BlackBerry Workspaces

Administration Guide

10.0

Contents

Introducing BlackBerry Workspaces administration console..... 7
Configuring and managing BlackBerry Workspaces..... 7
BlackBerry Workspaces specifications.....8

Getting started..... 11
Sign in to BlackBerry Workspaces.....11
Sign in with username and password.....11
Sign in using your email account.....11
Sign out of BlackBerry Workspaces.....11
Introducing BlackBerry Workspaces administration console..... 12

Managing resources using Central Management.....13
Locate entities in Central Management..... 13
Display a list of workspace files that can be accessed by a specific user..... 13
Search for all workspaces used by a specific user..... 13
Data display options.....13
Managing users.....14
Administrator and user roles..... 14
Add users.....17
Edit users.....17
Delete users.....18
Bulk delete users..... 18
Import users..... 18
Export users.....19
Reset the password for a user.....20
Managing workspaces.....20
Create a regular workspace.....20
Create a transient workspace.....20
Share a workspace..... 21
Add a group or user..... 21
Edit workspaces.....22
Edit workspace permissions.....22
Generate a workspace report..... 22
Create a snapshot.....23
Delete workspaces.....23
Ransomware recovery..... 23
Export workspaces list..... 24
Managing distribution lists.....24
Add distribution lists.....24
Edit distribution lists.....24
Remove distribution lists.....24
Import distribution lists..... 25
Export distribution lists..... 25
Managing permissions.....25
Edit permission sets..... 26

Manage permissions.... 26
Send a message to workspace members.... 26
Generate a members management log.... 27
Delete permission sets.... 27
Export the permissions table.... 27
Managing documents.... 27
Download documents.... 28
Edit document permissions.... 28
Add a group to a file.... 28
Delete documents.... 28
Export a list of documents.... 29

Provisioning users and devices.... 30
Provisioning roles by email domain.... 30
Add domain roles.... 30
Edit domain roles.... 30
Delete email domains.... 30
Provisioning roles using Active Directory.... 31
Working with Microsoft Active Directory.... 31
Configure an Active Directory connection.... 31
Add Active Directory roles.... 32
Edit Active Directory roles.... 32
Delete roles from an Active Directory group.... 33
Managing blocked users.... 33
Block an email address or Active Directory group.... 33
Remove users from the blocked users list.... 33
Search for blocked users.... 33
Import a list of blocked users.... 34
Export the list of blocked users.... 34
Managing BlackBerry Workspaces apps.... 34
Manage BlackBerry Workspaces apps.... 34
Disable BlackBerry Workspaces apps.... 35
Enable devices.... 35
Export a list of user apps.... 35

Configuring integrations.... 36
Managing content connectors.... 36
Add a content connector.... 36
Edit a content connector.... 37
Verify a content connector.... 37
Delete a content connector.... 37
Managing SharePoint protectors.... 38
Define default workspace administrators.... 38
Manage the internal users whitelist.... 38
Add a SharePoint protector.... 38
Edit a SharePoint protector.... 39
Define libraries to sync.... 39
Remove synced libraries.... 40
Managing Windows File Share connectors.... 40
Define default workspace administrators.... 40
Add a Windows File Share connector.... 40

Edit a Windows File Share connector.....41
Define network drives to sync.....41
Remove synced network drives.....41
Managing the Workspaces Email Protector.....41
Enable the BlackBerry Workspaces Email Protector.....41
Remove the email protector.....42
Enable Office Online integration.....42
About Office Online configuration.....42
Managing the DocuSign integration.....43
Enable DocuSign in BlackBerry Workspaces.....43
About DocuSign Integration.....43
Managing the Dropbox connector.....43
Create a Dropbox app for accessing a Dropbox repository.....43
Add a Dropbox connector.....44
Managing the iManage connector.....44
Add an iManage connector.....44
Add an iManage Cloud connector.....45
Workspaces Connector for BEMS.....45

Setting security policies.....48
Set file policies.....48
Set mobile policies.....49
Set sharing policies.....49
Set sync policies.....50
Bring Your Own Key (BYOK).....50
Set watermarks as an organizational policy.....52
About working with watermarks.....53

Generating logs and reports.....55
Generate a user activity report.....55
Generate a workspace activity report.....55
Generate an audit log.....55
Generate a licensing report.....55
Generating usage reports.....56
Generate an active users report.....56
Generate an active users report by date range.....56
Generate an inactive users report.....57
Generate a weekly file activity per user report.....57
Generate a weekly organization activity report.....57
Generate a workspaces snapshot report.....57
Generating storage reports.....57
Configure storage alerts.....57
Generate a workspaces storage report.....58
Generate a sent files storage report.....58
Generate a weekly organization storage report.....58
Generate an organization activities report.....58
Generate an authentication activities report.....59

Configuring BlackBerry Workspaces.....60
Customize BlackBerry Workspaces Web Application.....60

Configure and customize emails....61
Configure ICAP....61
Configure Syslog....61
Defining tags....62
Add a tag....62
Edit a tag....62
Delete a tag....62
Defining workspace roles....62
Add a workspace role....62
Edit a workspace role....63
Delete a workspace role....63
Configure the Enterprise mode....63

Managing authentication....64
Automatically authenticate a user....64
Block unprovisioned users from creating accounts....64
Configure browser inactivity timeout....65
Configure the organization authentication method....65
About email authentication....65
About username and password authentication....66
About Microsoft Active Directory authentication....66
About BlackBerry Enterprise Identity authentication....66
About OAuth integration with third-party providers....67
About multimode authentication....67
About BlackBerry Dynamics authentication....67
Simplified login process for internal users....67
Configure service accounts....67
Add a service account....67
Edit a service account....68
Delete a service account....68

Introducing BlackBerry Workspaces administration console

BlackBerry Workspaces administration console allows you to manage BlackBerry Workspaces for your organization. To access the console you must be assigned to one of the four administration user roles. Each role has different permissions that control the functionality that is available for that role.

Configuring and managing BlackBerry Workspaces

Use the administration console to access and configure the following features of BlackBerry Workspaces:

Manage and provision users

- To provision users, either add them directly in the administration console or import a large number of users from a .csv file. Assign users to administration and user roles that control their ability to use BlackBerry Workspaces features.
- Create and manage groups to control access rights to files in workspaces.
- Create and manage BlackBerry Workspaces Distribution Lists in the the administration console or using a .csv file.
- Create and manage your organization's workspaces.
- Set access permissions for files in workspaces and export lists of workspace files.
- Prepare and export logs of user activity in shared files. Log files are filtered by sender.
- Prepare and export logs of workspace activities.
- Assign roles at the email domain level.
- Assign roles to Microsoft Active Directory groups.
- Configure the integration to Active Directory servers and groups.
- Prepare and export logs of all user activity for selected users.
- Prepare and export logs of all group activity for selected groups.
- Manage BlackBerry Workspaces app on users' devices. For example, enable or disable access to your organization's workspaces and view device details.

Configure integrations

- Add and manage connectors to external repositories, such as SharePoint and Windows File Share connectors
- Enable BlackBerry Workspaces Email Protector
- Enable Office Online integration

Set security policies

- Set policies to protect files in workspaces and shared items.
- Tune system performance to upload files.
- Set policies for mobile devices.
- Set file sharing policies on mobile devices.
- Set default file sharing permissions for workspaces and shared items.
- Set policies for retaining files prepared for online viewing.
- Set the default parameters for recipient access to shared files

- Define the offline access period of files.
- Set document watermarks.

Generate logs and reports

Generate logs and reports for:

- User activities
- Workspace activities
- Administrator audit log
- Licensing

Configure parameters

- Customize the interface with your organization's logo and links that point to information such as support, terms and conditions, and so on
- Set the service to send a welcome email, and customize the email as desired for new users
- Configure ICAP
- Connect to a Syslog server
- Monitor storage use and set when to receive storage-related reports
- Define organization tags that can be applied to files.
- Set the enterprise mode for your service
- View and create workspace roles

Configure authentication

- Block accounts for unprovisioned users users and automatic sign out for the web application
- Set and configure the authentication method for your organization.
- Set up service accounts

BlackBerry Workspaces specifications

General specifications

BlackBerry Workspaces meets the following size specifications:

Specifications	Limit
Maximum number of workspaces	No limit
Maximum number of files per workspace	100,000

Conversion

Large documents may take some time to convert. For organizations using Conversion on Demand, the first time a document is opened there may be a delay in displaying the file while conversion is performed. For large files, it is recommended that you open the file after you upload it to convert the document at that time.

File size limits

BlackBerry Workspaces imposes the following file size limits on uploaded files:

- Files marked for secure transfer (encrypted transfer, recipients have full access permissions):
  - 10 GB when uploaded using BlackBerry Workspaces for Windows or the BlackBerry Workspaces app for Mac
  - 2 GB when uploaded BlackBerry Workspaces Web Application using Mozilla Firefox
  - 200 MB when uploaded using the BlackBerry Workspaces Web Application using Google Chrome, Internet Explorer or Safari
  - 70 MB when uploaded from another app using an iPad
  - 40 MB when uploaded from another app using an iPhone
- For documents sent with Workspaces protection:
  - 100 MB for Microsoft Office (Excel, Word, PowerPoint)
  - 500 MB for Adobe PDF

If you have Microsoft Office or PDF files larger than the file limit, they will be sent using secure transfer.

Permissions and supported file types

This section lists the supported file types for each group of permission templates.

Full access

Users can download a copy of the file for full access.

Users can view Office, PDF, and image files through the Workspaces Online Viewer*** and Workspaces mobile apps.

All file types can be securely transferred with Workspaces.

Advanced Rights Management

These permission templates enable users to download protected files with rights management controls. Workspaces app for Windows or the Workspaces app for Mac is needed to open the protected files.

Users can also view rights protected files through the Workspaces Online Viewer*** and the Workspaces mobile apps.

- Supported files: *.doc, *.docx, *.xls, *.xlsx, *ppt, *pptx, *.pps, *.ppsx, *.txt, pdf
- Image files: *.jpg, *.jpe, *.jpeg, *.gif, *.bmp, *.png, *.tif, *.tiff, are also supported, if enabled by your organization.
- All other file types (e.g. *.avi, *.mp4, *.xlsm) are granted with "Full access".

Online only

These permission templates enforce users to only access protected files through the Workspaces Online Viewer***.

Users can also view files through the Workspaces mobile apps.

- Supported files: *.doc, *.docx, *.xls, *.xlsx, *ppt, *pptx, *.pps, *.ppsx, *.txt, pdf
- Image files: *.jpg, *.jpe, *.jpeg, *.gif, *.bmp, *.png, *.tif, *.tiff, are also supported, if enabled by your organization.
- All other file types (e.g. *.avi, *.mp4, *.xlsm) are granted with "Full access".

******* Such files are converted for viewing with the Workspaces Online Viewer. If you are unable to access a file, contact BlackBerry Workspaces Support.

Getting started

Sign in to BlackBerry Workspaces

1. In your browser, enter the URL for the BlackBerry Workspaces administration console.

   Note: If the BlackBerry Workspaces service or your organization has its own dedicated subdomain on the BlackBerry Workspaces cloud, the URL is your organization followed by the domain (for example, https://organization.watchdox.com/ngdox/admin).
2. Enter your email address and click **Sign in**.
   The authentication method for your organization is determined.
3. Do one of the following:
   - If your organization is configured for sign-in by email, sign in using your email address.
   - If your organization is configured for sign-in by username and password, sign in using your username and password.
   - If your organization is configured for any other authentication method, follow the instructions on the screen to sign in.

Sign in with username and password

Before you begin: Sign in to BlackBerry Workspaces. If your organization uses username and password authentication, a sign-in screen with **Email** and **Password** fields appears.

1. If you are an existing user, enter your email address and password.
2. Click **Sign in**.
3. If you are a new user, complete the following steps:
   a) Click the **Create account** tab.
   b) Enter the required information and click **Create account**.

   You are signed in, and the main screen of the BlackBerry Workspaces administration console appears.

Sign in using your email account

Before you begin: Sign in to BlackBerry Workspaces. If your organization uses username and password authentication, a sign-in screen with the **Email** field appears.

1. Enter your email address and click **Sign in**.
   An email is sent to the email address you entered.
2. Open this email in your regular mail, copy the verification code, and return to the sign-in screen.
3. Enter the verification code.
   You are signed in, and the main screen of the BlackBerry Workspaces administration console appears.

Sign out of BlackBerry Workspaces

Click 👤 and then click **Sign out**.
You are signed out.

Introducing BlackBerry Workspaces administration console

In BlackBerry Workspaces administration console, use the toolbar to access other areas of the web application: workspaces, mail, notifications, and account settings.

BlackBerry Workspaces administration console is split into two panes:

- The left pane displays a menu containing all the administration and configuration items. Click an item in the menu to display the settings in the right pane
- The right pane displays the selected menu item, where you can configure settings.

Click ‹ to expand and › to contract the right pane.

Managing resources using Central Management

You can manage users, groups, lists, workspaces, and documents using the tabs in the **Central Management** area. You can filter the contents of the pane to work with organizational entities, for more information, see Locating entities in Central Management.

Locate entities in Central Management

1. In the left pane, click **Central Management**.
2. In the entity type drop-down list, click the arrow, and select the type of entity you want to search for.
3. In the search box, enter the name of the entity that you want to locate.
   The autocomplete mechanism is activated as you type your entry into the search box, offering results that match your entry.
4. Select the desired entity.
   The selected entity is added as a filter and the results displayed in the right pane are filtered accordingly.
5. Access the tabs to view the entity types associated with the chosen entity.
   For example, if you select the **Workspaces** tab after searching for a specific user, the **Workspaces** tab displays a list of all workspaces containing the user.
6. If desired, repeat steps 2-4 to sharpen your search by adding additional filters.
7. To remove a filter, click **x** in the filter area.

Display a list of workspace files that can be accessed by a specific user

You can filter the **Central Management** pane to view all workspace files that can be accessed by a particular user.

1. Select **Users** in the entity type drop-down list, and enter and select the user's name in the search box.
2. Select **Workspaces** in the drop-down list and enter and select the workspace name in the search box.
3. Access the **Documents** tab.
   A list of all files that can be accessed by the user in the workspace is displayed.

Search for all workspaces used by a specific user

You can filter the **Central Management** pane to view all workspaces that can be accessed by a particular user.

1. Access the **Users** tab.
2. From the list of users, click a name.
   The selected user is added as the search filter.
3. Access the **Workspaces** tab.
   A list of all workspaces that the user can access is displayed.

Data display options

Toggle the column heading arrow to sort the data in each tab as follows:

Tab	Data can be sorted by:
Users	• Email • Username

Tab	Data can be sorted by:
Workspaces	• Workspace name • Creation date
Distribution lists	• List name • Creation date
Documents	• File name • Original uploader • Date of last uploaded version • Size

Managing users

You can add users, designate one or more BlackBerry Workspaces roles, and manage users in the **Central Management** > **Users** tab. When you access the tab without filtering, a list of all users that have been defined in the organization is shown.

Administrator and user roles

You can assign BlackBerry Workspaces users to one or more roles. These roles define the user's working context and the actions that are permitted for that user.

Note: When working in BlackBerry Workspaces Web Application, users can also define non-administrative roles for users that they share their workspaces and documents with in the workspace **Permissions** tab.

Note: In some cases, users are automatically assigned certain roles. For example, users who have a file shared with them, or who are invited by a workspace administrator to become an administrator or contributor, are automatically added to BlackBerry Workspaces with certain user roles.

Overview: BlackBerry Workspaces administrator roles

You can assign BlackBerry Workspaces users to one or more Workspaces roles. These roles define the user's working context and the actions that are permitted for that user. This section describes the available administration roles.

Super Admin

Super administrators have full rights to manage all users, groups, distribution lists, and workspaces in the organization and access to all functions of the administration console. Super administrators can view all documents in any of the organization's workspaces. Assign this role to a user who should have all aspects of the BlackBerry Workspaces system. This is an optional role that need not be assigned.

Organization Administrators

Organization administrators can access all functions of the administration console, and can assign new users to any workspace, including new organization administrators. Assign this role to at least one member of the team to configure and administer BlackBerry Workspaces.

Organization administrators cannot view documents in organization workspaces unless they are assigned access permissions as a workspace user.

It is recommended that this role is provisioned to a trustworthy member of the organization because an organization administrator is able to add themselves as a member of any workspace and therefore gain access to all files.

Helpdesk administrator

Helpdesk administrators have access to **Central Management** and **Manage Applications**. Helpdesk administrators cannot view or access documents in any workspace in the organization, but can generate reports. Assign this role to members of the team who are responsible for providing help desk support to your users.

Audit helpdesk administrator

Audit helpdesk administrators have access to **Central Management**, and generate reports. Audit helpdesk administrators have no other administrative rights, cannot access other areas of the administration console, and cannot view documents in organization workspaces unless they are assigned access permissions as a workspace user (see About assigning user roles). Assign this role to a member of the team who is responsible for generating reports either for compliance or management reasons.

Permissions for BlackBerry Workspaces administrator roles

The table below summarizes the permissions for each of the organizational administrator roles described in Overview: BlackBerry Workspaces administrator roles.

	Super administrator	Organization administrator	Helpdesk administrator	Audit helpdesk administrator
Central Management	Full functionality. Access to **Documents** tab	Full functionality but no access to **Documents** tab	Full functionality but no access to **Documents** tab	View only. No access to **Documents** tab
Provisioning Users and Devices	Full functionality	Full functionality	No Access	No Access
Connectors	Full functionality	Full functionality	No Access	No Access
Security Policies	Full functionality	Full functionality	No access	No access
Configuration	Full functionality	Full functionality	No access	No access

Permissions for assigning user roles

The following table shows what user roles each administrator type can assign:

This role:	Can assign the following user roles:
Super administrator	Administrator roles: All User roles: All

This role:	Can assign the following user roles:
Organization administrator	Administrator roles: Organization administrator, Helpdesk administrator, Audit helpdesk administrator User roles: All, except for Legal Investigator
Helpdesk administrator	Administrator roles: Helpdesk administrator, Audit helpdesk administrator User roles: Workspace owner, Exchange sender, MyDox workspace owner
Audit helpdesk administrator	Cannot assign any roles.

Overview: BlackBerry Workspaces user roles

Administrators can assign non-administrative user roles to workspace and Exchange senders. These users can access the BlackBerry Workspaces Web Application, but not the administration console. You can assign more than one of the following roles per user. When multiple roles are assigned, the user has the combined capabilities of the different roles.

Note: Some organization administrator roles are restricted in what rights they can grant to the user roles. For more information, see About assigning user roles.

Workspace owner

Workspace owners have a personal workspace that they can manage with workspace administrator capabilities. In addition, workspace owners can create and delete workspaces within their organization.

Sender

Senders can send files as protected links. An **Exchange sender** does not need be a member of any particular group for any particular workspace. This role can be assigned to a user in addition to the other user roles.

Workspace Contributor

Workspace Contributors can create, view, update, and delete documents in the workspaces they are members of, depending on the access permissions for files that are controlled by the Workspace owner or Admin users. Workspace Contributors can also be assigned the role by Workspace Administrators.

Visitor

Visitors can view documents in a workspace but cannot create or modify them. A visitor is invited to view documents by workspace owners, exchange senders, and workspace contributors, and can be assigned the role by workspace administrators.

Their access permissions for documents are controlled by the user sending them the document, or by the Workspace Owner or Admin users.

MyDox workspace owner

MyDox workspace owners have a personal workspace only, and cannot manage groups. MyDox owners can share files from their personal workspace, and cannot send and receive files in their Inbox and Sent items.

Individual connector workspace owner

Individual connector workspace owners can add and manage external repositories, such as Alfresco, Dropbox, OneDrive for Business, iManage, Sharepoint, and Windows File Share.

Protected user

Protected users have their email attachments automatically protected according to the organization whitelist and blacklist rules defined in the Email Protector section of the Administration console. These users do not have access to other sharing features unless enabled by a different role.

Legal Investigator

Legal investigators can download all files with full access from any workspace, including the Recycle bin.

Note: The use of this role must be licensed from BlackBerry Workspaces.

Add users

1. In the left pane, click **Central Management**.
2. Select the **Users** tab in the right pane.
3. Click +.
4. In the **Email** box, enter the user email address.
5. In the **Aliases** box, add any email aliases that are associated with the user, in a comma-delimited list.
   In BlackBerry Workspaces, the alias is used to associate files with the user. The alias cannot be used to sign in to BlackBerry Workspaces.

   Note: You cannot define an alias that has already been defined for another user.
6. In the **User Name** box, enter the user name.
7. In the **Enable organization roles** area, select the roles that you want the user to have.
8. Click **Add**.
   A confirmation message confirms the operation.

Edit users

1. In the left pane, click **Central Management**.
2. Select the **Users** tab in the right pane.
3. Select one user in the user list.
4. Click ✎.
   The user's identifying information is shown in the **Edit User** dialog.
5. Edit the user information or roles, as relevant.
6. Click **Save** to save the new settings.
   A confirmation message confirms the operation.

Delete users

1. In the left pane, click **Central Management**.
2. Select the **Users** tab in the right pane.
3. Select one or more users in the user list.

   Note: The users that are workspace administrators must be replaced and cannot be fully removed.
4. Click 🗑.
5. Do one of the following:
   - Select **Remove the user from all designated roles, workspace memberships, and any distribution lists, and delete all files in the user's sent items. Note: All files uploaded by this user to workspaces, and all workspaces created by the user, are not deleted and will remain in the organization**.
   - Select **Move ownership of files owned by this user, designated roles, workspace memberships and distribution lists to**, and enter the email address of the desired user.

   Note: If the user you are deleting is a workspace administrator, only the “move” option is available.
6. Click **Apply** to delete the selected users.
   A confirmation message confirms the operation.

Bulk delete users

Use list of multiple users to delete them in bulk from the system. To create a list of inactive users, see Generate an inactive users report.

1. In the left pane, click **Central Management**.
2. Select the **Users** tab in the right pane.
3. Select **Bulk delete**.

   Note: Users that are workspace administrators must be replaced and cannot be fully removed.
4. Copy and paste a .csv format list or enter multiple user emails in .csv, and click **Next**.
5. Do one of the following:
   - Select **Remove the user from all designated roles, workspace memberships, and any distribution lists, and delete all files in the user's sent items. Note: All files uploaded by this user to workspaces, and all workspaces created by the user, are not deleted and will remain in the organization**.
   - Select **Move ownership of files owned by this user, designated roles, workspace memberships and distribution lists to**, and enter the email address of the desired user.

   Note: If one or more of the users you are deleting is a workspace administrator, only the “move” option is available.
6. Click **Apply** to delete the selected users.
   A confirmation message confirms the operation.

Import users

You can import a large number of users using a .csv file. The .csv file columns should be defined so that they correspond to the user data fields in the BlackBerry Workspaces administration console: Email, Name, Aliases, Distribution Lists, and Roles. You can also create distribution lists using the .csv file that you import. You can update the .csv file to add new users and add or update user data. However, you cannot delete users by deleting them from the .csv file and re-importing it. Users must be deleted in the BlackBerry Workspaces administration console.

1. In the left pane, click **Central Management**.
2. Select the **Users** tab in the right pane.

3. Click .
4. Do one of the following:
   - If you have already created a .csv file that contains the new user data, click **Select file** to browse to the CSV data file and select that file. Proceed to step 6.
   - If you would like to create a .csv data file with the new user data, click **Get Template** to download a convenient .csv file with the column headings defined and the table rows blank.
5. Enter the user data in the appropriate columns, including the following information:
   - **User email address**: The main email address used to identify this user. This field is required.
   - **User name**: The user's name.
   - **User aliases**: Additional email addresses associated with this user.
   - **User Distribution Lists**: Names of all BlackBerry Workspaces distribution lists for which this user is a member. For more information on distribution lists, see Managing distribution lists.
   - **User Roles**: Enter the names of all roles assigned to this user, according to the **Role name in import file** column in the following table:

ID	Role name in import file	Role, as defined in BlackBerry Workspaces
0	VISITOR	Visitor
1	VDR_OWNER	Workspace Owner
2	ORG_ADMIN	Admin
4	SDS_USER	Exchange Sender
5	SUPER_ADMIN	Super Admin
6	HELP_DESK	Help Desk
7	VDR_SUBSCRIBER	Workspace Contributor
8	AUDIT_HELP_DESK	Audit Help Desk
11	MOBILE_EDITING	BlackBerry Workspaces Editor User
16	LEGAL_INVESTIGATOR	Legal Investigator

6. Click **Import** to import user data from the .csv file. **Open** or **Save** the .csv file, as relevant.

Export users

Export a list of users in your organization. If necessary, use filters and export only the displayed list.

1. In the left pane, click **Central Management**.
2. Select the **Users** tab in the right pane.
3. Click .
   The user table is downloaded as a .csv data file.

Reset the password for a user

When you reset the password for a user, they receive an email message with instructions to set a new password.

1. In the left pane, click **Central Management**.
2. In the right pane, click the **Users** tab.
3. Select the user that you want to reset the password for.
4. Click **Reset password**.
5. Click **Reset password** to confirm.

Managing workspaces

On the **Central Management** > **Workspaces** tab, you can create new workspaces, view a list of workspaces filtered by workspace name, users, groups, or distribution lists, and export these lists.

Create a regular workspace

Regular workspaces are those that are created directly in your BlackBerry Workspaces account, and appear in the **Workspaces** list.

1. In the left pane, click **Central Management**.
2. Select the **Workspaces** tab in the right pane.
3. Click +.
4. In the **Select workspace type** box, select **Workspaces** to create a regular workspace.
5. In the **Workspace name** box, enter the name of the new workspace.
6. In the **Workspace description** box, enter the workspace description.
7. In the **Workspace administrators** box, enter the email addresses of all the users that you want to define as administrators of the workspace.
8. Select **Read acknowledgement required** to require read acknowledgement for every workspace file.
9. Click **Add**.
   A confirmation message confirms the operation and the new workspace is added to the list.

Create a transient workspace

Transient workspaces are those that are created in an external repository, and appear in the external repository workspaces list.

1. In the left pane, click **Central Management**.
2. Select the **Workspaces** tab in the right pane.
3. Click +.
4. In the **Select workspace type** box, select the external repository where you want to create the workspace.
5. In the **Workspace name** box, enter the name of the new workspace.
6. In the **Workspace description** box, enter the workspace description.
7. In the **Path** box, enter the repository path.

   The path value determines the root level of the repository. It must begin with the same **Allowed path** as set by the Organization Administrator when the connector was configured.

   For example: Where the Organization Administrator set the allowed path to `\\fileshare\`, the following paths are valid:

   - `\\fileshare\`

- `\\fileshare\folderA\folderB`

8. For Windows File Share and SharePoint repositories, enter the **Domain**.
9. In the **User name** and **Password** boxes, enter your access credentials for the external repository.
10. Click **Add**.
    A confirmation message confirms the operation and the new workspace is added to the list.

Share a workspace

1. In the left pane, click **Central Management**.
2. Select the **Workspaces** tab in the right pane.
3. Select the workspace that you want to share.
4. Click ↗.
   The **Share workspace** dialog appears.
5. In the **Add members** box, enter the email addresses of the users you want to make contributors or visitors to this workspace.

   Contributors can add files to and remove files from the workspace. Visitors can access files in the workspace but cannot remove or add new files.

   Note: The default permissions for contributors and visitors are set and can be changed by an organization administrator. For more information, see Set sharing policies.
6. In the **Message** box, enter a message for the users you are sharing the workspace with (optional).
7. In the **Role** drop-down list, select the role to give the users for the workspace.
8. In the **Permission** drop-down list, select the permissions to give the users for the workspace.
9. In the **File expiration** drop-down list, set the time for when access to the files will expire. Select a specific date or never.
10. In the **Watermark** drop-down list, set whether workspaces PDF files are displayed with a watermark.
11. In the **Commenting** drop-down list, set whether users can comment on files in the workspace.
12. Select the **Notify members** check box to notify members that users have been added to the workspace.
13. Click **Share**.
    A confirmation message confirms the operation.

Add a group or user

1. In the left pane, click **Central Management**.
2. Select the **Workspaces** tab in the right pane.
3. Select the workspace that you want to add a group or user to.
4. Click +.
   The **Add new permissions** dialog appears.
5. Select **Group** or **User**.
6. If you select **Group**:
   a) In the **Group name** box, enter a group name.
   b) In the **Group description** box, enter a description (optional).
   c) In the **Group members** box, enter the email addresses or distribution lists for the group that you want to add (optional).
   d) In the **Group Managers** box, enter the email addresses for the group managers (optional).
7. If you select **User**, in the **Users** box, enter the email addresses for the users that you want to add.
8. Click the **Notify members** check box to notify users that new groups or users have been added to the workspace.

9. Click **Next** to set permissions for the new group.
10. Select the group's **Role**.
11. Select the group's **Permission**.

    Note: The **Advanced Rights Management** permissions set is available for BlackBerry Workspaces Enterprise ES Mode and BlackBerry Workspaces Enterprise ES (Restrict Full Access) Mode only.
12. In the **File expiration** list, set the time for when access to the file will expire. Select a specific date, a time period from the list, or never.
    - If you select **Specific date**, click and choose the desired date from the calendar.
13. In the **Watermark** list, set whether workspaces PDF files are displayed with a watermark.
14. In the **Commenting** list, set commenting to On or Off.
15. In the **Apply permissions to** area, choose **This folder and subitems that inherit permissions only** or **This folder and all subitems**.
16. Click **Add**.
    A confirmation message appears confirming the operation. The new group is added to the workspace and all its subfolders and files.

Edit workspaces

1. In the left pane, click **Central Management**.
2. Select the **Workspaces** tab in the right pane.
3. Select the workspace that you want to edit.
4. Click .
   The workspace information is shown in the Edit workspace dialog.
5. Edit the workspace name or description, as relevant.
6. Click **Save** to save the new settings.
   A confirmation message confirms the operation.

Edit workspace permissions

1. In the left pane, click **Central Management**.
2. Select the **Workspaces** tab in the right pane.
3. Select the workspace that you want to edit group permissions for.
4. Click .
5. Select the workspace group that you want to edit permissions for and click **Next**.

   Note: Enter the name of a group member in the search box to filter the displayed group members.
6. Edit the group **Name** and **Description** as desired.
7. Set the group **Role**, **Permissions**, **File expiration**, **Watermark** and **Commenting** settings as desired.
8. Click **Apply**.
   A confirmation message appears.

Generate a workspace report

Export a workspace activities or group management report for workspaces in your organization. If necessary, use filters and export only the displayed list.

Note: The workspace report is capped at 200,000 entries.

1. In the left pane, click **Central Management**.
2. Select the **Workspaces** tab in the right pane.

3. Select one or more workspaces and click .
4. Choose the report type:
   - **Workspace activities**
   - **Group management**
   - **Read acknowledgment compliance report**
5. Choose to generate the report by **All activities** or by **Date range**.
6. Do one of the following:
   - Click **Download** to download the report.
   - Click **Send by email** to send the report to your email.

   A confirmation message appears.

Create a snapshot

Super Admins and Legal Investigators can create a snapshot of a workspace to download the contents of the selected workspace, including the workspace Recycle bin, in a zip file.

1. In the left pane, click **Central Management**.
2. Select the **Workspaces** tab in the right pane.
3. Right-click the desired workspace, and select .
   The workspace contents are downloaded as a zip file.

Delete workspaces

1. In the left pane, click **Central Management**.
2. Select the **Workspaces** tab in the right pane.
3. Select one or more workspaces and click .
   A confirmation message appears.
4. Click **Delete** to delete the workspace.
   The workspace and all its files is deleted. A confirmation message confirms the operation.

Ransomware recovery

Ransomware is a form of cryptovirology extortion, in which your data is encrypted and the attacker demands payment to restore access to that data. Ransomware Recovery allows an organization administrator to recover workspaces infected by malicious software. Workspace files are reverted to a point in time prior to the ransomware infection.

Note: You cannot recover workspaces for deleted users.

1. In the left pane, click **Central Management**.
2. Enter the email address of the target user in the search field.
3. Select the **Workspaces** tab.
4. Select one or more workspaces and click .
5. In the **Select the recovery date and time** area, click .
6. Choose a recovery date from the calendar.
7. Click the **Enter time** field and choose a recovery time.
8. Click **OK**.
9. Deselect the **Block user** check box to allow the user to access BlackBerry Workspaces once recovery is finished.

10. Click **Recover**.
11. Click **Confirm**.

Export workspaces list

Export a list of workspaces in your organization and their details. If necessary, use filters and export only the displayed list.

1. In the left pane, click **Central Management**.
2. Select the **Workspaces** tab in the right pane.
3. Click .
   The workspace table is downloaded as a .csv data file.

Managing distribution lists

On the Central Managmeent > **Distribution Lists** tab, you can manage distribution lists that are added to BlackBerry Workspaces. You can use distributions lists to manage groups of users. Users can use distribution lists when sharing files.

Add distribution lists

1. In the left pane, click **Central Management**.
2. Select the **Distribution Lists** tab in the right pane.
3. Click +.
4. In the **Name** box, enter the name of the new distribution list.
5. In the **Users and distribution lists** box, enter the email addresses of the users and the names of other distribution lists that you want to define as members of the new distribution list. Separate email and addresses with commas.

   Note: Distribution lists can be nested within other distribution lists.
6. Enter an informative description in the **Comment** field (optional).
7. Click **Add**.
   A confirmation message confirms the operation and the new distribution entry appears in the list.

Edit distribution lists

1. In the left pane, click **Central Management**.
2. Select the **Distribution Lists** tab in the right pane.
3. Locate the distribution list that you want to edit by performing a search. For more information, see Locating entities in Central Management.
4. Select the distribution list that you want to edit.
5. Click .
   The distribution list information is listed in the Edit Distribution List window, including the list name, descriptive comments, and the complete list of member names.
6. Edit the distribution list as desired.
7. Click **Save** to save the changes.

Remove distribution lists

1. In the left pane, click **Central Management**.

2. Select the **Distribution Lists** tab in the right pane.
3. Locate the distribution list(s) that you want to remove by performing a search. For more information, see Locating entities in Central Management.
4. Select one or more distribution lists.
5. Click .
6. Click **Delete** to delete the selected distribution lists.
   A confirmation message confirms the operation and the select distribution lists are removed from the list.

Import distribution lists

You can import multiple distribution lists using a .csv file. The columns in your .csv files should correspond to the distribution list data fields in the BlackBerry Workspaces administration console (distribution list name, member names).

You can add new users to a distribution list and add or update user data by importing updated .csv files. However, you cannot remove distribution lists from BlackBerry Workspaces by deleting them in the .csv file and then reimporting it. You can delete distribution lists in the BlackBerry Workspaces administration console only.

1. In the left pane, click **Central Management**.
2. Select the **Distribution Lists** tab in the right pane.
3. Click .
   The Import Distribution List window opens.
4. If you have already created a .csv file that contains the new distribution list data, click **Select file** to browse to the .csv file and select that file.
5. If you would like to create a .csv file with the new distribution list data, click **Get template** to download a convenient .csv file with the column headings defined and the table rows blank.
6. Enter the user data in the appropriate columns, including the following information:
   - **Distribution list name**: The name of the distribution list.
   - **Distribution list members**: List of all members of this distribution list. Individual users who are members of the list are identified by their email address. List members should appear one per line. Distribution lists may also be nested within other distribution lists. In this case, the distribution list is identified by name
7. Click **Import** to import distribution list data from the .csv file.

Export distribution lists

You can export a list of distribution lists in your organization. If necessary, you can use filters and export only the displayed list or lists.

1. In the left pane, click **Central Management**.
2. Select the **Distribution Lists** tab in the right pane.
3. Click . The distribution list table is downloaded as a .csv file.

Managing permissions

On the **Central Management** > **Permissions** tab, you can manage permissions for workspace members.

Note: You can access the **Permissions** tab only if you filter **Central Management**. For more information, see Locate entities in Central Management.

Edit permission sets

1. In the left pane, click **Central Management**.
2. Filter the **Central Management** pane to show the desired entities. For more information, see Locate entities in Central Management.
3. Access the **Permissions** tab.
4. Select the permissions set that you want to edit.
5. Click ✎.
6. If you are editing a group, edit the **Name** and **Description** as desired.
7. Set the **Role**, **Permissions**, **File expiration**, **Watermark**, and **Commenting** settings as desired.
8. Click **Apply**.
   A confirmation message appears.
9. Click **Change permissions**.

Manage permissions

Add or remove members for existing permission sets.

1. In the left pane, click **Central Management**.
2. Filter the **Central Management** pane to show the desired entities. For more information, see Locate entities in Central Management.
3. Access the **Permissions** tab.
4. Select the permissions set that you want to edit.
5. Click 👤.
6. To add members:
   a) Click +
   b) In the **Add members** box, enter the email addresses or distribution lists that you would like to add to the group.
   c) To notify members that users were added, click **Notify members**.
   d) Click **Add**.
   e) Repeat these steps to add more members.
7. To remove users:
   a) Select the user(s) that you want to remove.
   b) Click 🗑. The user is removed from the group.

   Note: Enter the name of a member in the search box to filter the displayed members.
8. Click **Close**.

Send a message to workspace members

1. In the left pane, click **Central Management**.
2. Filter the **Central Management** pane to show the desired entities. For more information, see Locate entities in Central Management.
3. Access the **Permissions** tab.
4. Select the permissions set that you want to message the members of.
5. Click ✉.
6. In the **Subject** box, enter the mail subject.
7. In the **Message** box, enter the message text.

8. Click **Send**.

Generate a members management log

1. In the left pane, click **Central Management**.
2. Filter the **Central Management** pane to show the desired entities. For more information, see Locating entities in Central Management.
3. Access the **Permissions** tab.
4. Select one or more permissions sets, and click .
5. Choose to download the log by **All activities** or by **Date range**.
6. Do one of the following:
   - Click **Download** to download the log.
   - Click **Send by email** to send the log to your email.

   A confirmation message appears.

Delete permission sets

1. In the left pane, click **Central Management**.
2. Filter the **Central Management** pane to show the desired entities. For more information, see Locating entities in Central Management.
3. Access the **Permissions** tab.
4. Select one or more permission sets and click .
   A confirmation message appears.

   Note: You cannot delete "Administrators" groups.
5. Click **Delete**.
   Members with these permission sets no longer have access to files in the workspace. A confirmation message confirms the operation.

Export the permissions table

Export the permissions table. If necessary, use filters and export only the displayed list.

1. In the left pane, click **Central Management**.
2. Filter the **Central Management** pane to show the desired entities. For more information, see Locating entities in Central Management.
3. Access the **Permissions** tab.
4. Click .
   The permissions table is downloaded as a .csv data file.

Managing documents

On the **Central Management** > **Documents** tab, you can manage documents in BlackBerry Workspaces. The document management tab is available only to Super Administrators, and you must filter **Central Management** to view it. For more information, see Locate entities in Central Management.

On the **Documents** tab, you can view a list of all documents in workspaces and search for documents by workspace, user, group, or distribution list. You can also select and download documents, change document permissions, delete documents, or export a list of documents.

Download documents

1. In the left pane, click **Central Management**.
2. Filter the **Central Management** pane to show the desired entities. For more information, see Locate entities in Central Management.
3. Access the **Documents** tab.
4. Select one or more documents in the list.

   Tip: Locate the document that you want to download by performing a search. For more information, see Locate entities in Central Management.
5. Do one of the following:

   - To download the file with full access, click .
   - To download the file as a BlackBerry Workspaces protected file, click .

   The file is downloaded.

Edit document permissions

1. In the left pane, click **Central Management**.
2. Filter the **Central Management** pane to show the desired entities. For more information, see Locating entities in Central Management.
3. Access the **Documents** tab.
4. Select one or more documents. If necessary, perform a search to locate a document. For more information, see Locate entities in Central Management.
5. Click .
6. Select the group that you want to edit permissions for. Click **Next**.
7. Edit the group **Name** and **Description** if desired.
8. Set the group **Role**, **Permissions**, **File expiration**, and **Watermark** settings as desired.

   Note: To revoke permissions, Set the **Permission** setting to **No access**.
9. Click **Apply**.
   A confirmation message appears.
10. Click **Change permissions**.
    Your changes are saved and a message is sent to inform all group members.

Add a group to a file

1. In the **Admin Categories** > **Management** list, click **Central Management**.
2. Filter the **Central Management** pane to show the desired entities. For more information, see Locate entities in Central Management.
3. Select the **Documents** tab.
4. Select one or more documents. If necessary, perform a search to locate a document.
5. Click .
6. Follow steps 4-11 in Add a group or user.

Delete documents

1. In the **Admin Categories** > **Management** list, click **Central Management**.
2. Select the **Documents** tab in the right pane.

3. Locate the document that you want to edit permissions for by performing a search. For more information, see Locating entities in Central Management.
4. Select one or more documents.
5. Click 🗑.
6. In the **Note to recipients** box, enter a message that will be shown to any user who tries to access the selected documents after they are deleted.

Export a list of documents

Export a list of documents uploaded by the user. If necessary, use filters and export only the displayed list.

1. In the **Admin Categories** > **Management** list, click **Central Management**.
2. Select the **Documents** tab in the right pane.
3. Click ➡.
   A browse window opens.
4. Browse to the appropriate folder and enter the export file name.
5. Click **OK** to create a .csv file containing information for all documents in the list.
   The document table that is displayed in the **Documents** tab is downloaded as a .csv file.

Provisioning users and devices

You can provisions roles by email domain and Microsoft Active Directory group. You can also manage blocked users and BlackBerry Workspaces apps on devices.

Provisioning roles by email domain

Create and modify domain roles, and specify a user role for a workspace for all users with a specific email domain (for example **@example.com**).

Add domain roles

1. In the left pane, click **Roles by Email Domain**.
2. Click +.
3. In the **Email Domain** box, enter the domain name.
4. In the **Roles** area, select the role(s) for users in the domain:
   - **Visitor**
   - **Workspace Owner**
   - **Sender**
   - **MyDox workspace owner**
5. In the **If there are existing Users of the same email domain** area, set whether the selected roles replace or are added to existing roles held by users in the domain:
   - **Replace their roles with the selected options**
   - **Add the selected roles to their existing roles**
6. Click **Add**.

Edit domain roles

1. In the left pane, click **Roles by Email Domain**.
2. Select a domain from the list.
3. Click ✎.
4. In the **Roles** area, select the role(s) for users of this domain:
   - **Visitor**
   - **Workspace Owner**
   - **Sender**
   - **MyDox workspace owner**
5. In the **If there are existing Users of the same email domain** area, set whether the selected roles replace or are added to existing roles held by users in the domain:
   - **Replace their roles with the selected options**
   - **Add the selected roles to their existing roles**
6. Click **Save**.

Delete email domains

1. In the left pane, under **Provisioning Users and Applications**, click **Roles by Email Domain**.
2. Select a domain from the list.

3. Click 🗑.
4. Select whether to remove all existing roles for users (except for Visitor role), or leave existing roles for the domain.
   - **Remove all roles except for Visitor**
   - **Do not remove their existing roles**
5. Click **Delete**.

Provisioning roles using Active Directory

You can assign BlackBerry Workspaces roles to users that belong to Microsoft Active Directory groups.

Working with Microsoft Active Directory

Active Directory and BlackBerry Workspaces

BlackBerry Workspaces workspace owners and administrators can define groups based on Active Directory Security groups. BlackBerry Workspaces maintains an association between the BlackBerry Workspaces group and the Active Directory group.

Workspace owners can share workspaces with BlackBerry Workspaces groups, in the same way they share workspaces with Workspaces groups. Permissions can be assigned to these groups in the same way they are assigned to Workspaces groups.

When an Active Directory user attempts to access the Workspaces server, to access a workspace for example, Workspaces queries the Active Directory server for all the Active Directory groups the user is a member of, then checks whether any of these (Active Directory) groups are associated with Workspaces groups that permit the access that the user is attempting. If one is found, access is permitted. The user will see, for example, only those workspaces or folders that can be seen by the Workspaces groups associated with Active Directory Security groups for which the user is a member.

To improve performance, BlackBerry Workspaces caches the query response from Active Directory for a particular user for one hour, so subsequent queries will check the cache first. If the information is no longer in the cache, the query will go to the Active Directory server.

Metadata about Active Directory groups, such as name and description, is updated on the associated BlackBerry Workspaces groups once per day.

Active Directory and sharing with BlackBerry Workspaces

BlackBerry Workspaces Exchange users can send emails with secured attachments to Active Directory Distribution Groups. They cannot send to Active Directory Security groups or to the Active Directory Domain Group (of all users). Permissions for recipients of emails to access the secure attachments are those that are explicitly set in the email or the default permissions for sending emails (for the sender). BlackBerry Workspaces uses Active Directory, in essence, as an address book to obtain the email addresses of all members of the Active Directory Distribution Group.

Configure an Active Directory connection

If the BlackBerry Workspaces server will be working with a Microsoft Active Directory server on your organization’s network, you must set parameters for the connection between these servers.

Note:

For appliance customers, using a valid signed certificate for Active Directory FQDN is recommended. If you are using a self-signed certificate, contact support for help to manually importing the root and intermediate certificates to the server.

For cloud customers that connect to a local Active Directory server, a valid signed certificate must be used.

1. In the left pane, click **Roles by Active Directory**.
2. Do one of the following:
   - If this is the first time you are configuring an Active Directory connection in your organization, proceed to step 3.
   - If you already have a configured connection, click ⚙ > +.
3. Select **Enable provisioning of Active Directory Users and Groups**, and set the following:
   - **Expose Active Directory Users with the following email domains**: set names of domains of users who will be able to query the Active Directory.
   - **Active Directory Server Addresses**: set up to three IP address(es) of the DNS server of the Active Directory domain.
   - **Port**: set the port of the Active Directory server. Default value is 389, the LDAP port.
   - **Base DN**: set the base Distinguished Name in the Active Directory tree that will be exposed to the Workspaces server (for example, if only part of the Active Directory tree will be accessible to the Workspaces server).
   - **Username to connect to Active Directory**: set the username in the Active Directory by which the Workspaces server can connect.
   - **Password to connect to Active Directory**: set the password for the above user.
   - **This is a global catalog server**: set the server as a global catalog server. When enabling this option, make sure that the server port is set to match that of the global catalog port (**3268** by default).
4. Click **Apply** to test the parameters against the server to verify them.
5. Repeat the above steps for all connections. There can be multiple connections to the same Active Directory server, but each connection must connect to different parts of the tree. There can also be connections to multiple Active Directory servers.
6. To verify a connection, click **Verify**.
7. To remove a connection, click **Delete**.

Add Active Directory roles

Before you begin: You must have a connection configured.

1. In the left pane, click **Roles by Active Directory**.
2. Click +.
3. In the **Active Directory** box, enter the name of the Active Directory group to which to assign the roles (the autocomplete feature suggests names).
4. In the **Users' Roles** area, select all the roles that you want to assign to the group.
5. Click **Add**.

Edit Active Directory roles

1. In the left pane, click **Roles by Active Directory**.
2. Select a Microsoft Active Directory group from the list.
3. Click ✎.
4. Select or clear the roles, as desired.
5. Click **Save**.

Delete roles from an Active Directory group

1. In the left pane, click **Roles by Active Directory**.
2. Select an Active Directory group from the list.
3. Click 🗑.
4. Click **Delete** to remove all roles associated with this Microsoft Active Directory group. This operation cannot be reversed.

Managing blocked users

You can create and manage a list of email addresses that are denied access to your organization's BlackBerry Workspaces account.

Block an email address or Active Directory group

1. In the left pane, click **Blocked users**.
2. Click +.
3. Do one of the following:
   - To block and email address: In the **Users** box, enter the full email address of the user that you want to block.
   - To block an Microsoft Active Directory group: In the **Active Directories** box, enter the name of the Active Directory group that you want to block.
4. Click **Save**.
   The email address or Active Directory group is added to the blocked users list. The user or members of the Active Directory group will not be able to sign in to your organization, and will not have access to any files protected by BlackBerry Workspaces in your organization.

Remove users from the blocked users list

1. In the left pane, click **Blocked Users**.
2. Select the email addresses or Microsoft Active Directory groups that you want to remove from the list of blocked users.
3. Click 🗑.
4. Click **Delete**.
   The email is removed from the blocked users list.

Search for blocked users

Search for users to check if they are in the blocked users list.

Note: Searching for blacklisted Active Directory groups is not available.

1. In the left pane, click **Blocked Users**.
2. In the search box, begin entering the user email.
   The autocomplete feature suggests matching emails.
3. Select the desired email address.
   The blocked users list is filtered to show only the requested email.
4. Clear the **Enter user's email** box to return to the full list of blocked users.

Import a list of blocked users

1. In the left pane, click **Blocked Users**.
2. Click .
   The Import blocked users list window opens.
3. If you have already created a .csv file that contains the list of blocked users, click **Select file** to browse to the .csv file and select that file.
4. If you would like to create a .csv file with the new distribution list data, click **Get template** to download a convenient .csv file with the column headings defined and the table rows blank.
5. Enter the user data in the appropriate columns, including the following information:
   - **Permitted Entity Address**: Full email address or Microsoft Active Directory group UUID
   - **Permitted Entity Type**: email or Microsoft Active Directory group
6. Click **Import**.
   The blocked users list data is imported from the .csv file and the email addresses are added to the blocked users list.

Export the list of blocked users

1. In the left pane, click **Blocked Users**.
2. Click .
   The Blocked Users table is download as a .csv data file.

Managing BlackBerry Workspaces apps

You can manage BlackBerry Workspaces apps for users in the organization, list all devices registered to a specific user, and disable and re-instate use of the BlackBerry Workspaces app for a user on a particular device.

If a user reports a lost mobile device, you can identify that specific device (based on the user's identifying email address, device type, and last activity date) and wipe all Workspaces-controlled files cached on that device and disable the device for document access. Wiping files off the mobile device is conducted the next time that device connects to the Workspaces service.

When working with a Windows or a Mac computer, a disable request simply signs the user out of the session that is currently active on that computer. This is useful, for example, if a user forgot to sign out of BlackBerry Workspaces on a computer to which the user no longer has access. If the user downloaded Workspaces-controlled files to that computer, the files are not wiped clean; however, there is no way to open or access those files until an authorized user signs in on that computer.

By default, each BlackBerry Workspaces app on a user's mobile device or computer must connect to the Workspaces service at least once every 72 hours in order to stay registered and maintain access permissions; otherwise the user is not able to open any controlled files cached on that device until they reconnect and sign back in.

Manage BlackBerry Workspaces apps

1. In the left pane, click **Manage applications**.
2. In the search box, enter the email address of the user you want to manage BlackBerry Workspaces apps for.
   The autocomplete feature offers matching results.
3. Select the desired user.
   A list of all the devices used by that user to access BlackBerry Workspaces is displayed. The following information is included:

- **Device Id**: Unique identifier of device used.
- **Type**: Type of device used to access BlackBerry Workspaces, for example, iPad, iPhone, BlackBerry, Windows, or Mac.
- **Status**: Whether the device is enabled or disabled.
- **Last Document Activity**: Last activity performed in BlackBerry Workspaces, for example "Opened file".
- **Last Location**: Last location the device registered.
- **Last IP**: Last IP address the device registered.
- **Last Activity Date**: Latest date the user was active in BlackBerry Workspaces on the device.

Disable BlackBerry Workspaces apps

1. In the left pane, click **Manage applications**.
2. In the search box, enter the email address of the user you want to disable BlackBerry Workspaces apps for. The autocomplete feature offers matching results.
3. Select the desired user.
4. Select one or more devices from the list.
5. Click .
   A confirmation message appears.
6. Click **Disable**.

Enable devices

1. In the left pane, click **Manage applications**.
2. In the search box, enter the email address of the user you want to enable BlackBerry Workspaces apps for. The autocomplete feature offers matching results.
3. Select the desired user.
4. Select one or more disabled devices from the list.
5. Click .
   A confirmation message appears.
6. Click **Enable**.

Export a list of user apps

1. In the left pane, click **Manage applications**.
2. In the search box, enter the email address of the user you want to manage BlackBerry Workspaces apps for. The autocomplete feature offers matching results.
3. Select the desired user.
4. Click .
   The Manage Applications table is downloaded as a .csv file.

Configuring integrations

Manage connectors to external repositories and other services in the **Integrations** area.

Connectors

The following table describes where to configure your connectors:

Repository:	Connector:	Configure in:
Microsoft OneDrive for Business	Unified Content Connector	**Integrations** > **Content Connectors**
Microsoft SharePoint	Unified Content Connector	**Integrations** > **Content Connectors**
SharePoint Online	Unified Content Connector	**Integrations** > **Content Connectors**
Alfresco	Dedicated connector	**Integrations** > **Content Connectors**
Windows File Share (CIFS)	Unified Content Connector (BEMS)	**Integrations** > **Content Connectors** **Note:** This option is for organizations configuring a new Windows File Share with the BlackBerry Workspaces Unified Content Connector.
Windows File Share	Dedicated connector	**Integrations** > **Windows File Share Connector** **Note:** This option is for organizations to manage an existing Windows File Share configuration.
Dropbox for Business	Unified Content Connector	**Integrations > Content Connectors**
iManage	Unified Content Connector	**Integrations > Content Connectors**
iManage Cloud	Unified Content Connector	**Integrations > Content Connectors**

Managing content connectors

You can add and manage existing content connectors, verify the connection, and delete content connectors.

Add a content connector

1. In the left pane, click **Content Connectors**.
2. Click +.
3. In the **Repository Type** list, select the type of connector that you want to configure.
4. In the **Connector display name** box, enter a name for the connector.

5. In the **Allowed path** box, enter the root path of the repository.
   - If you selected **Alfresco**, the allowed path should match the CMIS service URL. For example:

     ```
     http://<server ip or FQDN>:8080/alfresco/api/-default-/public/cmis/
     versions/1.1/atom/
     ```

     You can add a relative path to the end of the service URL; however, **do not** use the Alfresco site or shared files location in the allowed path. Refer to the Alfresco documentation (https://community.alfresco.com/docs/DOC-5527-cmis#w_cmisserviceurl), section 3.1, **CMIS Service URL** for more details.

     Note: If the Alfresco connector URL changes when upgrading the Alfresco server, the connector and all associated workspaces will need to be recreated.
   - If you selected **OneDrive for Business**, the allowed path should match the root FQDN of the OneDrive site.
   - If you selected **SharePoint** or **SharePoint Online**, the allowed path can be either a site URL or a document library path.
6. If you selected **SharePoint** or **Windows File Share** and are working with KCD, select **Enable KCD**.
7. In the **Provide access to** area, select one of the following:
   - **All organization**: All workspace owners (users that are assigned the **Workspace owner** role) in the organization can access this repository.
   - **An individual user**: Only users that are assigned the **Individual connector workspace owner** role can access this repository.
8. In the **UCC credentials** area:
   - If your organization is working with Appliance-X, the BEMS credentials are auto-populated and need not be changed.
   - If your organization is working with vApp or has a Cloud service (i.e., manual installation), for **Alfresco**, **SharePoint** and **Windows File Share** connectors, click **Edit** to enter the required BEMS **URL**, **Username**, and **Password**.
9. Click **Add**.

Edit a content connector

1. In the left pane, click **Content Connectors**.
2. Click the name of the connector that you want to edit.
3. Update the connector details, as desired.
4. Click **Apply changes**.

Verify a content connector

Verify the connection with the external repository.

1. In the left pane, click **Content Connectors**.
2. Click the name of the connector that you want to verify.
3. Click **Verify**.
   The connection is verified.

Delete a content connector

1. In the left pane, click **Content Connectors**.
2. Click the name of the connector that you want to delete.
3. Click **Delete**.

Managing SharePoint protectors

If using a dedicated connector and SharePoint protector, manage the protector in the administration console to assign workspace administrators and define which Microsoft SharePoint libraries are synced in BlackBerry Workspaces.

Define default workspace administrators

Define users as default workspace administrators so that they automatically become workspace administrators for Microsoft SharePoint libraries that you add to the list of synced libraries.

Note: You must be a BlackBerry Workspaces administrator to share a SharePoint workspace with external parties.

1. In the left pane, click **SharePoint Protector**.
2. In the **Default Workspace Administrators** area, click +.
3. In the **Add members** box, enter the email addresses or distribution lists for the desired users, and click **Add**.

   Note: When you add default workspace administrators, the defined users become workspace administrators only to libraries that you later add to the **Synced libraries** list. To define administrators for existing synced libraries, add the user in the workspace **Groups** tab.

Manage the internal users whitelist

Manage the internal users whitelist to define users that always have full access permissions, notably including the ability to download original versions. This option is only available for organizations with a defined Microsoft SharePoint Protector.

1. In the left pane, click **SharePoint Protector**.
2. In the **Internal users whitelist** area, click +.
3. In the **Add members** area, enter the email addresses or distribution lists for the desired users, and click **Add**. All users that are on the whitelist are able to access any file in SharePoint with full access, regardless of the defined permission template.

   Note: The user defined in the SharePoint connector configuration (see Add a SharePoint protector) is added to the whitelist by default; this username is not shown in the whitelist here.

Add a SharePoint protector

1. In the left pane, click **SharePoint Protector**.
2. Next to the **Choose connector** area, click +.
3. Enter the following BlackBerry Workspaces iApp credentials:
   - **Username** – Enter the username of your organization administrator.
   - **Password** – Enter the password of your organization administrator.
4. Enter the following **Proxy machine details**:
   - **Connector display name** – Provide a name for this connector.
   - **SharePoint version** – Select the SharePoint version.
   - **Connector URL** – Provide the URL of the BlackBerry Workspaces SharePoint connector web-service.
   - **Use SharePoint permissions** – Use constraint delegation (impersonation) to copy group access rights from SharePoint to BlackBerry Workspaces. (Not available with SharePoint version 1 or SharePoint online).
5. Enter the following **SharePoint credentials**:
   - **SharePoint URLs** – enter the address(es) of the SharePoint site collections that you want to sync with.

- **Domain** – enter the domain of the SharePoint username and password. (Not available SharePoint online)
- **Username** – Enter the username of your SharePoint Site Collection administrator.
- **Password** – Enter the password of your SharePoint Site Collection administrator.

Note: To connect to multiple SharePoint sites, make sure that you provide credentials for a SharePoint Site Collection administrator that has access to all the given SharePoint URLs.

6. Click **Apply changes**.
7. Repeat steps 2-5 for each connector that you want to add.
8. Click **Close** to close the **Add New Connector** pane.

Edit a SharePoint protector

1. In the left pane, click **SharePoint protector**.
2. In the **Choose connector** area, choose a connector from the drop-down list.
3. Click ✎.
4. Edit the following BlackBerry Workspaces credentials, as desired:
   - **Username** – Enter the username of your organization administrator.
   - **Password** – Enter the password of your organization administrator.
5. Edit the following **Proxy machine details**, as desired:
   - **Connector display name** – Provide a name for this connector.
   - **SharePoint version** – Select the SharePoint version.
   - **Connector URL** – Provide the URL of the BlackBerry Workspaces SharePoint connector web-service.
   - **Use SharePoint permissions** – Use constraint delegation (impersonation) to copy group access rights from SharePoint to BlackBerry Workspaces. (Not available with SharePoint version 1 or SharePoint online).
6. Edit the following **SharePoint credentials**, as desired:
   - **SharePoint URLs** – enter the address(es) of the SharePoint site collections that you want to sync with.
   - **Domain** – enter the domain of the SharePoint username and password. (Not available for SharePoint online)
   - **Username** – Enter the username of your SharePoint Site Collection administrator.
   - **Password** – Enter the password of your SharePoint Site Collection administrator.

   Note: To connect to multiple SharePoint sites, make sure that you provide credentials for a SharePoint Site Collection administrator that has access to all the given SharePoint URLs.
7. Click **Apply changes**.
8. Click **Close** to close the **Edit Configuration** pane.

Define libraries to sync

Set which SharePoint libraries are synced with BlackBerry Workspaces.

1. In the left pane, click **SharePoint Protector**.
2. If your organization has defined more than one SharePoint protector, in the **Choose connector** list, select the desired SharePoint protector.
3. In the **Choose SharePoint URL** list, select the URL for the relevant SharePoint site.
   The synced libraries list appears.
4. To add a library, in the **Add libraries** area, click +.
5. Select the desired library(ies) and click **Add**.

The libraries are synced and added to the synced libraries list. Default BlackBerry Workspaces workspace administrators can now access the SharePoint libraries through BlackBerry Workspaces, and assign user groups to access the workspace.

6. If your organization is defined with the associated plans in the BlackBerry Workspaces Configuration Tool, configure internal protection per library:
   a. Click the **Internal protection** checkbox.
   b. In the **Permission template** area, select the desired permission template from the drop-down list.
   c. In the **Apply to** area, select one of the following:
      - **All files** to apply the selected permissions to users accessing any file in the SharePoint library
      - **Based on ICAP** to have BlackBerry Workspaces check the ICAP permissions per access and to enable the user full access permissions when in compliance with the ICAP policy. If the policy does not allow full access permissions, the user has access based on the library permission template as set here.
7. Repeat this task to sync libraries for different SharePoint URLs.

Remove synced libraries

1. In the left pane, click **SharePoint Protector**.
2. If your organization has defined more than one SharePoint protector, in the **Choose connector** list, select the desired SharePoint protector.
3. In the synced libraries list, click **x** next to the library that you want to remove from sync.
   The library is no longer synced.

Managing Windows File Share connectors

You can add, configure, and manage your organization's Windows File Share workspaces using the Windows File Share connector.

Define default workspace administrators

1. In the left pane, click **Windows File Share**.
2. In the **Default Workspace Administrators** area, click +.
3. In the **Add members** box, enter the email addresses or distribution lists for the desired users, and click **Add**.
4. Click **Add**.
   The users are added as workspace administrators for all defined network drives.

Add a Windows File Share connector

1. In the left pane, click **Windows File Share**.
2. Next to the **Choose connector** area, click +
3. Enter the following organization credentials:
   - **Username** – Enter the username of your organization administrator.
   - **Password** – Enter the password of your organization administrator.
4. Enter the following **Proxy machine details**:
   - **Connector display name** – Provide a name for this connector.
   - **Connector version** – Select the connector version.
   - **Connector URL** – Provide the URL of the Windows File Share connector web-service.
5. Click **Apply changes**.

Edit a Windows File Share connector

1. In the left pane, click **Windows File Share**.
2. Next to the **Choose connector** area, click ✎
3. Click **Edit** to edit the following organization credentials, as desired:
   - **Username** – Enter the username of your organization administrator.
   - **Password** – Enter the password of your organization administrator.
4. Edit the following **Proxy machine details**, as desired:
   - **Connector display name** – Provide a name for this connector.
   - **Connector version** – Select the connector version.
   - **Connector URL** – Provide the URL of the Windows File Share connector web-service.
5. Click **Apply changes**.

Define network drives to sync

1. In the left pane, click **Windows File Share connector**.
2. If your organization has defined more than one Windows File Share connector, in the **Choose connector** list, select the desired Windows File Share connector.
3. To add a network drive, in the **Add libraries** area, click +.
4. Select the desired network drives and click **Add**.
5. Click **Apply**.
   The drive is added to the synced network drives list.

Remove synced network drives

1. In the left pane, click **Windows File Share connector**.
2. If your organization has defined more than one Windows File Share connector, in the **Choose connector** list, select the desired Windows File Share connector.
3. In the synced network drives list, click **x** next to the network drive that you want to remove from sync.
   The network drive is no longer synced.

Managing the Workspaces Email Protector

You can enable the Workspaces Email Protector, define default permissions, set whitelists, and define protected file types.

Enable the BlackBerry Workspaces Email Protector

1. In the BlackBerry Workspaces administration console, in the left pane, click **Email Protector**.
2. Click **Enable email protector**.
3. In the **File extensions to protect** area, to create a list of file types that you want to protect, do one of the following:

Action	Task
To protect all file types	• Click **Protect all file types**.

Action	Task
To specify the file types that you want to protect	**a.** Click **Select file extensions to protect**. **b.** Select the file types that you want to protect. To add a specific file type to protect, in the **Add specific file types to be controlled by the Email Protector** field, type the file extension and press the return key.

4. In the **Set default permissions** area, set the default **Permissions**, **File expiration**, and **Watermark** settings as desired.
5. In the **User whitelist** area, enter the email addresses or distribution lists of users that are able to open files shared using the email protector with full access permissions.
6. In the **Email domain whitelist** area, enter the email domain of users that are able to open files shared using the email protector with full access permissions.
7. In the **Notify senders** area, select **Notify senders when files are controlled by the email protector**, if desired.
8. Click **Apply changes**.

Remove the email protector

1. In the left pane, click **Email Protector**.
2. Clear the **Enable email protector** checkbox.
3. Click **Apply changes**.

Enable Office Online integration

Enable Office Online to allow users to edit files using Office Online. Your organization must be a Microsoft Volume License customer.

1. In the left pane, click **Office Online**.
2. Select **Enable Office Online integration**.
3. Click **Apply changes**.

About Office Online configuration

Office Online integration enables organization users to view and edit documents using Office Online.

Editing using Office Online is available when the following conditions are met:

- Your organization must be a Microsoft Volume License customer.
- Office Online has been configured for your organization. Contact BlackBerry Support for help configuring Office Online to work with BlackBerry Workspaces.
- Office Online is enabled in the administration console.
- The file is from OOXML format (.docx, .pptx, .xlsx).
- The user has been granted copy-paste capabilities via BlackBerry Workspaces for the file.
- The file has not been restricted to "Spotlight" mode via BlackBerry Workspaces.
- If working on a file in a workspace, the user must have been granted the capability to update all documents in the parent folder.
- If working on a received file, the user must be the file owner, or the file must have been shared in collaboration mode.

Managing the DocuSign integration

You can enable DocuSign in BlackBerry Workspaces.

Enable DocuSign in BlackBerry Workspaces

Before you begin: Verify that your organization is a DocuSign API account customer.

1. In the left pane, click **DocuSign**.
2. Select **Enable DocuSign integration**.
3. Enter your organization's DocuSign Account Administrator **Username** and **Password**.
4. Click **Apply**.

About DocuSign Integration

DocuSign integration enables organization users to send documents using BlackBerry Workspaces for DocuSign signing and other workflows.

Users can send documents using BlackBerry Workspaces with DocuSign if the following conditions are met:

- DocuSign has been configured for your organization's BlackBerry Workspaces users.
- DocuSign is enabled in the BlackBerry Workspaces admin console. See Enable DocuSign in BlackBerry Workspaces .
- Users must have upload and send capabilities for the file as defined in their BlackBerry Workspaces permissions and access.

To receive DocuSign requests, users do not require BlackBerry Workspaces or DocuSign licenses.

Managing the Dropbox connector

BlackBerry Workspaces supports a connection to Dropbox repositories so that users can access files in those repositories from the Workspaces interface.

Create a Dropbox app for accessing a Dropbox repository

BlackBerry Workspaces on-premise customers must create a Dropbox app before they can access their organization’s Dropbox repository.

1. Go to the Dropbox developer site.
2. Click **Create Apps**.
3. In the Choose an API section, click **Dropbox API**.
4. In the Choose the type of access you need, click **Full Dropbox– Access to all files and folders in a user's Dropbox**.
5. Name your app. For example, Workspaces app.
6. Select the **I agree to Dropbox API Terms and Conditions** checkbox.
7. Click **Create app**.
8. In the Redirect URIs field, enter https://<FQDN>/ngdox/dropbox_auth_finish, where FQDN is the FQDN of your organization’s Workspaces server.
9. Click Add.

After you finish:

- After you have created the app, contact BlackBerry Support for help configuring BlackBerry Workspaces to connect to your organization's Dropbox repository.

Add a Dropbox connector

When you add a Dropbox connector, users that have the appropriate permissions can access the Dropbox repository from BlackBerry Workspaces. To add a connector for a Dropbox repository:

1. In the BlackBerry Workspaces Admin Console, click **Content Connectors**.
2. Click +.
3. In the **Repository Type** dropdown menu, select **Dropbox**.
4. In the **Connector Display Name** field, enter a name.
5. In the **Allowed Path** field, enter the path to the Dropbox repository, such as https://www.dropbox.com.
6. In the **Provide access to** field, select one of the following:
   - **All organization**: All workspace owners (users that are assigned the **Workspace owner** role) in the organization can access this repository.
   - **Individual user**: Only users that are assigned the **Individual connector workspace owner** role can access this repository.
7. Click **Add**.

Note that if your organization is blocking access to Dropbox, you must allow the OAuth authenticattion page through your firewall to allow users to login. All other operations through Dropbox are completed through a server to server integration. The path that must be allowed is: https://www.dropbox.com/oauth2/ and any other URL with this prefix.

Managing the iManage connector

BlackBerry Workspaces supports a connection to iManage and iManage Cloud repositories so you can access files in those repositories from the BlackBerry Workspaces interface. iManage is the leading provider of work product management solutions for law firms, corporate legal departments, and other professional services firms such as accounting and financial services.

The BlackBerry Workspaces connector provides Workspace access to iManage matters (i.e. root folders), folders, and files.

iManage integration requires an additional license to be purchased, contact your account manager for more details.

The iManage connector requires the iManage Connector tier in the BlackBerry Workspaces configuration. Contact your account manager for more information..

Note: BlackBerry Workspaces supports iManage Work 10 and later.

Add an iManage connector

1. In the BlackBerry Workspaces Admin Console, click **Content Connectors**.
2. Click +.
3. In the **Repository Type** drop-down list, select **iManage**.
4. In the **Connector Display Name** field, enter a name.
5. In the **Allowed Path** field, enter the path to the iManage matter.

6. In the **Provide access to** field, select one of the following:
   - **All organization**: All workspace owners (users that are assigned the **Workspace owner** role) in the organization can access this repository.
   - **Individual user**: Only users that are assigned the **Individual connector workspace owner** role can access this repository.
7. In the **URL** field, enter the URL of your iManage repository.
8. In the **Username** and **Password** fields, enter your iManage credentials.
9. Click **Add**.

Add an iManage Cloud connector

1. In the BlackBerry Workspaces administrator console, click **Content Connectors**.
2. Click +.
3. In the **Repository Type** drop-down list, select **iManage Cloud**.
4. In the **Connector Display Name** field, enter a name.
5. In the **Allowed Path** field, enter the path to the iManage matter.
6. In the **Provide access to** field, select one of the following:
   - **All organization**: All workspace owners (users that are assigned the **Workspace owner** role) in the organization can access this repository.
   - **Individual user**: Only users that are assigned the **Individual connector workspace owner** role can access this repository.
7. Click **Add**.

Workspaces Connector for BEMS

A new connector for BEMS has been developed to allow the BlackBerry Work Docs app to access BlackBerry Workspaces repositories. Workspaces repositories are exposed in the Docs app, allowing the user to see Workspaces locations as a place to Save documents. A user can also see Workspaces files when choosing to Open from the Docs app. The connector is able to:

- List, create, and delete workspaces and folders
- List, upload, download, and delete files

For example, a manager receives a sensitive document as an attachment in the Work email app. The manager can tap to download the attachment, then **Save to Docs** and choose a Workspaces location to save the file. From the Docs app, the manager can later retrieve the file from the Workspaces location.

Note: Only local workspaces can be accessed, not transient workspaces.

Note: If you are upgrading BEMS, you must redeploy the Workspaces Connector after the upgrade.

The minimum requirements for the Workspaces Connector for BEMS are:

- BlackBerry Enterprise Mobility Server (BEMS) 2.8.7 and above
- BlackBerry Workspaces Server 6.0.0 and above

To configure and deploy the Workspaces Connector for BEMS:

1. Create an OAuth Client ID and details for the organization.

   You must be a Workspaces administrator and have access to Workspaces Rotisserie to perform this step. For some Workspaces clients, this step will need to be performed by BlackBerry Support.

a) Log in to Workspaces Rotisserie at *https://<workspaces server>/rotisserie*, using a Workspaces admin email and password.
b) Select the **Identity Provider Manager** tab (key icon at upper right).
c) Select the **OAuth Client Details** tab.
d) Click **Create** to create a new OAuth client.
e) In the **Client Id** field, enter a client id. (e.g., *servername.bems*)
f) Click the key icon to the right of the **Client Secret** field to generate a key.
g) Leave the default values as is in the **Authorities**, **Authorized Grant Types**, and **Access Token Validity** fields.
h) In the **Webserver Redirect URI** field, enter the Workspaces FQDN.

   This field is required for the BEMS Docs App to work properly.
i) Click **Create OAuth Client**.

2. Install the Workspaces Connector for BEMS.

a) BlackBerry will provide a custom .jar (Java ARchive) file to the client, based on the Client ID configuration in the previous step.
b) Copy the .jar file to the following BEMS server location:

```
C:\Program Files\BlackBerry\BlackBerry Enterprise Mobility Server\Good Server
Distribution\gems-quickstart-x.x.x\deploy
```

   Note: The location may be different depending on your BEMS installation.
c) If the connector jar is deployed successfully then the **Workspaces** type will appear under the Storage Provider dropdown in BEMS.

3. Add a new Workspaces connector in the BEMS dashboard.

You must be a BEMS administrator to complete the following.

a) Log in to BEMS dashboard at *https://<bems_server>:8443/dashboard*.
b) Create a new Storage by selecting **Home** > **Docs** > **Storages** > **New Storage**.
c) Enter a name for the storage (e.g., Workspaces).
d) Select **Workspaces** from the **Storage Provider** drop down.
e) Select **OAuth2** from the **Authentication Provider** drop down. The OAuth2 Base URL format depends on the user's authentication method. The Client ID and Client Secret were defined in the previous steps.
   - If the user uses OAuth2 or EID for authentication: `https://<FQDN server>/saml-idp/oauth`
   - If the user logs in with their email address and password: `https://<FQDN server>/api/3.0/authentication`
f) To make the storage available on user devices, select **Enable Storage**.

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.

4. Add a new Workspaces repository in the BEMS dashboard.

a) Select **Home** > **Docs** > **Repositories** > **New Repository**
b) Add a name in the **Display Name** field (e.g., Workspaces).
c) Select **Workspaces** from the **Storage** drop down.
d) In the **Path** field, enter the path to the Workspace repository.
e) Configure the rest of the form according to the steps documented in Managing Content Connectors
f) Click **Save**.

Once the Workspaces and BEMS configuration are complete, no additional setup is required on the Docs client. The Workspaces connector will be available automatically in the Docs App.

Note:

To upgrade to a new version of the connector:

1. Go to the `/gems-quickstart-x.x.x/deploy` folder and delete the existing connector jar.
2. Copy the new connector jar to the deploy folder.

Setting security policies

Configure service security policies at the organizational level.

Set file policies

1. In the left pane, click **File**.
2. Set the **General settings**:
   a) To allow the upload of any file type (including types not protected by BlackBerry Workspaces) including files uploaded via sharing, in the **Upload files that cannot be protected** section, select **Apply to workspace files** and **Apply to sent files**, as desired.
   b) To enable curtain mode on files uploaded to BlackBerry Workspaces and shared, in the **Enable curtain mode** section, select **Apply to workspace files** and **Apply to sent files**, as desired.
   c) Select **Lock workspace name and description after creation** to allow organization and super administrators only to edit workspaces and to block the ability to delete workspaces after they are created.
   d) To enable file locking in your organization, select **Enable file locking**.
   e) To enable file commenting in your organization, select **Allow all organization members to make comments**. If this option is selected, you can choose to **Allow the content of comments to display in emails**.

      Hiding the content of comments in email notifications is a good security practice, since it prevents sensitive comments from being transmitted over plain text.
3. Set the **Online Access Settings**: enter the number of hours files are available for offline viewing.
4. Set the **Conversion settings**. To delete unopened copies of converted files, select **Delete converted copies of unopened files** and enter the desired number of days after which to delete the files.
5. Set the upload and download restrictions for specific file types:
   a) Select **Allow upload and sync of the following file types only**, and enter the file types that users can upload and sync using the following format: *.file extension (for example, *.exe).
   b) Select **Restrict upload and sync of the following file types only**, and enter the file types that users cannot upload and sync using the following format: *.file extension (for example, *.exe)
   c) Select **Limit upload and sync file size**, and enter the maximum size, in MB.
6. Set the **File Retention** settings:
   a) To move inactive workspaces to the Recycle bin after a certain amount of time, select **Move inactive files to the Recycle bin** in the **Workspaces** area, and enter desired the number of days after which to move the workspace.
   b) To move inactive files from the Sent items to the Recycle bin after a certain amount of time, select **Move inactive files to the Recycle bin** in the **Sent items** area, and enter desired the number of days after which to move the files.
   c) To permanently delete files stored the Recycle bin after a certain amount of time, select **Permanently delete files stored in the Recycle bin** in the **Recycle bin** area, and enter desired the number of days after which to delete the files.
7. To set the **File versions** settings, select one of the following:
   - To limit the number of versions saved for each file, select **Maximum number of versions saved for each file**, and enter the maximum number of file versions.
   - To set the number of versions saved for each file per day, week, and month, select **Number of versions saved daily, weekly and monthly**, and enter the maximum number of file versions for day, week, and month.
8. Set the **File Acknowledgement** settings:

a) Select **Enable read acknowledgement** to have the Require read acknowledgement check box appear when users create new workspaces or send files.
b) Select **Require read acknowledgement by default** to make Require read acknowledgement the default setting.

9. Click **Apply changes**.

Set mobile policies

Set which mobile devices users can access their BlackBerry Workspaces files from. Disable access to prevent users from using the BlackBerry Workspaces apps to access your organization's workspaces. When disabled, the user can log in to BlackBerry Workspaces, but cannot see any of your organization's workspaces.

Note: This setting is available to Organization Administrators only.

1. In the left pane, click **Mobile**.
2. Set the **General settings**:
   a) To enable access to BlackBerry Workspaces from iPhones and iPads, select **Enable access from iPhone and iPad devices**.
   b) To enable access to BlackBerry Workspaces from Android devices, select **Enable access from Android devices**
   c) To enable access to BlackBerry Workspaces from BlackBerry 10 devices, select **Enable access from Blackberry devices**.
   d) To enable access to BlackBerry Workspaces from Windows Mobile devices, select **Enable access from Windows Mobile devices**.
   e) To allow users to open protected files in third party applications on mobile devices, select **Allow users to open protected files (Office, PDF, Images, Text) when shared with Full Access permissions in 3rd party applications on mobile devices**.
   f) To enable users to open file types that cannot be protected in third party applications on mobile devices, select **Allow users to open non-protected files in 3rd party applications on mobile devices**.
   g) To require users to set a passcode when using BlackBerry Workspaces on Android and iOS devices, select **Enable passcode lock in order to open BlackBerry Workspaces for Android and iOS**.
3. Click **Apply changes**.

Set sharing policies

1. In the left pane, select **Security policies > Sharing**.
2. In the **Enable autocomplete** area, to enable the autocomplete feature, select **Enable autocomplete when sharing files**, and choose one of the following:

Only for workspace administrators and users	Select this setting to allow autocomplete for workspace administrators and Exchange senders only.
For all users	Select this setting to enable autocomplete for anyone sharing an organization file, including external users and visitors.

When autocomplete is enabled, potentially all email addresses of all users in the organization can be seen when beginning to enter an email address.

3. In the **Outlook Plugin** area, to offer BlackBerry Workspaces for Windows user the option to send files of over 25 MB, select **Enable sharing of large files via the Outlook plugin**.
4. In the **Workspaces** area, do the following: .
   a) If you want to restrict individual users from changing the default file permissions when sharing or sending files, select **Disallow users from changing default sharing or sending permissions by default**.

      Note: For existing users, you must edit the user account and select the **Disallow user from changing default sharing or sending permissions** setting to apply the restriction. For new users, this setting is applied to the user account by default.
   b) Configure the default permissions that are applied when a user shares a workspace. The default permissions that you can set are: Role, Permission, File expiration, Watermark, and Commenting.
5. In the **Sent files** area:
   a) Select **Enable sharing without email notification** to enable users to decide whether to notify recipients when new files are uploaded. When selected, an additional option appears to select **Share files with notification by default**. This additional option (when selected) ensures that the notification option is selected by default and must be manually turned off by the sender, if desired.
   b) Select **Enable users to share files without requiring recipients to sign in**, if you want to give senders the option to allow recipients to view files without signing in. If you want to require that recipients to sign in by default, select **Require recipients to sign in by default** .
   c) Configure the default permissions for sent files. The permissions that you can set are: Permission, File expiration, Watermark, and Commenting.

      Note: The available permissions depend on which Enterprise mode has been set (see Configure the Enterprise mode). The permissions in the drop-down lists are the permissions templates for the different users. For more information on permissions, see Overview: BlackBerry Workspaces user roles.
6. Click **Apply changes**.

Set sync policies

Restrict the file size and file type that users in the organization can upload.

1. In the left pane, click **Sync**.
2. To set all files synced via the BlackBerry Workspaces for Windows and BlackBerry Workspaces app for Mac, in the **General settings** area, select **Always download files as protected via Workspaces for Windows and Workspaces app for Mac**.
3. To set the upload and download rate:
   a) Select **Limit download rate** and enter the rate limit in MB.
   b) Select **Limit upload rate** and enter the rate limit in MB.
4. Click **Apply changes**.

Bring Your Own Key (BYOK)

Note: This feature is available only for hosted cloud environments.

A cryptographic key is used to encrypt and decrypt a BlackBerry Workspaces organization's files. As of version 7.0, the Bring Your Own Key (BYOK) security policy for public cloud instances of BlackBerry Workspaces allows third party key management solutions to be used instead of BlackBerry provided keys. This allows organizations to:

- Encrypt and decrypt documents from storage using their own key

- Revoke the key if needed

A cloud organization who wishes to use this feature provides its own Amazon Web Services (AWS) Key Management Service (KMS) Key to encrypt organizational files. Decryption requires Workspaces to be integrated as an External Account with access to the AWS KMS Key. Access to both the AWS KMS interface and the Workspaces Admin Console is necessary.

BYOK requires an additional license to be purchased; contact your account manager for more details.

BYOK requires the BYOK tier in the Workspaces configuration. Contact your account manager for more information.

Take the following steps to Bring-Your-Own-Key (BYOK) in a BlackBerry Workspaces cloud environment:

1. Create or retrieve the Master Key from Amazon Web Services (AWS):
   a. Sign into your AWS IAM Account with your Account ID.
   b. At the IAM Home Screen, select the appropriate Region.
   c. Select the **Encryption Keys** link from the left-hand sidebar.
   d. Click the **Create Keys** button.
   e. Type the **Name** of the Key and click the **Next** button.
   f. If desired, add a **Tag** for the Key and click the **Next** button.
   g. Define a **Key Administrator**.
2. Confirm the Key Administrator has the ability to Generate Data Keys:
   a. Sign into the AWS IAM Account and access the **Policies** section from the left-hand sidebar.
   b. Review the JSON of the Policy you intend to use with the Key Administrator.
   c. Confirm that the Policy's JSON includes the line **kms:generateDataKey**.
   d. Access the **Users** section from the left-hand sidebar.
   e. Select the relevant Key Administrator.
   f. Add the relevant Policy that includes the ability to **kms:generateDataKey**.
3. Grant access to the Master Key for the Workspaces organization:
   a. Sign into the AWS IAM Account and access the **Encryption Keys** section from the left-hand sidebar.
   b. Find the **External Accounts** header.
   c. Click the **Add External Account** button.
   d. Add the Workspaces Amazon Account ID as an External Account.
4. Create an AWS KMS Encryption Key to be used for encrypting and decrypting Workspaces organizational files:
   a. Download the Amazon Command Line Interface tool.
   b. Add the AWS EXE to your Operating System's PATH environmental variables. For example, add **C:\Program Files\Amazon\AWSCLI** to the PATH variable.
   c. Run the EXE.
   d. Input **aws configure**.
      1. When prompted, input the AWS Access Key ID. This should be the Master Key Administrator's User Access Key.
      2. When prompted, input the AWS Secret Access Key.
      3. When prompted, input the default region name. For example, us-east-1.
      4. When prompted, input the default output format. For example, json.
   e. Input **aws kms generate-data-key --key-id <key-ARN> --key-spec AES_256**. For example, **aws kms generate-data-key --key-id arn:aws:kms:us-east-1:############:key/########-####-####-####-############ --key-spec AES_256**. **Note**: This value can be located within the **Policy JSON** listed in Step #2 above as the contents of the **Resource** field.

f. The Response JSON will include the following information:

```
{
 "Plaintext" : "aStringOfCharactersWillBeReturned"
 "KeyId": "TheSameKeyIdWilBeReturnedThatWasInput"
 "CiphertextBlob" :
 "aStringOfCharactersToBeEnteredInTheBlackBerryWorkspacesAdminConsoleWithoutTheQuotesAt
}
```

g. Save these encrypted values as they will be used in the BlackBerry Workspaces Admin Console.

5. Add the AWS KMS Encryption Key to the BlackBerry Workspaces Admin Console:
   a. In the BlackBerry Workspaces admin console, click **Security Policies** > **Bring Your Own Key**.
   b. Select an appropriate Amazon Web Services (AWS) region from the dropdown.
   c. In the **Customer Master Encryption Key** field, input the **CiphertextBlob** that was returned in the **generate-data-key Response JSON**.
   d. Click **Activate Key**.

To revoke the key, click **Revoke Key**. Access to all documents uploaded before and after the key was generated will be revoked.

Additional considerations include:

- Files which has been synced with full access permissions will still be available after the revoke
- DocuSign integration fails for files which were uploaded before revoking the BYOK
- Annotation symbols still appear after revoking access for a document with annotations
- Revoking a key in organizations which were created before BlackBerry Workspaces version 5.3 will still allow access to documents uploaded before BYOK configuration
- Text and office 97-2003 and non converted documents will show non-readable characters when opened after revoking the key. PDF documents will not open.

Warning: Revoking a key is a destructive action that you must consider carefully before performing.

Set watermarks as an organizational policy

Enable watermarks per organization.

1. In the left pane, click **Watermarks**.
2. Select one or more options to set the position of the watermark:
   - **Apply a Top Watermark**
   - **Apply a Bottom Watermark**
   - **Apply a Diagonal Watermark**
3. For each watermark, define the watermark:
   - **Font Size**: select **Small**, **Medium**, or **Large**.
   - **Color**: select **Black**, **Gray**, **White**, **Red**, or **Blue**.
   - **Opacity**: select the opacity in increments of 10%.
   - **Line Content**: select **Date and Time**, **Viewer's IP address**, **Viewer's name**, **Text**, or **Viewer's email**.
4. Click **Apply changes** to save the settings.

Watermarks are now set for the organization. By default, watermarks are not shown to users for any documents, unless configured otherwise by workspace administrators, contributors, and when files are shared.

About working with watermarks

The following sections describe how users can set documents to be shown with watermarks, and in what circumstances watermarks cannot be shown.

About users setting watermarks

Workspace administrators, contributors, and users sharing files can determine whether or not watermarks should be displayed in their documents for certain users.

In the BlackBerry Workspaces Web Application, create groups of users per workspace to manage which users can access documents with or without watermarks.

Watermarks are one of the workspace group permission settings. Watermarks are set for a group in the workspace. Users in groups with watermarks enabled view the document with watermarks displayed.

Create a group of users that view workspace documents with watermarks

1. In the BlackBerry Workspaces Web Application, access the **Groups** tab of a workspace.
2. Click **Add**.
3. Enter the **Group** details and click **Next**.
   The **Add a permitted group** window opens.
4. In the **Default permissions** area, click **Advanced**. Make sure that **Watermark** is selected.
5. Click **Add**.
   The group is created. Anytime users from this group access the workspace documents, watermarks are displayed. Users can also add or remove watermarks using the watermark setting per document when sending documents via the BlackBerry Workspaces plugin for Microsoft Outlook.

Changing watermarks settings

Watermarks settings can be changed when needed simply by editing the group settings in the BlackBerry Workspaces Web Application.

Changes apply to documents that are later downloaded and viewed.

When watermarks are not shown

Watermarks are never displayed to users that uploaded the original document, or to users of workspace administrator level in the workspace where the document is located.

In addition, there are some circumstances where watermarks are not supported. The following table describes when watermarks are shown to users that are designated as watermark-viewers:

Note: Where a user belongs to more than one group, and one of the groups that they are a member of has watermarks set to **Off**, the user does not see watermarks in the document.

Microsoft Office documents	
Viewed in Microsoft Office applications	Watermarks are not supported.

Microsoft Office documents	
Viewed in Workspaces Online Viewer	Watermarks are shown.
Viewed on Mac	Watermarks are shown as a diagonal only (even when set to Top or Bottom, watermark is automatically changed to diagonal)
Viewed on iOS mobile device	Watermarks are shown.
Viewed from Android device	Watermarks are shown.

PDF documents	
Viewed in PDF viewer	Watermarks are shown.
Viewed in Workspaces Online Viewer	Watermarks are shown.
Viewed on Mac	Watermarks are shown as a diagonal only (even when set to Top or Bottom, watermark is automatically changed to diagonal)
Viewed on iOS mobile device	Watermarks are shown.
Viewed from Android device	Watermarks are shown.

Generating logs and reports

You can generate logs and reports for users and workspaces. Organization administrators can also generate an audit log.

Note: You can also export data from Central Management to generate logs and reports.

Generate a user activity report

Generate a report on user activity for all activities or items sent by the user only.

1. In the left pane, click **User activities**.
2. In the box, enter the email address of the desired user.
3. Select **All user activities** or **Activities on sent files**.
4. To filter the report by dates, select a start and end date.
5. To export the report, click .
   The report is downloaded as a .csv file.

Generate a workspace activity report

Generate a report on workspace activity.

Note: This report is limited to the latest 200,000 records. If necessary, reduce the report period to generate a report that contains the information you need.

1. In the left pane, click **Workspace activities**.
2. In the box, enter the name of the desired workspace.
3. To filter the report by dates, select a start and end date.
4. To export the report, click .
   The report is downloaded as a .csv file.

Generate an audit log

Generate a report on all the activities performed in the administration console.

1. In the left pane, click **Administrator audit log**.
2. To filter the report by dates, select a start and end date.
3. To export the report, click .
   The report is downloaded as a .csv file.

Generate a licensing report

There are two types of licensing report:

- The **Licensing Snapshot** report gives a detailed list of every user in your account, and whether or not they consume a "contributor" or "sender" license.

- The **Licensing Snapshot including internal domains** report gives a summary of the total number of internal users that consume a license in the given internal domains.

Both reports can be generated on demand, or you can select to have it generated weekly and automatically sent to all organization super-administrators and administrators. The reports reflect the current state only; removed users are not counted, but may still be counted in your license. Therefore, the reports may not fully represent your organization's licensing information. Contact your BlackBerry account representative for more information on your licensing model.

Tip: BlackBerry recommends that you have both licensing reports sent automatically every week and correlate the information to fully capture your license status.

1. In the left pane, click **Licensing**.
2. To generate the licensing snapshot report, in the **Licensing snapshot report** area, click **Generate Report**.
3. To generate and send this report once a week to your organization's super-administrators, select **Send licensing snapshot report to organization administrators once a week** and then click **Apply**.
4. To generate the licensing snapshot report that includes internal domains, perform the following steps in the **Licensing snapshot report including internal domains** area:
   a) In the **Internal domains** area, enter the domains to include in the report.
   b) Click **Generate Report**.
5. To generate and send this report once a week to your organization's super-administrators, select **Send licensing snapshot report to organization administrators once a week** and then click **Apply**.

Generating usage reports

You can generate reports to give you insight into the state of your organization.

Generate an active users report

Generate the active users report to create a list of all active users and their last activity. The report also lists currently inactive users and displays their last activity or shows that no activity has been recorded.

Before you begin: Data for this report is only available starting from the version 5.8.0 release of BlackBerry Workspaces server. Activities performed by users that authenticated via custom OAuth IDP or as a Service Account are not captured in these reports.

1. In the left pane, click **Usage**.
2. In the **Active users** area, click **Generate Report**.
   The report is generated and sent to your email address as a .csv file.

Generate an active users report by date range

Generate an active users report by specific date range to create a list of all active users and their last activity. The report also lists currently inactive users and displays their last activity or shows that no activity has been recorded during the period specified.

1. In the left pane, click **Usage**.
2. In the **Active users** area, select **Click here** in the yellow note area.
3. Select the date range (up to a maximum of 30 days)
4. Click **Generate Report**
   The report is generated and sent to your email address as a .csv file.

Generate an inactive users report

Generate an inactive users report to create a list of all inactive users from a selected date.

Before you begin: Data for this report is only available starting from the version 5.8.0 release of BlackBerry Workspaces server. Activities performed by users that authenticated via custom OAuth IDP or as a Service Account are not captured in these reports.

1. In the left pane, click **Usage**.
2. In the **Inactive users** area, select the date to begin the report.
3. Click **Generate Report**.
   The report is generated and sent to your email address as a .csv file.

Generate a weekly file activity per user report

Generate this report to create a summary of all activities on files, listed by user, within the selected week.

1. In the left pane, click **Usage**.
2. In the **Weekly file activity per user** area, click and select the week you want to generate the report for.
3. Click **Generate Report**.
   The report is generated and sent to your email address as a .csv file.

Generate a weekly organization activity report

Generate this report to create a list of the active users, workspaces created, and files uploaded, updated, and accessed within the selected week.

1. In the left pane, click **Usage**.
2. In the **Weekly organization activity** area, click and select the week you want to generate the report for.
3. Click **Generate Report**.
   The report is generated and sent to your email address as a .csv file.

Generate a workspaces snapshot report

Generate this report to create a snapshot of all workspaces in your organization and their details.

1. In the left pane, click **Usage**.
2. In the **Workspaces snapshot** area, click **Generate Report**.
   You can downloaded the report as a .csv file.

Generating storage reports

Configure storage report alerts and generate storage reports to get detailed information on how storage allocation is being used by your organization.

Configure storage alerts

For configurations where BlackBerry Workspaces is hosted on a virtual appliance, set an alert to show when a user exceeds the maximum amount of storage that you configure. After the threshold is passed, the alert is sent daily until the user goes under the threshold. Reports are sent to the designated recipients when the storage utilization exceeds the thresholds that you set. Reports are sent daily by email until the level falls under the threshold.

The alert can be sent to Administrators and Super Administrators.

1. In the left pane, click **Storage**.
2. To generate an alert when the total organization storage exceeds a certain threshold, select **Send daily alert when storage exceeds a certain capacity threshold** and set the following:
   a) In the **Set capacity threshold** box, enter the percentage of your total storage for when you want to receive an alert about the storage size. (Appliance only).
   b) Select who to send the email alerts to: **Super Admins**, **Admins**.
3. To generate an alert when a user's storage exceeds a certain threshold, select **Send storage reports on users that have reached a certain storage threshold** and set the following:
   a) In the **Set storage threshold** box, enter the amount of storage in GB for when you want to receive an alert about the storage used for each user.
   b) Select who to send the email alerts to: **Super Admins**, **Admins**.
4. Do one of the following:
   - Click **Apply** to apply changes.
   - Click **Apply and Generate Reports Now** to apply the changes and generate and send the reports in near real time.

   A confirmation message confirms the operation.

Generate a workspaces storage report

Generate the active users report to create a list of the amount of storage consumed per workspace in the organization.

1. In the left pane, click **Storage**.
2. In the **Workspaces storage** area, click **Generate Report**.
   The report is generated and sent to your email address as a .csv file.

Generate a sent files storage report

Generate the active users report to create a list of the amount of storage utilized by sent files for each user.

1. In the left pane, click **Storage**.
2. In the **Sent files storage** area, click **Generate Report**.
   The report is generated and sent to your email address as a .csv file.

Generate a weekly organization storage report

Generate this report to create a summary of how much new storage was utilized by the organization within the specified week.

1. In the left pane, click **Storage**.
2. In the **Weekly organization storage** area, click and select the week you want to generate the report for.
3. Click **Generate Report**.
   The report is generated and sent to your email address as a .csv file.

Generate an organization activities report

Generate this report to create a list of all organization activities in workspaces and sharing for a specified time period.

1. In the left pane, click **Organization activities**.
2. Click and select the start and end dates for the report.

3. Click **Generate Report**.
   The report is generated and sent to your email address as a .csv file.

Generate an authentication activities report

Generate this report to get a summary of all authentication activities (sign in, refresh, and sign out), within a specific month.

Before you begin: Data for this report is only available on BlackBerry Workspaces server 5.8.0 or later. Authentication activities performed by custom OAuth IDPs and Service Accounts are not captured in this report.

1. In the left pane, click **Authentication Activities**.
2. In the Select month drop-down list, select the month you want to generate the report for.
3. Click **Generate Report**.
4. On the bottom of the screen, click **Download** and save the file to your computer.

Configuring BlackBerry Workspaces

You can customize the appearance of the BlackBerry Workspaces Web Application.

Customize BlackBerry Workspaces Web Application

Customize the appearance of the BlackBerry Workspaces Web Application. For example, you can add your organization's logo and redirect legal and support links to external webpages that you maintain.

Note: These features are supported only for organizations that use a customized subdomain within BlackBerry Workspaces cloud or for organizations that host BlackBerry Workspaces on an on-premise virtual appliance.

Before you begin: If your organization is working within a separate BlackBerry Workspaces subdomain, replace the logo within that subdomain with your own organization's logo.

1. In the left pane, click **Customization**.
2. In the **Name and Logo** area, enter the **Application name**.

   Note: If your organization does not have its own BlackBerry Workspaces subdomain, then to implement this feature you must contact BlackBerry Workspaces technical support to reconfigure the settings appropriately.
3. Select a logo:
   - Select **Use default application logo** to use the default logo.
   - Select **Upload logo** and click **Upload** to choose your custom organization's logo file. A "logo uploaded successfully" message appears, confirming the logo upload.
4. Enter the link that you want used for the **Terms of service** element where it appears in the BlackBerry Workspaces apps.
5. Enter the link that you want used for the **Privacy policy** element where it appears in the BlackBerry Workspaces apps.
6. In the **Contact Support** area, define what happens when the **Contact Support** link is accessed by end users.
   - If you would like an email to be sent with a support message, select the **Support emails** radio button then enter one of more email addresses in the field provided. By default, organization administrator email addresses are used.
   - If you would like to define a custom support url instead, select the **Support link** radio button and then enter an url in the field provided.
7. Select **Show about us link** to include the element in BlackBerry Workspaces apps, and enter the link that you want used.
8. Select **Show Help link** to include the element in BlackBerry Workspaces apps, and enter the link that you want used.
9. Select **Show Contact us link** to include the element in BlackBerry Workspaces apps, and enter the link that you want used.
10. Select **Show PC download link** to include the element in BlackBerry Workspaces Web Application, and enter the link that you want used.
11. Select **Show Mac download link** to include the element in BlackBerry Workspaces Web Application, and enter the link that you want used.
12. If you would like to include links in the BlackBerry Workspaces Web Application to your organization's branded versions of the Quick Start and User Guides, select **Show Quick start guide link** and **Show user guide link** and enter the links that you want to use.
13. Click **Apply**. A confirmation message confirms the operation.

Configure and customize emails

Configure and customize the system emails that are sent to new users.

1. In the left pane, click **Emails**.
2. To send a welcome email the first time a user is provisioned to the system, select **Welcome Email**.
3. To add a secondary language (other than English), select **Secondary language** and choose the language from the **Secondary language** drop-down list.
4. To customize the About Workspaces text, select **Customize the "About" Workspaces text** and enter the customized text to use. If you selected Secondary language in the previous step, you can also enter customized text in the secondary language.
5. To enable inclusion of the default Getting Started video, select **Enable "Get started" video**.
6. To include PC, MAC, iOS, and/or Android app download links, select the related download link options.
7. To enable the ability to change the email "from" field to the user account name, instead of the "sender" name, select **Enable "On Behalf Of" for Email Notifications**.
8. To have a daily activity report sent by default to each user on file activity for workspaces they own, select **Turn on daily activity report email for all users in my organization**.
9. To send email notifications without the workspace, folder, and file names, select **Turn off email notification details (Workspaces, folders and file names)**. If you select this option, daily activity reports aren't sent to users.
10. Click **Apply changes**.

Configure ICAP

1. In the left pane, click **ICAP**.
2. Enter the following ICAP credentials:
   - **Host** – enter the ICAP service host name or IP address.
   - **Port** – enter the number of the ICAP service port.
   - **Service name** – Enter the ICAP service name.
   - **Timeout** – Enter the amount of time in seconds after which Workspaces stops waiting for the ICAP service to respond.
3. To allow upload of files when the ICAP service is not responding or timeout is reached, select **Accept files when ICAP is unavailable**.
4. If the ICAP server requires SSL, select the **SSL enabled** checkbox.
5. Click **Apply changes**.

Configure Syslog

Enable BlackBerry Workspaces to send the Workspaces activity log, to your organization's Syslog server.

1. In the left pane, click **Syslog**.
2. Enter the following Syslog credentials:
   - **Syslog server address**
   - **Syslog server port**
3. If necessary, select the **Use Syslog over TCP** checkbox.

4. Click **Apply changes**.

Defining tags

You can define tags that you can associate with files in your organization's workspaces. Tags are useful to help you find files. There are three types of tags:

- **Text**: tags for which you can define any text
- **Number**: numeric tags
- **Date**: date tags

Add a tag

1. In the left pane, click **Tags**.
2. Click +.
3. Enter a **Category** or name for the tag.
4. Select the **Tag Type** from the drop-down list: **Text**, **Number**, or **Date**
5. Click **Save** to save the tag.
   A confirmation message confirms the operation, and the new tag appears in the list.

Edit a tag

1. In the left pane, click **Tags**.
2. Select a tag in the list.
3. Click ✎.
4. Edit the **Category** or name for the tag.
5. Change the **Tag Type** as desired.
6. Click **Save** to save the tag.
   A confirmation message confirms the operation, and the modified tag appears in the list.

Delete a tag

1. In the left pane, click **Tags**.
2. Select a tag in the list.
3. Click 🗑.
4. In the confirmation window, click **Delete** to remove the selected tags fields with their associated tags from all documents and workspaces where they are used. Note that this operation cannot be reversed.
   A confirmation message confirms the operation, and the tag(s) are removed from the list.

Defining workspace roles

You can create custom roles and define their capabilities for use in your organization. Workspace administrators can assign roles to individuals, groups, and email domains. Role capabilities enable users to perform operations on workspaces, folders, and files that they can access. The assigned role does not affect the user's capabilities for files they upload.

Add a workspace role

1. In the left pane, click **Workspace Roles**.

2. Click +.
3. Enter a **Role name**.
4. Enter a **Description** for the role.
5. Enter an **Acronym** of two capital letters to identify the role.
6. Select all the workspace capabilities that you want to give the role.
7. Click **Save**.
   A confirmation message confirms the operation, and the new role appears in the list.

Edit a workspace role

1. In the left pane, click **Workspace Roles**.
2. Select a role in the list.
3. Click ✎.
4. Edit the **Role name**, **Description**, or **Acronym** as desired.
5. Select or clear workspace capabilities as desired.
6. Click **Save** to save your changes.
   A confirmation message confirms the operation, and the modified tag appears in the list.

Delete a workspace role

1. In the left pane, click **Roles**.
2. Select one or more roles in the list.
3. Click 🗑.
4. In the confirmation window, click **Delete** to delete the role.
   A confirmation message confirms the operation, and the role(s) are removed from the list.

Configure the Enterprise mode

Set the enterprise mode for your organization.

1. In the left pane, click **Workspaces Mode**.
2. Select the Enterprise mode:
   - **Enterprise ES Mode**: to provide the full range of file controls to the end users, including downloading original, downloading controlled documents, or online viewing.
   - **Enterprise ES (Restrict Full Access) Mode**: to enforce BlackBerry Workspaces controls on all Microsoft Office and PDF files. If the user is the document owner, this is not applied.
3. If you selected **Enterprise ES Mode** or **Enterprise ES (Restrict Full Access) Mode**, select **Allow [the organization] to track user actions on Workspaces-protected Microsoft Office files to track actions on downloaded files**, if desired.
4. Click **Apply changes**.

Managing authentication

You can manage authentication in the administration console.

Automatically authenticate a user

BlackBerry Workspaces can automatically authenticate a user if the user has already activated BlackBerry Dynamics on their device. After you implement this feature, users do not need to enter any details after installing the BlackBerry Workspaces app for the first time. This setting also automatically completes the BlackBerry Workspaces site URL field in the mobile login screen. Before you can enable this feature your organization must have the following products:

Before you begin:

- BlackBerry Workspaces plug-in for BlackBerry UEM
- BlackBerry Workspaces for BlackBerry Dynamics

1. In the BlackBerry UEM console, click **Apps**.
2. in the list of apps, click **BlackBerry Workspaces**.
3. In the **App configuration** table click **+**.
4. Add a name for the app configuration and a **Workspaces Site** URL. For more information about BlackBerry Workspaces app configuration settings, refer to the BlackBerry UEM Administration Guide.
5. Click **Save**.
6. Click **Save**.

After you finish: Note that if the **Workspaces Site URL** field does not display, you must update the server configuration payload. On the **BlackBerry Dynamics** tab, in the **Server configuration payload** section, click **Add** and enter the following information:

```
<setting name="workspacesSite">

<text>

                        <key>workspacesSite</key>

                        <label>Workspaces Site</label>

                        <value>blackberry.watchdox.com</value>

                  </text>

</setting>
```

For more information about BlackBerry Workspaces app configuration settings, see the BlackBerry Workspaces plug-in for BlackBerry UEM Administration content.

Block unprovisioned users from creating accounts

Perform these steps to block unprovisioned users from creating an account.

1. In the left pane, click **General**.
2. Select **Block non-provisioned users from creating accounts**.
3. Click **Apply**.

Configure browser inactivity timeout

You can configure Workspaces to automatically log a user out of their session after a predetermined time of inactivity.

1. In the left pane, click **General**.
2. Select **Browser inactivity timeout**.
3. In the **Browser inactivity timeout** box, enter the number of minutes of inactivity after which a user is logged out of their browser session.
4. Click **Apply**.

Configure the organization authentication method

1. In the left pane, click **Methods**.
   The **Methods** page differs depending on the pre-defined organization authentication method.
2. For organizations that have one authentication method, select the authentication type:
   - **Email Authentication**
   - **Username & Password**
   - **Active Directory**
   - **BlackBerry Enterprise Identity**
3. For all authentication types, set the default token management:
   a) In the **Access token TTL** box, enter the validity period in minutes for each specific token created. This value is usually shorter or equal to the Refresh token TTL.
   b) In the **Refresh token TTL** box, enter the period in minutes after which inactive users are required to sign in again.
   c) Select **Auto-renew refresh token** to require users to re-authenticate when the refresh token expires, even if users were active during this period.
4. If you enabled Office Online, in the **Access token TTL** box, enter the validity period in minutes for each specific token created.
5. If desired, manage the tokens for each BlackBerry Workspaces application.

   Note: If you change the token settings for a BlackBerry Workspaces application, the settings for that application are irrevocably decoupled from the default token management. Any subsequent changes to the default token management will not apply to the application.
6. If you selected **Username & Password** as the authentication type, or your organization is set to multimode authentication, configure the username and password settings. For more information, see About username and password authentication.
7. If you selected **BlackBerry Enterprise Identity** as the authentication type, configure the Enterprise Identity settings. For more information, see About BlackBerry Enterprise Identity authentication.
8. Click **Apply changes**.

About email authentication

If you select **Email Authentication**, users are prompted to click a link that is received via an email sent from BlackBerry Workspaces.

Users who authenticate via this method are prompted to enter their email address and to select whether the computing device is a trusted **Private Device** or a **Public Device**.

- If the device is designated as a **Private Device**, the authentication token does not expire unless the user explicitly signs out.
- If the device is designated as a **Public Device**, the authentication token expires after 5 minutes or if the session is closed.

About username and password authentication

When you select **Username & Password**, the following configurations are available:

Note: Username and password settings can be changed in Appliance configurations. In the public cloud environment, username and password authentication settings are set by BlackBerry Workspaces and cannot be changed.

- **Password Policy** enables you to set the desired password configurations for end users.
  - **Minimum length**: sets the minimum number of characters required
  - **Maximum length**: sets the maximum number of characters required
  - **Minimum uppercase character(s)**: sets the minimum number of uppercase characters (e.g. "T") required
  - **Minimum lowercase character(s)**: sets the minimum number of lowercase characters (e.g. "t") required
  - **Minimum numbers**: sets the minimum number of numbers (e.g. "8") required
  - **Minimum special character(s)**: sets the minimum number of special characters (e.g. "#") required
  - **Number of wrong password entry attempts**: sets the number of failed login attempts before the user account is locked out (the user would be able to recover the account by answering the Secret Question they had selected).
  - **"Remember me" duration in days**: sets the number of days that the user is signed-in to BlackBerry Workspaces through the browser web interface without the need to re-enter the password. **Note:** This setting does not apply to the BlackBerry Workspaces for Windows and the Workspaces mobile applications.
  - **Number of days until password expires**: sets the number of days that the password is valid.
  - **Number of passwords to remember**: sets the number of remembered passwords (maximum 10) so that users cannot change their passwords to a remembered password.
  - **Blacklist** is a configurable list of passwords that are not permitted by the organization (for example, "123456")

About Microsoft Active Directory authentication

Microsoft Windows credentials can be used by end users to log into BlackBerry Workspaces. Configuring the Workspaces server to integrate with Active Directory allows Windows credentials to be used during the authentication process.

To perform the integration for authentication with Windows credentials, contact your BlackBerry Workspaces Technical Account Manager for help with the configuration process.

Note: As of BlackBerry Workspaces version 7.0, ADFS metatdata can be retrieved from the identity provider every 15 minutes. This allows the most up-to-date metadata to be available, and reduces failed login attempts for new users. For more information on configuring a SAML-based identity provider such as ADFS, visit support.blackberry.com/community to read article 52826.

About BlackBerry Enterprise Identity authentication

If you select **BlackBerry Enterprise Identity**, users are prompted to sign in using their Enterprise Identity.

1. Make sure that BlackBerry Workspaces has been added as a service to your Enterprise Identity account.
2. Click **Upload** to upload the SAML Service Metadata XML file.
3. Click **Apply** to save your changes. A confirmation message appears.

4. Confirm your changes. Sign in again using Enterprise Identity to continue.

About OAuth integration with third-party providers

BlackBerry Workspaces simplifies user authentication while enhancing security through its ability to integrate with the customer's authentication scheme through a single sign-on procedure. The SSO implementation in Workspaces provides controlled access to all its services, with the customer maintaining control over user identity and authentication. Customers who choose to integrate with Workspaces using the OAuth 2.0 Single Sign On protocol may also choose to authenticate users through a third-party authentication or identity provider (for example, two-factor authentication, Single Sign On, and so on).

To integrate Workspaces to other third-party authentication and identity providers, contact your BlackBerry Workspaces Technical Account Manager for help with the configuration process.

About multimode authentication

Multimode authentication enables your organization to use multiple user authentication methods based on user email domain.

You can associate each authentication method with one or more domains. Set a default authentication method for undefined domains.

For example, you could define the following authentication policy for your organization and partners:

- All users accessing your BlackBerry Workspaces system with @company.com email address sign in using an Microsoft Active Directory single sign on authentication.
- All users accessing your Workspaces system with a @partner.com email address sign in using username and password authentication.
- All other users accessing your Workspaces system sign in using email authentication.

For more information on configuring multimode authentication, refer to the *Configuring Multimode Authentication Technical Note*.

About BlackBerry Dynamics authentication

Mobile devices running in a BlackBerry Dynamics container environment can automatically authenticate to Workspaces by leveraging the existing GDAuth token. The BlackBerry Workspaces UEM snapin is required.

Simplified login process for internal users

A simplified login process is available for internal/VPN users. Users can be identified by IP address range and automatically redirected to their IDP page without entering an email address, or in the case of Single Sign-on, automatically logged in.

The org policy **Is Allowed Multi Ip Ranges** is required.

Configure service accounts

If your organization has a SharePoint or a Windows File Share connector, define service accounts to allow API access to the system without going through web authentication.

To access Service Accounts, click **Service Accounts** in the left pane.

Add a service account

1. In the left pane, click **Service Accounts**.

2. Next to the **Service accounts** area, click +.
3. In the **Public key** box, enter the public key.
4. In the **System accounts** area, enter an email address or distribution list name.
5. In the **Domain system accounts** area, enter domain system accounts, as required.
6. In the **Algorithm** area, choose an algorithm from the drop-down list.
7. Click **Add**.

Edit a service account

1. In the left pane, click **Service Accounts**.
2. Select the service account that you want to edit.
3. To change the public key, enter a new key in the public key in the **Public key** box.
4. To change or add a system account, enter an email address or distribution list name in the **System accounts** area.
5. To change or add a domain system account, enter domain system accounts in the **Domain system accounts** area, as required.
6. Click **Apply**.
   A confirmation message confirms the operation, and the modified tag appears in the list.

Delete a service account

1. In the left pane, click **Service Accounts**.
2. Select the service account that you want to delete.
3. Click **Delete**.
4. In the confirmation window, click **Delete**.
   A confirmation message confirms the operation.