (Box only) |

Change access permissions

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

Define a repository

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

Before you begin: For users to access their Microsoft SharePoint repositories on their devices, make sure that they have the "Read" permission level and the "Browse Directories" permission assigned.

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

2. Click **Repositories**.
3. Click the **Admin defined** tab.
4. Click **New Repository**.
5. In the **Display Name** field, type the name of the repository that will be displayed to users granted mobile access to the repository.
 The repository name must be unique and can contain spaces. The following special characters cannot be used due to third-party limitations:
 - Microsoft SharePoint 2016, and 2019: ~ " # % & * : < > ? / \ { | }
 - File Share: \ / : * ? " < > |
 - Box: \ / |
6. In the **Storage** drop-down list, select a storage provider.
 If you select **SharePoint** or **SharePoint Online**, and the share is running SharePoint 2016 or later, select the **Add sites followed by users on this site** check box to make this feature available to users of this share. This setting only applies for personal (my) SharePoint or OneDrive for Business sites.
 If your environment is configured for Microsoft OneDrive for Business, select the SharePoint Online storage provider.
7. In the **Path** field, specify the path to the share. Complete one of the following tasks based on the storage type that you selected in step 6.

| Storage type | Description |
|---------------------------------|---|
| Box | Enter a fully qualified URL with or without Microsoft Active Directory attributes. |
| FileShare | The Path can include Microsoft Active Directory attributes. For example, \\fileshare1\<sAMAccountName> or <homeDirectory>. |
| SharePoint SharePoint Online | <p>If your storage provider is Microsoft OneDrive for Business, complete this task.</p> <p>Enter a fully qualified URL with or without Microsoft Active Directory attributes.</p> <p>To add "my" or personal SharePoint sites, specify the URL for the "my" site. For example,</p> <ul style="list-style-type: none"> • If your environment uses SharePoint and SharePoint Online, <i>https://<Microsoft SharePoint server>/my</i>. • If your environment uses Microsoft OneDrive for Business, <i>https://<your O365 domain>-my.sharepoint.com/personal/admin_<domain>_onmicrosoft_com/_layouts/15/onedrive.aspx</i> <p>If the personal site includes usernames or other Microsoft Active Directory attributes, enter the path including these attributes. For example, <i>https://sharepoint.example.com/my/<sAMAccountName></i>.</p> <p>Optionally, to automatically add followed sites, complete the following steps:</p> <ol style="list-style-type: none"> a. Add a repository for the "my" or personal SharePoint site. b. Select the Add sites followed by users on this site for the repository. c. On the User-defined tab, enable a user-defined repository permission. Make sure that you select the Enable 'User Defined Shares' and Automatically add sites followed by users check boxes. For instructions, see Enable user-defined repository permissions. |

| Storage type | Description |
|--------------|--|
| CMIS-based | <p>For storage providers using CMIS support that you have added to BEMS, both AtomPub and Web Services web addresses are supported. A repository ID may be optionally specified and a path inside the repository may also be optionally specified.</p> <p>If no repository ID is specified, then all repositories that a user has access to are listed to the user. If no path is specified, then the listing starts at the repository root.</p> <p>Following is the format of the paths for BEMS Docs repositories for accessing CMIS repositories:</p> <ul style="list-style-type: none"> • <code><ATOM-PUB-URL>?RepositoryId=<REPOSITORY-ID>&RelativePath=<REPOSITORY-PATH></code> • <code><WEB-SERVICES-URL>?RepositoryId=<REPOSITORY-ID>&RelativePath=<REPOSITORYPATH>&BindingType=WebService</code> <ul style="list-style-type: none"> • Where ATOM-PUB-URL and WEB-SERVICES-URL is specific to the CMIS vendor. Contact your CMIS vendor for more information. • Where REPOSITORY-ID is the CMIS repository ID (optional). • Where REPOSITORY-PATH is the path inside the CMIS repository (optional). |

8. Optionally, in the **List** drop-down list, select an existing list that you want this repository to belong to. If no list is defined, you can create one later or leave this field blank.

If a List is selected, select the **Enable inheriting of access control of repository list** checkbox to apply the Access Permissions of the List to the repository. If the check box is not selected, you must define specific access permissions for this share (repository).

9. Select **Manage access through WatchDox** if you have a BlackBerry Workspaces server in your environment, have configured the Unified Content Connector, and you want to manage access permissions from the BlackBerry Workspaces server. For more information about the Unified Content Connector, contact BlackBerry Technical Support Services.
10. In the **Access permissions** section, click **Add Users/Groups**.
11. In the **Search In** field, enter a new domain or keep the default domain.
12. In the **Search for Users in Active Directory** field, type a full or partial search string. Click **Search**.
13. In the search results, select one or more entries.
14. Optionally, select the **Use Different Credentials** and enter a username and password to configure a different Username and Password for accessing this repository by these users.
15. Click **Add**.
16. Optionally, specify files and folders to synchronize to users' Offline folder in the BlackBerry Work Docs app.
- Click **Add**.
 - Navigate to the file or folder that you want to synchronize to users' offline folder.
 - Click **Add**.
 - Repeat steps a to c for each file and folder that you want to synchronize.
17. Click **Test** and enter the test user login credentials to validate the repository information on behalf of the user, including the repository path, access to the user account, and the offline files and folders path. If the test fails, the appropriate message is displayed (for example, **No user or user group assigned permission to access the repository** or **Could not validate path(s) <file/folder path>**). Resolve the issue that is specified and test again.

18. Click **Save**. If the save fails and the issue is determined, the appropriate error message is displayed (for example, if you have a repository named Marketing and you create another repository with the same name, the error message **Repository already exists with name Marketing** is displayed). Resolve the issue that is specified and save again.

After you finish: To remove the offline files and folders, select the checkbox beside the files or folders to delete. Click **Delete**.

Edit a repository

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

Define a repository list

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

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

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Repositories**.
3. Click the **Admin Defined** tab.
4. Click **New List**.
5. In the **Display Name**, enter the name that will be displayed to authorized users on their mobile devices.
6. In the **Select Repositories to include** field, select the defined repositories to include.
7. Select **Manage access through WatchDox** if you have a BlackBerry Workspaces server in your environment, have configured the Unified Content Connector, and want to manage access permissions from the BlackBerry Workspaces server. For more information about the Unified Content Connector, contact BlackBerry Technical Support Services.
8. Click **Save**.

After you finish:

If you don't use a BlackBerry Workspaces server in your environment, complete the following tasks:

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

Add users and user groups to repositories and list definitions

You must add Microsoft Active Directory users and groups to a repository definition or a list definition before you can configure access permissions. Users and groups that are added automatically receive the default access permissions.

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

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

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

Allow user-defined repositories

You can allow users to create their own links to existing document repositories using the BlackBerry Work app or Docs Self-Service web console.

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

1. [Enable user-defined repository permissions](#)
2. [Change user access permissions](#)

Enable user-defined repository permissions

Before you begin: For users to access their Microsoft SharePoint repositories on their devices, make sure that they have the "Read" permission level and the "Browse Directories" permission assigned.

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Repositories**.
3. Click the **User Defined** tab.
4. Select the **Enable 'User Defined Shares'** checkbox to allow your mobile users to define their own data sources.
5. Optionally, select the **Automatically add sites followed by users** checkbox for authorized Microsoft SharePoint repositories with the required MySite plugin enabled.

To automatically add followed sites, complete the following steps:

- a. On the Admin-defined tab, add a repository for the "my" or personal SharePoint site. For instructions, see [Define a repository](#).
- b. Select the **Add sites followed by users on this site** for the repository.
- c. On the User-defined tab, make sure that you select the **Enable user-defined shares** and **Automatically add sites followed by users** check boxes.
6. In the **Storage** section, select one or more storage services.
If you do not select at least one storage option, the user-defined option is disabled.
7. In the **Access Permissions** section, click **Add users/groups**.
8. In the **Search In** field, enter a new domain or keep the default domain.
9. Select **Users** or **Groups**.
10. In the **Search for Users in Active Directory** field, type a full or partial search string. Click **Search**.
11. In the search results, select one or more entries.

12. Optionally, select the **Use Different Credentials** and enter a username and password to configure a different Username and Password for accessing this repository by these users.
13. Click **Add**. The users and groups added automatically receive the default access permissions.
14. Select **Add New Repositories** to allow users to create their own links to existing document repositories using the BlackBerry Work app or Docs Self-Service web console. For more information on access permissions, see [Access permissions](#).
15. Click **Save**.

Access permissions


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

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

| Permission | Permissions Attributes | Default setting |
|-----------------------|---|---------------------------|
| List (Browse) | View and browse repository content (for example, subfolders and files) in a displayed list, and sort lists by Name, Date, Size, or Kind | Enabled |
| Delete Files | Remove files from the repository | Enabled |
| Read (Download) | Download repository files to the user's device and open them to read | Enabled |
| Write (Upload) | Upload files (new/modified) from user's device to the repository for storage | Enabled |
| Cache (Offline Files) | Temporarily store a cache of repository files on the device for offline access You can designate files and folders to synchronize to users' BlackBerry Work Docs app Offline folder. | Enabled |
| Open In | Open a file in a format-compatible app on the device | Enabled |
| Create Folder | Add new folders to the repository | Enabled |
| Copy/Paste | Copy repository file content and paste it into a different file or app | Enabled |
| Check In/Check Out | When a file is checked out, the user can edit, close, reopen, and work with the file offline. Other users cannot change the file or see changes until it is checked back in | Enabled (SharePoint only) |
| Add New Repositories | Permits new repositories to be added from the user's mobile device | Disabled |

| Permission | Permissions Attributes | Default setting |
|----------------------|---|--------------------|
| Generate Shared Link | Users can generate a link to a file and folder and send the link to recipients The Generate Shared Link requires an updated BlackBerry Work app. | Enabled (Box only) |

Change user access permissions

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

View user repository rights


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

1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Repositories**.
3. Click **Users**.
4. In the **Search Users** field, begin typing the user's Microsoft Active Directory account name. If you don't see the user you want, extend or narrow the search string or click **Switch Domains** to search a different Microsoft Active Directory domain.
5. Click the user name. The **Defined by** column specifies if the repository is admin-defined or user-defined.
6. Click the name of the repository or on the row to view the user's access permissions. To modify the access permissions, see [Change user access permissions](#).
7. Optionally, if the repository is admin-defined, in the **Override Path for this user** field, enter an override path.
8. Optionally, if the repository is user-defined, in the **Repository name** field, enter a new repository name.

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

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

| Attributes | Task |
|---|---|
| <p>The Box email address matches one of the following Microsoft Active Directory attributes:</p> <ul style="list-style-type: none"> • mail • userPrincipalName • proxyAddresses • targetAddress | <p>No action is required.</p> |
| <p>The Box email address matches a Microsoft Active Directory attribute other than the attributes listed above.</p> | <p>Set the config value, LDAPUserCheckAttribute, to specify the Microsoft Active Directory attribute that contains the custom Box email address.</p> <ol style="list-style-type: none"> On the computer hosting BEMS, open a command prompt and navigate to the client.bat file. By default, the file is located at <code><drive>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<version>\bin</code>. Type <code>client.bat -u domain name\username</code>. Press Enter. <ul style="list-style-type: none"> • Where <i>domain name</i> is the name of the domain BEMS is located in. • Where <i>username</i> is the name of an administrator account on BEMS. Type the password for the BEMS user account. Press Enter. Set the LDAPUserCheckAttribute. Type <code>docs:config Config-Name Config-Value</code>. <ul style="list-style-type: none"> • Where <i>Config-Name</i> is LDAPUserCheckAttribute. • Where <i>Config-Value</i> is the name of the Microsoft Active Directory attribute you want to add. For example, BoxLogin. Optionally, confirm the <i>Config-Value</i> is set. Type <code>docs:config Config-Name</code> |

| Attributes | Task |
|--|---|
| The Box email address does not match any Microsoft Active Directory attribute. | <p>Complete one of the following tasks:</p> <ul style="list-style-type: none"> • Add an attribute to contain the Box email address and use the previous configuration. See the instructions above. • Enable the EnablePersonalBoxAccess config value to allow users to use personal Box email addresses without adding an attribute. <p> Warning: If you use this method to allow users to use custom Box email addresses to access Box, users can copy documents from your organization's network to their private Box accounts.</p> <ol style="list-style-type: none"> a. On the computer hosting BEMS, open a command prompt and navigate to the client.bat file. By default, the file is located at <code><drive>:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server Distribution\gems-quickstart-<version>\bin</code>. b. Type <code>client.bat -u domain name\username</code>. Press Enter. c. Type the password for the BEMS administrator account. Press Enter. d. Set the EnablePersonalBoxAccess to 1 to enable the attribute. Type <code>docs:config EnablePersonalBoxAccess 1</code>. e. Optionally, confirm EnablePersonalBoxAccess is enabled. Type <code>docs:config EnablePersonalBoxAccess</code>. |

Configuring Docs for Rights Management Services

Active Directory Rights Management Services (AD RMS) and Entra-IP RMS from Microsoft allows documents to be protected against access by unauthorized people by storing permissions to the documents in the document file itself. Access restrictions can be enforced wherever the document resides or is copied or forwarded to. For documents to be protected with AD RMS or Entra-IP RMS, the app that the document is associated with must be RMS aware. For more information about AD RMS and Entra-IP RMS, visit [Comparing Azure Information Protection and AD RMS](#).

Note: For this release, BEMS doesn't support both the AD RMS and Entra-IP RMS in the same environment.

Support for RMS protected documents is provided through two methods:

- In Docs and BlackBerry Work, support for RMS protected documents is provided through the Microsoft Office Web Apps and Office Online Server with viewing and editing enabled through the BlackBerry Access browser. Note that while BlackBerry Access browser is a BlackBerry Dynamics app with all the secure features it provides, it has only partial support for RMS features.
- In BlackBerry Work, support for RMS protected documents is provided directly in BlackBerry Work and through BlackBerry Work.

The following table compares the features of RMS protected documents in BlackBerry Work and through BlackBerry Access. These features require a client that is RMS aware.

| | RMS protected documents directly in BlackBerry Work | RMS protected documents through BlackBerry Access |
|----------|---|---|
| Features | <ul style="list-style-type: none"> • View protected documents directly in BlackBerry Work. • Protect unprotected documents in BlackBerry Work. • Change permissions for documents in BlackBerry Work. • Upload a new file and save it as protected. | View and edit protected documents in Docs and BlackBerry Work through the BlackBerry Access browser. |
| Security | Users can save what is on screen as a web clip and this screenshot file can be shared with other BlackBerry Dynamics apps. Mitigation is to disable web clips in the BlackBerry Access policy. | <ul style="list-style-type: none"> • Share the Microsoft Office Web Apps or Office Online Server URL that is used to render the document viewing or editing with other BlackBerry Dynamics apps. The URL expires in thirty minutes but during this time, other BlackBerry Dynamics apps might be able to access it without any authentication. For example, if it is shared with BlackBerry Work, the URL can be emailed to others. If it is shared with a BlackBerry Dynamics app that allows printing, then the page that is rendered might be printed. Mitigation would be to enable user agent in the BlackBerry Access policy and then use it to create filtering rules in the Microsoft Office Web Apps or Office OnlineServer so that only BlackBerry Access is able to access the URL. The Microsoft IIS URL Rewrite extension can be used to create the rules. • Users can save what is on screen as a web clip and this screenshot file can be shared with other BlackBerry Dynamics apps. Mitigation is to disable web clips in BlackBerry Access policy. • When editing a document, by default, copy and paste of content would be possible by default policies only within the BlackBerry Dynamics secure container environment. Ensure that the protection provided is adequate given these limitations and satisfies your RMS protection requirements before enabling this support. |

Rights Management Services restrictions

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

- View right is required to view documents.
- Edit right is required to edit documents.

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

Docs deployment for Active Directory Rights Management Services support




1. On the computer that hosts BEMS, install the Rights Management Services Client 2.1. To download the client, visit www.microsoft.com/downloads and search for ID=38396.
2. If using self-signed certificates in AD RMS server, add the SSL certificate for `https://<AD RMS server URL>` to trusted CA list.
3. In Internet Explorer, add `https://<AD RMS server URL>` to the Local Intranet site list.
4. Install the Docs service with the Good Technology Common Services service running as a domain user. If you installed BEMS using the service account, you can change the BEMS service account. For instructions, visit support.blackberry.com/community to read article 58463.
5. If a super users group is not already configured in AD RMS server, configure one. Then add BEMS process user (Good Technology Common Services service user) to this AD RMS super users group.
6. On the AD RMS server, find the file `%systemdrive%\Inetpub\wwwroot_wmcs\Certification\ServerCertification.asmx` and add Read and Read & Execute permissions for the following:
 - the "AD RMS Service Group".

Note: The AD RMS Service Group is a local group and not a domain group.

 - the computer account for each of the BEMS servers.
 - The Good Technology Common Services service user.

Steps to deploy Entra IP Rights Management Services support for the Docs service

When you configure Entra IP RMS support for the Docs service, you complete the following steps:

| Step | Action |
|---|---|
|  | On the computer that hosts BEMS, install the Rights Management Services Client 2.1. To download the client, visit www.microsoft.com/downloads and search for ID=38396. |
|  | Obtain an Entra app ID for the BEMS-Docs component service. |
|  | <p>If necessary, migrate any labels that you need in the environment.</p> <p>Note: BEMS-Docs service only supports migrated unified labels. For instructions to migrate labels, visit https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-migrate-labels.</p> |

| Step | Action |
|------|--|
| 4 | Convert protections templates to labels. For more information about converting templates to labels, visit https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-templates and read "To convert templates to labels". |
| 5 | Configure the Docs security settings |

Using the Docs Self-Service web console

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

The web address to access the Docs Self-Service web console can be one of the following web addresses. Contact your BEMS or BlackBerry Work administrator for the specific web address in your environment.

- If you configured single sign-on, navigate to `https://<bems_fqdn>:<port>/docsconsole-sso`
- If you require a username and password, navigate to `https://<bems_fqdn>:<port>/docsconsole`

Add a repository using the Docs Self-Service web console

Before you begin: You must be authorized to access the Docs Self-Service web console. For instructions on authorizing access to the Docs Self-Service web console, see [Allow user-defined repositories](#). Users must have the Add New Repositories permission to add a repository from the browser.

1. In your computer browser, open a browser and navigate to the Docs Self-Service console at one of the following web addresses:
 - If your environment is configured for single sign-on, go to `https://<bems_fqdn>:<port>/docsconsole-sso` (for example, `https://bemsserver.example.com:8443/docsconsole-sso`). If you are authorized, you are automatically logged in using your Microsoft Active Directory credentials.
 - If your environment is configured to require a username and password, go to `https://<bems_fqdn>:<port>/docsconsole` (for example, `https://bemsserver.example.com:8443/docsconsole`). You must enter your Microsoft Active Directory credentials.
2. Click **Add Repository** to define a new data source.
3. In the **Display Name** field, type a display name. This name is displayed in repository lists in the console and on your device.
4. In the **Storage Type** field, select a storage type (for example, File Share, SharePoint, or Box).
5. In the **Path** field, enter the path.
6. Click **Save**.

To remove a repository, click  beside it.

Configuring support for Microsoft SharePoint Online and Microsoft OneDrive for Business

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

Microsoft SharePoint Online provides the following ways for users to authenticate and perform SharePoint operations:

- Using on-premises Microsoft Active Directory
 - DirSync with Password Hash: Users and their passwords on Microsoft Active Directory are synchronized with Microsoft Office 365. Users are presented with a login page where they can enter their credentials to access Microsoft SharePoint Online.
 - Active Directory Federation Service (ADFS): ADFS serves as a Secure Token Service. Behind the scenes (in background), users are redirected to ADFS for authentication and are issued security tokens that are then used by Microsoft SharePoint Online to sign in. Microsoft SharePoint Online users do not need to enter credentials when accessing from the corporate network, which typically enables sign-on scenarios.
- Using modern authentication
 - Enable modern authentication in the BEMS Dashboard.

These authentication mechanisms are supported by the Docs service and all preparations take place on the server side exclusively. No device changes are required to use the on-premises Active Directory. The following prerequisites are required for users to authenticate to Microsoft SharePoint Online:

- For users to authenticate to Microsoft SharePoint Online using Microsoft Active Directory, Microsoft SharePoint Online is deployed in your environment based on DirSync with Password Hash or ADFS authentication mechanisms.
- For users to authenticate to Microsoft SharePoint Online using modern authentication, Microsoft SharePoint Online is deployed in your environment and enabled for modern authentication in the BEMS Dashboard.

Configure Microsoft SharePoint Online and Microsoft OneDrive for Business

For instructions on enabling modern authentication for Microsoft SharePoint Online, see [Enable modern authentication for Microsoft SharePoint Online](#).



1. In the **BlackBerry Enterprise Mobility Server Dashboard**, under **BlackBerry Services Configuration**, click **Docs**.
2. Click **Settings**.
3. In the **SharePoint Online** section, in the **SharePoint Online Domain** field, type the FQDN for your primary Microsoft SharePoint Online domain. Then, separated by a comma, type your FQDN for Microsoft OneDrive for Business. For example, example.sharepoint.com,myexample.sharepoint.com.
4. Click **Save**.
5. Restart the Good Technology Common Services service.
6. Click **Repositories**.
7. Click **New Repository**.
8. In the **Display Name** field, type a name for the repository,
9. In the **Storage Type** drop-down list, click **SharePoint**.
10. In the **Path** field, type path for your primary Microsoft SharePoint Online site from Step 2
11. Click **Save**.
12. Optionally, click **New Repository** for Microsoft OneDrive for Business and repeat steps 8 to 11 using the path for the Microsoft OneDrive for Business.
You can use the username wild card in the web address. For example, https://myexample.sharepoint.com/personal<username>_goodshare_us.
You can lookup the path web address by logging in to the Microsoft SharePoint Online website and click the Microsoft OneDrive option. Copy the web address into the Path field.
13. Click **Save**. Both repositories are listed in the repository list.

Auditing the Docs service

You can configure BEMS to audit user actions to assist in identifying and troubleshooting issues between users and the Docs service. After you enable the Docs service, user actions such as downloads, browsing history, and files created can be audited. For more information about configuring the Docs service audit properties and the audit operations that you want to log, see the [Monitoring and reporting content](#).

In a BlackBerry UEM environment, add an app server hosting the BEMS-Docs service to a BlackBerry Dynamics connectivity profile

To allow users in a BlackBerry UEM environment to access the BlackBerry Docs service on one or more BEMS-Docs servers, you must add the BEMS instances to a BlackBerry Dynamics Connectivity profile. Then you must assign the profile to users. When you add a BEMS instance to the BlackBerry Dynamics connectivity profile, you add the BEMS FQDN, the BEMS Port, one or more BlackBerry Proxy clusters, and other routing options.

1. On the menu bar, click **Policies and Profiles > Networks and Connections**.
2. Click  beside **BlackBerry Dynamics connectivity** profile to create a new connectivity profile or click on the default BlackBerry Dynamics connectivity profile to edit it.
3. In the **App servers** section, click **Add**.
4. Search for and select **Feature - Docs Service Entitlement** app.
5. Click **Save**.
6. In the table for the app, click .
7. In the **Server** field, specify the FQDN of the BEMS server.
8. In the **Port** field, specify the port of the BlackBerry Proxy cluster that is used to access BEMS. By default, the port is 8443.
9. In the **Priority** drop-down list, specify the priority for the BEMS instance that the BlackBerry Work Docs will use.
10. In the **Route type**, select **BlackBerry Proxy cluster**.
11. In the **Primary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster (primary cluster 1) that you want to set as the primary cluster.
12. In the **Secondary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
13. Click **Save**.
14. Assign the Feature - Docs Service Entitlement app to users or user groups. You can use one or more of the following options. For instructions, see the [see the BlackBerry UEM Administration content](#).
 - a) To assign the app, do one of the following:
 - Assign the app directly by completing one of the following tasks:
 - [Assign the entitlement app to a user group](#)
 - [Assign the entitlement app to a user account](#)
 - Assign the entitlement app to an app group by completing one of the following tasks:
 - [Assign the app group to a user group](#)
 - [Assign the app group to a user account](#)

Configuring Good Control for Docs service

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

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

Entitle users, configure the Docs service entitlement



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

Configure the Docs service entitlement, add BEMS to Good Control

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

Publish the Docs app to users

When you publish the Docs app, you publish it for all users in a group. The "Feature - Docs Service Entitlement - ALL" enables the Docs button in the BlackBerry Dynamics Launcher. You should create separate groups and assign the apps and features to the groups as required instead of the Everyone group. When the "Feature - Docs Service Entitlement - ALL" is assigned to users, the minimum license required is BlackBerry Enterprise Mobility Suite - Collaboration Edition for each user that it is assigned to. For more information about licenses, see the [Licensing content](#).

1. In Good Control, under **Apps**, click **App Groups**.
2. Beside the group that you want to assign the entitlement to, click .
3. Click the **Apps** tab.
4. Beside **Entitled enterprise apps**, click .
5. Select the **Feature - Docs Service Entitlement - ALL** checkbox.
6. Click **OK**.

Enable server affinity for Docs in BlackBerry Work



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

1. In Good Control, under **Policies**, click **Policy Sets**.
2. Click the policy you want to apply.
3. Click the **Apps** tab.
4. Expand **App Specific Policies**.
5. Click **BlackBerry Work** or **Good Control**.
6. Click the **Deprecated** tab.
7. Under **Preferred Docs Server Configuration**, in the **Server Hosts** field, type the FQDN of the computer that hosts BEMS and a colon followed by port 8443. For example, *<FQDN of the GEMS server>:8443*.
You can add additional preferred servers. Each server you add must be separated with a comma and no spaces.
8. Click **Update**.
9. Repeat steps 1 to 6 for each policy that you want to use with the Docs service.

Configuring the Docs instance for high availability

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

- 1. [Configure each new Docs instance to use the existing database.](#)
- 2. Complete one of the following actions:

| Environment | Tasks |
|--|---|
| If you have a BlackBerry UEM environment | Add the computer that hosts the Docs service, to the entitlement. |
| If you have a Good Control environment | <ul style="list-style-type: none">a. Whitelist each new Docs server host and port in Good Control. For instructions see, "Adding Client Connections" in the BlackBerry Administration content for Good Control.b. Configure each new Docs instance in Good Control for the BlackBerry Work app. For instructions, see "Adding BEMS to the BlackBerry Application Server List" in the BlackBerry Administration content for Good Control. |

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](#).

Next steps

After you complete the tasks to configure the Docs service, see to the following configuration content to configure the necessary services and install and configure BlackBerry Dynamics apps:

- For users to access, synchronize, and share documents natively using their enterprise file server, Microsoft SharePoint Online, SharePoint, Microsoft OneDrive for Business, Box, and content management systems supporting CMIS, without the need for VPN software, firewall reconfiguration, or duplicate data stores, assign the app entitlements to the organization to allow users to use the BlackBerry Work Docs app. For more information about managing BlackBerry Work, [see the BlackBerry Work, BlackBerry Notes, and BlackBerry Tasks Administration content](#).
- [BEMS Core service](#): This service provides the core functionality of BEMS. You must configure the Core services for the shared settings for all of the BEMS services (for example, certificates, database settings).
- [BlackBerry Mail \(BlackBerry Push Notifications\) service](#): This service accepts push registration requests from iOS and Android devices, and then communicates with Microsoft Exchange Server or Microsoft Office 365 using Microsoft Exchange Web Services protocol to monitor the user's enterprise mailbox for changes.
- [BlackBerry Connect service](#): This service provides secure instant messaging, company directory lookup, and user presence information to iOS and Android devices.
- [BlackBerry Presence service](#): This service provides real-time presence status to BlackBerry Work, BlackBerry Dynamics Launcher, and third-party BlackBerry Dynamics apps.

Appendix: File types supported by the BlackBerry Docs service

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

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

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

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

Supported files and storage types

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

- File Shares
- Microsoft SharePoint Online

- Microsoft SharePoint

For information about the supported Microsoft SharePoint versions, [see the BEMS Compatibility Matrix](#).

Supported devices

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

Windows Folder Redirection (Native)

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

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

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

The following different folders can be redirected.

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

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

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

Enable folder redirection and configure access

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

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

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

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

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

Local Folder Synchronization – Offline Folders (Native)

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

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

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

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

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

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

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

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

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

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

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

Once the files are synchronized to the "Home Directory," IT administrators can make use of the Docs service feature in which Microsoft Active Directory attributes can be specified in the path to expose the user's "Home Directory" to the BlackBerry Work app running on provisioned mobile devices. It is also important to remember

that for users who have their home folder defined in Microsoft Active Directory, Folder Redirection works when the folder redirection path is the same as the user's home folder in Microsoft Active Directory.

Supported Microsoft Office Web Apps and Office Online Server file types

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

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

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

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

| File format | View | Edit |
|------------------|------|--|
| Open XML (.xlsx) | ✓ | ✓ |
| Binary (.xlsb) | ✓ | ✓ |
| Binary (.xls) | — | — |
| Macro (.xlsm) | ✓ | ✓ However, you are prompted to create a copy of the file that has the macros removed when you save the changes that you have made |

| File format | View | Edit |
|---|------|------|
| Other file formats (.xltx, .xltn, .xlam, .xlm, .xla, .xlt, .xml, .xll, .xlw, ods, .prn, .txt, .csv, .mdb, .mde, .accdb, .accde, .dbc, .igy, .dqy, .rqy, .oqy, .cub, .uxdc, .dbf, .slk, .dif, .xlk, .bak, .xlb) | — | — |

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

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

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

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

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

Legal notice

©2023 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

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

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

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

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, 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