Windows 10 Planning and Deployment Guide

Contents

Introduction to Windows 10 deployment with BlackBerry UEM..... 5
Key features for Windows 10 devices in UEM....5

Checklist for managing devices with UEM only..... 8

Checklist for managing devices with UEM and SCCM..... 9

Enrolling Windows 10 devices with BlackBerry UEM..... 10
Enrolling a device to be managed with BlackBerry UEM....10
Create an activation profile for Windows 10 devices....10
Simplifying Windows 10 activations....11
Activate a Windows 10 device....11
Enrolling an unmanaged device with BlackBerry Access for Windows....12

Setting up UEM policies and profiles to manage Windows 10 devices..... 14
Restricting or allowing device capabilities....14
Setting device password requirements....14
How BlackBerry UEM chooses which IT policy to assign....14
Creating and managing IT policies....15
Create an IT policy....15
Copy an IT policy....15
Rank IT policies....15
View an IT policy....15
Change an IT policy....16
Remove an IT policy from user accounts or user groups....16
Delete an IT policy....16
Export IT policies....17
Sending certificates to devices using profiles....17
Choosing profiles to send client certificates to devices....17
Sending CA certificates to devices....18
Using SCEP to send client certificates to devices....18
Setting up work email for devices....19
Create an email profile....19
Create an IMAP/POP3 email profile....20
Using Exchange Gatekeeping....21
Allow a device to access Microsoft ActiveSync....21
Block a device from accessing Microsoft ActiveSync....21
Verifying that a device is allowed to access work email and organizer data....21
Creating a gatekeeping profile....22
Setting up work VPNs for devices....22
Create a VPN profile....23
Enabling per-app VPN....23

Setting up work Wi-Fi networks for devices.... 23
Create a Wi-Fi profile.... 24
Enforcing compliance rules for devices.... 24
Create a compliance profile.... 25
Windows: Compliance profile settings.... 25
Setting up Windows Information Protection for Windows 10 devices.... 27
Create a Windows Information Protection profile.... 28
Windows 10: Windows Information Protection profile settings.... 28
Managing Windows 10 devices that are enrolled in UEM and SCCM.... 32
Configuring policies in SCCM.... 32

Configuring UEM to manage apps for Windows 10 devices.... 34
Connecting BlackBerry UEM to Microsoft Azure.... 34
Create a Microsoft Azure account.... 35
Synchronize Microsoft Active Directory with Microsoft Azure.... 35
Create an enterprise endpoint in Azure.... 35
Configuring BlackBerry UEM to synchronize with the Windows Store for Business.... 36
Specify the shared network location for storing internal apps.... 38
Add a Windows 10 app to the app list.... 39
Allowing users to install online Windows 10 apps.... 39
Add an app category for a Windows 10 app.... 39
App behavior on Windows 10 devices.... 40
Setting up network connections for BlackBerry Dynamics apps.... 41
Create a BlackBerry Dynamics connectivity profile.... 41
Add an app server to a BlackBerry Dynamics connectivity profile.... 41
BlackBerry Dynamics connectivity profile settings.... 42

Remote management for Windows 10 devices.... 44
Sending commands to users and devices.... 44
Send a command to a device.... 44
Send a bulk command.... 44
Set an expiry time for commands.... 46
Commands reference.... 46
Locate a device.... 47

Managing Windows 10 device updates with BlackBerry UEM.... 48

Deactivating devices.... 49

Related information.... 50

Legal notice.... 51

Introduction to Windows 10 deployment with BlackBerry UEM

Organizations across various industries are including Windows 10 tablets and laptops in their mobility strategy planning. Currently, they might use traditional methods such as Microsoft System Center Configuration Manager (SCCM) or other client management tools to manage Windows 10 devices, while iOS and Android smartphones and tablets are managed with another MDM solution. To manage Windows 10, iOS, and Android devices in a unified management console, you can use BlackBerry UEM.

To support Windows 10 devices, BlackBerry UEM provides multiple deployment options and scenarios:

- **Specialized Windows 10 devices fully managed by BlackBerry UEM:** Administrators can manage Windows 10 devices from the UEM management console after users activate their devices with UEM. Administrators can view and manage activated devices through a unified interface. Users can also use the BlackBerry UEM Self-Service console to perform simple administrative actions (for example, wipe work data, locate a lost device, activate new devices, or generate access keys for BlackBerry Dynamics apps). When devices are activated with UEM, you can also easily deploy apps from the app store or enterprise apps (for example, BlackBerry Access, BBM Enterprise, and BlackBerry Workspaces) to users from the UEM management console.
- **Corporate Windows 10 devices managed by BlackBerry UEM and Microsoft SCCM (in coexistence):** Administrators can use either BlackBerry UEM and Microsoft SCCM solutions exclusively to manage Windows 10 devices in their organization or they can adopt the Windows 10 management features of BlackBerry UEM together with the group policies of SCCM. UEM and SCCM can co-exist: devices can be enrolled and managed by both solutions simultaneously.
- **Unmanaged devices (for personal devices, contractors, or external parties):** If you don't want to manage Windows 10 devices but still want users to access your organization's intranet and work email, users can install BlackBerry Access for Windows and activate it using a BlackBerry Dynamics access key. Administrators can generate access keys for users from the UEM management console, and if allowed, users can generate them from the BlackBerry UEM Self-Service console. Any device can activate BlackBerry Dynamics apps, even if it is not managed. For more information, see the BlackBerry Access product information and BlackBerry Workspaces product information.

Key features for Windows 10 devices in UEM

The following table highlights the features available to unmanaged devices and managed devices in BlackBerry UEM. You can manage Windows 10 devices, including Windows 10 tablets and computers. Silver licenses are required to activate Windows 10 devices.

Feature	Description
Unmanaged devices (devices that are not managed by UEM)	You can enable secure access to work content even if UEM does not manage the device. To enable secure access to the work intranet, email, and contacts, you deploy BlackBerry Access for Windows 10 devices. For more information about BlackBerry Access, see the BlackBerry Access Administration Guide. To enable secure file-sharing, you can deploy BlackBerry Workspaces. For more information, see the BlackBerry Workspaces server content.

Feature	Description
Managed devices (devices that are managed by UEM)	You can deploy Windows 10 devices to be managed with UEM only, or in coexistence with Microsoft System Center Configuration Manager (SCCM). When you use UEM to manage Windows 10 devices, it allows you to: • Apply IT policies and profiles • Deploy apps from the Windows Store for Business to the BlackBerry UEM App Catalog • Configure device update management settings • Set compliance rules (for example, Windows Health Attestation)

Device features

- Wireless activation
- Customize terms of use agreement
- Client app not required
- View and export device details (for example, hardware details)

Security features

- Separation of work and personal data
- Encryption of work data at rest
- Protection of devices using remote IT commands (for example, lock the device)
- Control device capabilities using IT policies (for example, disable camera)
- Enforce password requirements
- Enforce encryption of internal storage

Sending certificates to devices

- CA certificate profiles
- SCEP profiles

Managing work connections for devices

- BlackBerry Dynamics connectivity profiles
- Exchange ActiveSync email profiles
- IMAP/POP3 email profiles
- Wi-Fi and VPN profiles (with proxy)
- Windows Information Protection profiles

Managing your organization's standards for devices

- Activation profiles
- App lock mode profiles[1]
- BlackBerry Dynamics profiles
- Compliance profiles

- Device profiles
- Enterprise Management Agent profiles

[1] Only for Windows 10 Education and Windows 10 Enterprise devices.

Protecting lost or stolen devices

- Delete all device data
- Delete only work data

Configuring roaming

- Disable data when roaming

Managing apps

- Distribute public apps from storefront (Windows Store)
- Manage work app catalog
- Manage restricted apps[1]
- Distribute internal apps

[1] The restricted app list is not required for Windows 10 devices because only apps that an administrator assigns can be installed in the work space or on devices.

Checklist for managing devices with UEM only

The following check list is intended for administrators that want to manage Windows 10 devices with BlackBerry UEM only.

Step	Description
☐	Configure the latest version of BlackBerry UEM (12.10 or later) or BlackBerry UEM Cloud according to your organization's specifications. For more information, refer to the following: • BlackBerry UEM Installation Guide • BlackBerry UEM Configuration Guide • BlackBerry UEM Cloud Configuration Guide
☐	Configure IT policies and profiles for Windows devices. Assign the policies and profiles to the appropriate users and user groups. You must allow Windows devices to be activated in the activation profile. For more information, see Enrolling a device to be managed with BlackBerry UEM.
☐	Configure UEM to manage apps for Windows 10 devices. Assign the apps to the appropriate users and user groups.
☐	Activate a Windows 10 device.

After activation, you can manage Windows 10 devices in UEM. For example, you can make changes to IT policies and profiles at any time. They will be enforced on the users and user groups that they are assigned to. You can also manage the device remotely (for example, wipe the device), and define when Windows updates are allowed to occur.

Checklist for managing devices with UEM and SCCM

The checklist in the following section is intended for administrators that want to manage Windows 10 devices with both BlackBerry UEM and SCCM.

Step	Description
☐	Configure the latest version of BlackBerry UEM (12.10 or later) or BlackBerry UEM Cloud according to your organization's specifications. For more information, refer to the following: • BlackBerry UEM Installation Guide • BlackBerry UEM Configuration Guide • BlackBerry UEM Cloud Configuration Guide
☐	Verify that the following requirements are met: • Administrators must be running SCCM version build 1710 or later • Users must be running Windows 10 build 1709 or later on their devices
☐	Using the MDM Migration Analysis Tool (MMAT), determine the policies that can be managed with UEM. SCCM will continue to manage any group policy that does not have an equivalent MDM policy. 1. Download the MMAT. 2. Run the tool in the SCCM environment. The result is an output of the list of group policies that are currently in use and the equivalent policy that is available in MDM management. For more information, see the Microsoft CSP reference. 3. If necessary, use the information generated from the tool to create IT policies and profiles for Windows devices in UEM in the following step.
☐	Configure IT policies and profiles for Windows devices. Assign the policies and profiles to the appropriate users and user groups. You must allow Windows devices to be activated in the activation profile. For more information, see Enrolling a device to be managed with BlackBerry UEM.
☐	Configure UEM to manage apps for Windows 10 devices. Assign the apps to the appropriate users and user groups.
☐	Activate a Windows 10 device.

After activation, you can manage Windows 10 devices in UEM. For example, you can make changes to IT policies and profiles at any time. They will be enforced on the users and user groups that they are assigned to. You can also manage the device remotely (for example, wipe the device), and define when Windows updates are allowed to occur.

For any group policy that is not assigned by an IT policy in UEM, you can continue to manage the policy in SCCM.

Enrolling Windows 10 devices with BlackBerry UEM

In this section you can find information about how to enroll Windows 10 devices.

Enrolling a device to be managed with BlackBerry UEM

Administrators can manage Windows 10 devices with MDM management controls when they are activated with BlackBerry UEM. When a device is managed with UEM, you can use UEM to apply IT policies and profiles, push apps from the Windows Store for Business, configure device update management settings, and set compliance rules.

To enroll devices and manage them with UEM, do the following in the BlackBerry UEM management console:

Step	Description
1	Verify that the activation settings are configured in the BlackBerry UEM console: 1. Configure default activation settings in BlackBerry UEM. 2. Set up an email template for activation.
2	Create an activation profile for Windows 10 devices.
3	Set an activation password for the user.
4	Activate the Windows 10 device.

Create an activation profile for Windows 10 devices

Before users can activate a Windows 10 device, an activation profile that allows Windows 10 activations must be assigned to their accounts. You can create or modify an activation profile to allow Windows 10 activations. For more information about using and assigning profiles in UEM, see Using profiles, variables, and email templates.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > Activation**.
3. Click +.
4. Type a name and description for the profile.
5. In the **Number of devices that a user can activate** field, specify the maximum number of devices the user can activate.
6. In the **Device ownership** drop-down list, select the default setting for device ownership. Perform one of the following actions:
   - If some users activate personal devices and some users activate work devices, select **Not specified**.
   - If users typically activate work devices, select **Work**.
   - If users typically activate personal devices, select **Personal**.

7. Optionally, select an organization notice in the **Assign organization notice** drop-down list. If you assign an organization notice, users activating Windows 10 devices must accept the notice to complete the activation process.
8. In the **Device types that users can activate** section, select the device types as required (for example, **Windows**). Device types that you don't select are not included in the activation profile and users can't activate those devices.
9. On the **Windows** tab, do the following:
   - In the **Allowed device form factor** section, select **Phone** if you want to allow Windows 10 smartphones to be activated, and select **Tablet or computer** to allow Windows 10 tablets and computers to be activated.
   - In the **Device model restrictions** drop-down list, select whether to allow or restrict specified devices or to have no restrictions. Click **Edit** to select the devices you want to restrict or allow and click **Save**.
   - In the **Allowed version** drop-down list, select the minimum allowed version.
10. Click **Add**.

After you finish: If necessary, rank profiles.

Activation types: Windows devices

Activation type	Description
MDM controls	This activation type provides basic device management using device controls made available by Windows 10. A separate work space is not installed on the device, and there is no added security for work data. You can control the device using commands and IT policies. Windows 10 users activate devices through the Windows 10 Work access app.

Simplifying Windows 10 activations

You can deploy a discovery service to simplify the activation process for Windows 10 device users. If you use the discovery service, users don't need to type a server address during the activation process. If you choose not to use a discovery service, users can still activate Windows 10 devices but they will be required to type the server address when prompted.

For information about how to deploy the discovery service, see the BlackBerry UEM configuration content.

Activate a Windows 10 device

You can activate your Windows 10 tablet or computer to associate it with your organization's environment so that you can access work data on your device.

Before you begin:

- In BlackBerry UEM Self-Service, Create an activation password or QR code.
- Watch a video tutorial available at https://docs.blackberry.com/en/endpoint-management/blackberry-uem-activation-videos.

1. To activate your Windows 10 tablet or computer on BlackBerry UEM, you must install a certificate. You can find a link to the certificate in the activation email you received. If you did not receive a link to the certificate, contact your administrator for assistance. Using the Microsoft Outlook app, or using your online email service in the browser, open your Inbox.
2. In your Inbox, tap the activation email message that you received from your administrator.
3. Tap the link to the certificate server.
4. In the certificate download notification, tap **Open**.

5. Tap **Install Certificate**.
6. Select the **Local Machine** option. Tap **Next**.
7. Select the **Place all certificates in the following store** option. Tap **Browse**.
8. Select **Trusted Root Certification Authorities**. Tap **OK**.
9. Tap **Next**.
10. Tap **Finish**.
11. Tap **Yes**.
12. Tap **OK**.
13. Tap the **Start** button.
14. Tap **Settings**.
15. Tap **Accounts**.
16. Tap **Work access**.
17. Tap **Connect**.
18. In the **Email address** field, type your email address. Tap **Continue**.
19. If you are asked for your server address, in the **Server** field, type your server address or activation URL and tap **Continue**. You can find your server address or activation URL in the activation email that you received from your administrator or in BlackBerry UEM Self-Service when you set your activation password.
20. In the **Activation password** field, type your activation password and tap **Continue**. You can find your activation password in the activation email that you received from your administrator, or you can set your own activation password in BlackBerry UEM Self-Service.
21. Tap **Done**.
22. The activation process is complete.

After you finish: To verify that the activation process completed successfully, perform one of the following actions:

- On the device, open the Work access app and check that your account is listed. Tap your account and select Info. Check the sync status information to make sure that your device is connected to BlackBerry UEM.
- In BlackBerry UEM Self-Service, verify that your device is listed as an activated device. It can take up to two minutes for the status to update after you activate the device.

Enrolling an unmanaged device with BlackBerry Access for Windows

BlackBerry Access for Windows is a BlackBerry Dynamics app that allows users to access the work intranet, email, and contacts on Windows devices without the need to allow MDM management. Administrators can revoke access to work content at any time.

BlackBerry Dynamics apps need to be activated using an access key. Administrators can generate access keys for users in the UEM management console. Users can also generate access keys in BlackBerry UEM Self-Service. Users do not need to activate their device with UEM to receive access keys.

To enroll a device (that UEM does not manage) with BlackBerry Access for Windows:

Step	Description
1	Deploy BlackBerry Access. For more information about the requirements of BlackBerry Access and how to deploy it, see the BlackBerry Access Administration Guide.

Step	Description
2	Users must install and activate the BlackBerry Access for Windows app on their devices. To activate the app, administrators generate access keys and email them to users. For more information about how to install and activate BlackBerry Access on the device, see the BlackBerry Access for Windows User Guide.

Setting up UEM policies and profiles to manage Windows 10 devices

In this section, you can learn about the policies and profiles that are available for Windows 10 devices in BlackBerry UEM and how to set them up.

- **IT policies**: Set password requirements and restrict device capabilities.
- **Certificate profiles**: Choose which certificates are sent to the devices for authentication.
- **Email profiles**: Specify settings for work email accounts so that users can access their work email from the native mail app on their device.
- **VPN and Wi-Fi profiles**: Specify network settings so that users can access work resources from their device.
- **Compliance profiles**: Set rules to encourage users to follow your organization's standards for the use of devices.
- **Windows Information Protection profiles**: Configure Windows 10 devices to protect work data.

Restricting or allowing device capabilities

When you configure IT policy rules, you can restrict or allow device capabilities. The IT policy rules available for each device type are determined by the device OS and version and by the device activation type. For example, depending on the device and activation type, you can use IT policy rules to:

- Enforce password requirements for the device or the work space on a device
- Prevent users from using device features, such as the camera
- Control connections that use Bluetooth wireless technology
- Control the availability of certain apps
- Require encryption and other security features

Depending on the device activation type, you can use IT policy rules to control the entire device, only the work space on a device, or both.

Setting device password requirements

In BlackBerry UEM, you can use IT policy rules to set the password requirements for devices. For example, you can set requirements for password length and complexity, password expiration, and the result of incorrect password attempts. The following topics explain the password rules that apply to the various device and activation types.

For more information about the IT policy rules, download the Policy Reference Spreadsheet.

How BlackBerry UEM chooses which IT policy to assign

In BlackBerry UEM, you can assign more than one IT policy to a device, but BlackBerry UEM uses predefined rules to choose which IT policy to assign to a user and the devices that the user activates. For more information about IT policies, see the BlackBerry UEM administration content.

Creating and managing IT policies

You can use the Default IT policy or create custom IT policies (for example, to specify IT policy rules for different user groups or device groups in your organization). If you plan to use the Default IT policy, you should review it and, if necessary, update it to make sure that the rules meet your organization's security standards.

For more information about the IT policy rules, download the Policy Reference Spreadsheet.

Create an IT policy

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Click +.
4. Type a name and description for the IT policy.
5. Click the tab for each device type in your organization and configure the appropriate values for the IT policy rules.

   Hold the mouse over the name of a rule to display help tips.
6. Click **Add**.

After you finish: Rank IT policies.

Copy an IT policy

You can copy existing IT policies to quickly create custom IT policies for different groups in your organization.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Click the name of the IT policy that you want to copy.
4. Click .
5. Type a name and description for the new IT policy.
6. Make changes on the appropriate tab for each device type.
7. Click **Add**.

After you finish: Rank IT policies.

Rank IT policies

Ranking is used to determine which IT policy BlackBerry UEM sends to a device in the following scenarios:

- A user is a member of multiple user groups that have different IT policies.
- A device is a member of multiple device groups that have different IT policies.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Click .
4. Use the arrows to move IT policies up or down the ranking.
5. Click **Save**.

View an IT policy

You can view the following information about an IT policy:

- IT policy rules specific to each device type
- List and number of user accounts that the IT policy is assigned to (directly and indirectly)
- List and number of user groups that the IT policy is assigned to (directly)

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Click the name of the IT policy that you want to view.

Change an IT policy

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Click the name of the IT policy that you want to change.
4. Click .
5. Make changes on the appropriate tab for each device type.
6. Click **Save**.

After you finish: If necessary, change the IT policy ranking.

Remove an IT policy from user accounts or user groups

If an IT policy is assigned directly to user accounts or user groups, you can remove it from users or groups. If an IT policy is assigned indirectly by user group, you can remove the IT policy from the group or remove user accounts from the group. When you remove an IT policy from user groups, the IT policy is removed from every user that belongs to the selected groups.

Note: The Default IT policy can only be removed from a user account if you assigned it directly to the user.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Click the name of the IT policy that you want to remove from user accounts or user groups.
4. Perform one of the following tasks:

Task	Steps
Remove an IT policy from user accounts	**a.** Click the **Assigned to users** tab. **b.** If necessary, search for user accounts. **c.** Select the user accounts that you want to remove the IT policy from. **d.** Click .
Remove an IT policy from user groups	**a.** Click the **Assigned to groups** tab. **b.** If necessary, search for user groups. **c.** Select the user groups that you want to remove the IT policy from. **d.** Click .

Delete an IT policy

You cannot delete the Default IT policy. When you delete a custom IT policy, BlackBerry UEM removes the IT policy from the users and devices that it is assigned to.

1. On the menu bar, click **Policies and Profiles**.

2. Click **Policy > IT policies**.
3. Select the check boxes for the IT policies you want to delete.
4. Click .
5. Click **Delete**.

Export IT policies

You can export IT policies to an .xml file for auditing purposes.

Note:

Profiles that are associated with IT policies are not exported.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > IT policies**.
3. Select the check boxes for the IT policies you want to export.
4. Click .
5. Click **Next**.
6. Click **Export**.

Sending certificates to devices using profiles

You can send certificates to devices using the following profiles available in the Policies and Profiles library:

Profile	Description
CA certificate	CA certificate profiles specify a CA certificate that devices can use to trust the identity associated with any client or server certificate that has been signed by that CA.
User credential	User credential profiles send certificates to devices in the following ways: • They can specify a connection to your organization's PKI software to send client certificates to devices. • They can allow you to manually upload certificates in BlackBerry UEM.
SCEP	SCEP profiles specify how devices connect to, and obtain client certificates from, your organization's CA using a SCEP service.

For BlackBerry Dynamics, to use certificates sent by profiles, you must select "Allow BlackBerry Dynamics apps to use user certificates, SCEP profiles, and user credential profiles" in the settings for the app.

Choosing profiles to send client certificates to devices

You can use different types of profiles to send client certificates to devices. The type of profile that you choose depends on how your organization uses certificates and the types of devices that your organization supports. Consider the following guidelines:

- To use SCEP profiles, you must have a CA that supports SCEP.
- If you have set up a connection between BlackBerry UEM and your organization's PKI solution, use user credential profiles to send certificates to devices. You can connect directly to an Entrust CA or OpenTrust CA.

- To use client certificates for Wi-Fi, VPN, and mail server authentication, you must associate the certificate profile with a Wi-Fi, VPN, or email profile.
- Shared certificate profiles and certificates that you add to user accounts do not keep the private key private because you must have access to the private key. Connecting to a CA using SCEP or user credential profiles is more secure because the private key is sent only to the device that the certificate was issued to.

Sending CA certificates to devices

You might need to send CA certificates to devices if your organization uses S/MIME or if the devices use certificate-based authentication to connect to a network or server in your organization's environment.

When you send a CA certificate to a device, the device trusts the identity associated with any client or server certificate signed by the CA. When the certificate for the CA that signed your organization's network and server certificates is stored on devices, the devices can trust your networks and servers when they make secure connections. When the CA certificate that signed your organization's S/MIME certificates is stored on devices, the devices can trust the sender's certificate when a secure email message is received.

Multiple CA certificates that are used for different purposes can be stored on a device. You can use CA certificate profiles to send CA certificates to devices.

Create a CA certificate profile

Before you begin: You must obtain the CA certificate file that you want to send to devices.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Certificates > CA certificate**.
3. Click +.
4. Type a name and description for the profile. Each CA certificate profile must have a unique name. Some names (for example, ca_1) are reserved.
5. In the **Certificate file** field, click **Browse** to locate the certificate file.
6. Click **Add**.

Using SCEP to send client certificates to devices

You can use SCEP profiles to specify how Windows 10 devices obtain client certificates from your organization's CA through a SCEP service. SCEP is an IETF protocol that simplifies the process of enrolling client certificates to a large number of devices without any administrator input or approval required to issue each certificate. Devices can use SCEP to request and obtain client certificates from a SCEP-compliant CA that is used by your organization. The CA that you use must support challenge passwords. The CA uses challenge passwords to verify that the device is authorized to submit a certificate request.

Depending on the device capabilities and activation type, devices can use the client certificates obtained using SCEP for certificate-based authentication from the browser or to connect to a work Wi-Fi network, work VPN, or work mail server.

Note: If your organization uses an Entrust CA or OpenTrust CA, SCEP profiles are not supported for Windows 10 devices.

Create a SCEP profile

The required profile settings vary for each device type and depend on the SCEP service configuration in your organization's environment.

Note: If you want to use a SCEP profile to distribute OpenTrust client certificates to devices, you must apply a hotfix to your OpenTrust software. For more information, contact your OpenTrust support representative and reference support case SUPPORT-798.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Certificates > SCEP**.
3. Click +.
4. Type a name and description for the profile. Each certificate profile must have a unique name.
5. In the **URL** field, type the URL for the SCEP service. The URL should include the protocol, FQDN, port number, and SCEP path.
6. In the **Instance name** field, type the instance name for the CA.
7. In the **Certification authority connection** drop-down list, perform one of the following actions:
   - To use an Entrust connection that you configured, click the appropriate connection. In the **Profile** drop-down list, click a profile. Specify the values for the profile.
   - To use an OpenTrust connection that you configured, click the appropriate connection. In the **Profile** drop-down list, click a profile. Specify the values for the profile.
     - The following settings in the SCEP profile do not apply to OpenTrust client certificates: Key usage, Extended key usage, Subject, and SAN.
   - To use another CA, click **Generic**. In the **SCEP challenge type** drop-down list, select **Static** or **Dynamic** and specify the required settings for the challenge type.

     Note: For Windows devices, only static passwords are supported.
8. Optionally, clear the check box for any device type that you do not want to configure the profile for.
9. For each device type that you want to configure in your organization, perform the following actions:
   a) Click the tab for a device type.
   b) Configure the appropriate values for each profile setting to match the SCEP service configuration in your organization's environment.
10. Click **Add**.

After you finish: If devices use the client certificate to authenticate with a work Wi-Fi network, work VPN, or work mail server, associate the SCEP profile with a Wi-Fi, VPN, or email profile.

Setting up work email for devices

You can use email profiles to specify how devices connect to your organization's mail server and synchronize email messages, calendar entries, and organizer data using Exchange ActiveSync or IBM Notes Traveler.

If you want to use Exchange ActiveSync, you should note the following:

- If you enable S/MIME, you can use other profiles to allow devices to automatically retrieve S/MIME certificates and check certificate status.

You can also use IMAP/POP3 email profiles to specify how Windows devices connect to IMAP or POP3 mail servers and synchronize email messages.

Create an email profile

The required profile settings vary for each device type and depend on the mail server used in your organization's environment.

Before you begin:

- If you use certificate-based authentication between devices and your mail server, you must create a CA certificate profile and assign it to users. You must also make sure that devices have a trusted client certificate.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Email, calendar and contacts > Email**.
3. Click +.
4. Type a name and description for the profile.
5. If necessary, type the domain name of the mail server. If the profile is for multiple users who may be in different Microsoft Active Directory domains, you can use the `%UserDomain%` variable.
6. In the **Email address** field, perform one of the following actions:
   - If the profile is for one user, type the email address of the user.
   - If the profile is for multiple users, type `%UserEmailAddress%`.
7. Type the host name or IP address of the mail server.
8. In the **Username** field, perform one of the following actions:
   - If the profile is for one user, type the username.
   - If the profile is for multiple users, type `%UserName%`.
   - If the profile is for multiple users in an IBM Notes Traveler environment, type `%UserDisplayName%`.
9. If you configured server groups to direct BlackBerry Secure Gateway traffic or BlackBerry Gatekeeping Service traffic to a specific regional connection to the BlackBerry Infrastructure, in the **BlackBerry Secure Gateway Service server group** drop-down list, click the appropriate server group.
10. Click the tab for each device type in your organization and configure the appropriate values for each profile setting. For details about each profile setting, see Email profile settings.
11. Click **Add**.

After you finish: If necessary, rank profiles.

Create an IMAP/POP3 email profile

The required profile settings vary for each device type and depend on the settings that you select.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Email, calendar and contacts > IMAP/POP3 email**.
3. Click +.
4. Type a name and description for the profile.
5. In the **Email type** field, select the type of email protocol.
6. In the **Email address** field, perform one of the following actions:
   - If the profile is for one user, type the email address of the user.
   - If the profile is for multiple users, type `%UserEmailAddress%`.
7. In the **Incoming mail settings** section, type the host name or IP address of the mail server for receiving mail.
8. If necessary, type the port for receiving mail.
9. In the **Username** field, perform one of the following actions:
   - If the profile is for one user, type the username.
   - If the profile is for multiple users, type `%UserName%`.
10. In the **Outgoing mail settings** section, type the host name or IP address of the mail server for sending mail.
11. If necessary, type the port for sending mail.
12. If necessary, select **Authentication required for outgoing mail** and specify the credentials used for sending mail.

13. Click the tab for each device type in your organization and configure the appropriate values for each profile setting. For details about each profile setting, see IMAP/POP3 email profile settings.
14. Click **Add**.

Using Exchange Gatekeeping

Your organization can use the BlackBerry Gatekeeping Service to control which devices can access Exchange ActiveSync.

To use gatekeeping in BlackBerry UEM, you must complete the following tasks:

- Create a gatekeeping configuration. In the configuration content, see Controlling which devices can access Exchange ActiveSync.
- Create a gatekeeping profile

When your organization uses the BlackBerry Gatekeeping Service, any device that is not whitelisted for Microsoft Exchange is reported in the BlackBerry UEM Restricted Exchange ActiveSync devices list.

If you add a user account and assign a gatekeeping profile, all previously blocked, quarantined, or manually allowed devices related to the user account appear in the Restricted Exchange ActiveSync devices list.

Allow a device to access Microsoft ActiveSync

If BlackBerry UEM cannot obtain an Exchange ActiveSync ID from a device, it is not added to the allowed list for Microsoft Exchange. You can manually add these devices to the allowed list from the Restricted Exchange ActiveSync devices list. For example, if an Android device is activated using the MDM activation type, BlackBerry UEM is not able to obtain an Exchange ActiveSync ID and you must manually whitelist the device in the Restricted Exchange ActiveSync devices list.

1. On the menu bar, click **Users > Exchange gatekeeping**.
2. Search for a device.
3. In the **Action** column, click ✓.

Block a device from accessing Microsoft ActiveSync

You can manually block a previously allowed device from accessing Microsoft ActiveSync. Blocking a device prevents a user from retrieving email messages and other information from the Microsoft Exchange Server on the device.

1. On the menu bar, click **Users**.
2. Click **Exchange gatekeeping**.
3. Search for a device.
4. In the **Action** column, click ⊘.

Verifying that a device is allowed to access work email and organizer data

When your organization uses BlackBerry Gatekeeping Service to control which devices can access work email and organizer data from Exchange ActiveSync, at least one gatekeeping server is configured on an email profile. When the email profile with gatekeeping configured is assigned to a user account, you can verify the connection status between a device and Exchange ActiveSync. You can locate the status by looking at the device details page, in the IT policy and profiles section. The following statuses display in the device details beside the email profile.

Status	Description
Unknown	A status of Unknown is displayed when BlackBerry UEM cannot determine the ID of the device. The device is listed in the Restricted device list and must be manually added to the allow list.
Connection pending	A status of Connection pending is displayed when BlackBerry UEM knows the ID of the device and the device is queued waiting to be added to the allow list.
Connection allowed	A status of Connection allowed is displayed when BlackBerry UEM knows the ID of the device and the device is on the allow list.

Verify that a device is allowed

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of a user account.
4. Select the tab for the device that you want to verify.
5. In the **IT policy and profiles** section, if the device is allowed, **Connection allowed** is displayed beside the email profile.

Creating a gatekeeping profile

If you configured the BlackBerry Gatekeeping Service, you need to create a gatekeeping profile and assign it to user accounts, user groups, or device groups. The gatekeeping profile allows you to select the Microsoft Exchange servers for automatic gatekeeping.

Create a gatekeeping profile

If you use automatic gatekeeping, create a gatekeeping profile.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Email, calendar and contacts > Gatekeeping**.
3. Click +.
4. Type a name and description for the profile.
5. Click **Select servers**.
6. Select one or more servers and click →.
7. Click **Save**.

Setting up work VPNs for devices

You can use a VPN profile to specify how Windows 10 devices connect to a work VPN. You can assign a VPN profile to user accounts, user groups, or device groups.

Device	Apps and network connections
Windows 10	• You can configure VPN profiles to allow apps to connect to your organization's network. In the VPN profile, you can specify a list of apps that must use the VPN.

Create a VPN profile

The required profile settings vary for each device type and depend on the VPN connection type and authentication type that you select.

Note: Some devices may be unable to store the xAuth password. For more information, visit support.blackberry.com/kb to read KB30353.

Before you begin:

- If devices use certificate-based authentication for work VPN connections, create a CA certificate profile and assign it to user accounts, user groups, or device groups. To send client certificates to devices, create a user credential, SCEP, or shared certificate profile to associate with the VPN profile.
- The proxy server for Windows 10 devices is configured in the VPN profile.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > VPN**.
3. Click +.
4. Type a name and description for the VPN profile. This information is displayed on devices.
5. Optionally, clear the check box for any device type that you do not want to configure the profile for.
6. Perform the following actions:
   a) Click the tab for a device type.
   b) Configure the appropriate values for each profile setting to match the VPN configuration in your organization's environment. If your organization requires that users provide a username and password to connect to the VPN and the profile is for multiple users, in the **Username** field, type `%UserName%`.

   For details about each profile setting, see VPN profile settings.
7. Repeat step 5 for each device type in your organization.
8. Click **Add**.

Enabling per-app VPN

You can set up per-app VPN for Windows 10 devices to specify which apps on devices must use a VPN for their data in transit. Per-app VPN helps decrease the load on your organization's VPN by enabling only certain work traffic to use the VPN (for example, accessing application servers or webpages behind the firewall).

For Windows 10 devices, apps are added to the "App trigger list" setting in the VPN profile.

Setting up work Wi-Fi networks for devices

You can use a Wi-Fi profile to specify how devices connect to a work Wi-Fi network behind the firewall. You can assign a Wi-Fi profile to user accounts, user groups, or device groups.

Device	Apps and network connections
Windows	Work and personal apps can use the Wi-Fi profiles stored on the device to connect to your organization's network.

Create a Wi-Fi profile

The required profile settings vary for each device type and depend on the Wi-Fi security type and authentication protocol that you select.

Before you begin:

- If devices use certificate-based authentication for work Wi-Fi connections, create a CA certificate profile and assign it to user accounts, user groups, or device groups. To send client certificates to devices, create a SCEP, shared certificate, or user credential profile to associate with the Wi-Fi profile.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > Wi-Fi**.
3. Click +.
4. Type a name and description for the Wi-Fi profile. This information is displayed on devices.
5. In the **SSID** field, type the network name of a Wi-Fi network.
6. If the Wi-Fi network does not broadcast the SSID, select the **Hidden network** check box.
7. Optionally, clear the check box for any device type that you do not want to configure the profile for.
8. Perform the following actions:
   a) Click the tab for a device type.
   b) Configure the appropriate values for each profile setting to match the Wi-Fi configuration in your organization's environment. If your organization requires that users provide a username and password to connect to the Wi-Fi network and the profile is for multiple users, in the **Username** field, type `%UserName%`.

   For details about each profile setting, see Wi-Fi profile settings.
9. Repeat step 7 for each device type in your organization.
10. Click **Add**.

Enforcing compliance rules for devices

You can use compliance profiles to encourage users to follow your organization’s standards for the use of devices. A compliance profile defines the device conditions that are not acceptable in your organization. For example, you can choose to disallow devices that are jailbroken, rooted, or have an integrity alert due to unauthorized access to the operating system.

A compliance profile specifies the following information:

- Conditions that would make a device non-compliant
- Email messages and device notifications that users receive if they violate the compliance conditions
- Actions that are taken if users do not correct the issue, including limiting a user’s access to the organization's resources, deleting work data from the device, or deleting all data from the device

BlackBerry UEM includes a Default compliance profile. The Default compliance profile does not enforce any compliance conditions. To enforce compliance rules, you can change the settings of the Default compliance profile or you can create and assign custom compliance profiles. Any user accounts that are not assigned a custom compliance profile are assigned the Default compliance profile.

Create a compliance profile

Before you begin:

- If you want to send an email notification to users when their devices are not compliant, edit the default compliance email, or create a new email template. For more information, see Create a template for compliance email notifications.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Compliance > Compliance**.
3. Click +.
4. Type a name and description for the compliance profile.
5. If you want to send a notification message to users when their devices become non-compliant, perform any of the following actions:
   - In the **Email sent when violation is detected** drop-down list, select an email template. To see the default compliance email, click Settings > General settings > Email templates.
   - In the **Enforcement interval** drop-down list, select how often BlackBerry UEM checks for compliance.
   - Expand **Device notification sent out when violation is detected**. Edit the message if necessary.

   If you want to use variables to populate notifications with user, device, and compliance information, see Variables. You can also define and use your own custom variables using the management console. For more information, see Custom variables.
6. Click the tab for each device type in your organization and configure the appropriate values for each profile setting. For details about each profile setting, see Compliance profile settings.
7. Click **Add**.

After you finish: If necessary, rank profiles.

Windows: Compliance profile settings

See Common: Compliance profile settings for descriptions of the possible actions if you select a compliance rule.

Windows: Compliance profile setting	Description
Required app is not installed	This setting creates a compliance rule to ensure that devices have required apps installed.
Restricted OS version is installed	This setting creates a compliance rule to ensure that devices do not have a restricted OS version installed as specified in this setting. You can select the restricted OS versions.
Restricted device model detected	This setting creates a compliance rule to restrict device models as specified in this setting. Possible values: • Allow selected device models • Do not allow selected device models You can select the devices models that are allowed or restricted.
Device out of contact	This setting creates a compliance rule to ensure that devices are not out of contact with BlackBerry UEM for more than a specified amount of time.

Windows: Compliance profile setting	Description
BlackBerry Dynamics library version verification	This setting creates a compliance rule that allows you to select the BlackBerry Dynamics library versions that cannot be activated. You can select the blocked library versions.
BlackBerry Dynamics connectivity verification	This setting creates a compliance rule to ensure that BlackBerry Dynamics apps are not out of contact with BlackBerry UEM for more than a specified amount of time. The enforcement action is applied to BlackBerry Dynamics apps.
Antivirus signature	This setting creates a compliance rule to ensure that devices have an antivirus signature enabled.
Antivirus status	This setting creates a compliance rule to ensure that devices have antivirus software enabled.
Firewall status	This setting creates a compliance rule to ensure that devices have a firewall enabled.
Encryption status	This setting creates a compliance rule to ensure that devices require encryption.
Windows update status	This setting creates a compliance rule to ensure that devices allow BlackBerry UEM to install Windows OS updates or notify users of required updates.
Restricted app is installed	This setting creates a compliance rule to ensure that devices do not have restricted apps installed. To restrict apps, see Add an app to the restricted app list.
Grace period expired	This setting creates a compliance rule to specify actions that occur if the attestation grace period has expired.
Attestation Identity Key not present	This setting creates a compliance rule to specify actions that occur if an AIK is not present on the device.
Data Execution Prevention Policy is disabled	This setting creates a compliance rule to specify actions that occur if the DEP policy is disabled on the device.
BitLocker is disabled	This setting creates a compliance rule to specify actions that occur if BitLocker is disabled on the device.
Secure Boot is disabled	This setting creates a compliance rule to specify actions that occur if Secure Boot is disabled on the device.
Code integrity is disabled	This setting creates a compliance rule to specify actions that occur if the Code Integrity feature is disabled on the device.
Device is in safe mode	This setting creates a compliance rule to specify actions that occur if the device is in safe mode.

Windows: Compliance profile setting	Description
Device is in Windows preinstallation environment	This setting creates a compliance rule to specify actions that occur if the device is in the Windows preinstallation environment.
Early launch antimalware driver is not loaded	This setting creates a compliance rule to specify actions that occur if the early launch antimalware driver is not loaded.
Virtual Secure Mode is disabled	This setting creates a compliance rule to specify actions that occur if Virtual Secure Mode is disabled.
Boot debugging is enabled	This setting creates a compliance rule to specify actions that occur if boot debugging is enabled.
OS kernel debugging is enabled	This setting creates a compliance rule to specify actions that occur if OS kernel debugging is enabled.
Test signing is enabled	This setting creates a compliance rule to specify actions that occur if test signing is enabled.
Boot manager revision list is not the expected version	This setting creates a compliance rule to specify actions that occur if the boot manager revision list is not the expected version.
Code Integrity revision list is not the expected version	This setting creates a compliance rule to specify actions that occur if the code integrity revision list is not the expected version.
Code Integrity policy hash is present and is not an allowed value	This setting creates a compliance rule to specify actions that occur if the code integrity policy hash is present and is not an allowed value.
Custom Secure Boot configuration policy hash is present and is not an allowed value	This setting creates a compliance rule to specify actions that occur if the Custom Secure Boot configuration policy hash is present and is not an allowed value.
PCR value is not an allowed value	This setting creates a compliance rule to specify actions that occur if the PCR value is not an allowed value.

Setting up Windows Information Protection for Windows 10 devices

You can set up Windows Information Protection (WIP) for Windows 10 devices when you want to:

- Separate personal and work data on devices and be able to wipe only work data
- Prevent users from sharing work data outside of protected work apps or with people outside of your organization
- Protect data even if it is moved to or shared on other devices, such as a USB key
- Audit user behavior and take appropriate actions to prevent data leaks

When you set up WIP for devices, you specify the apps that you want to protect with WIP. Protected apps are trusted to create and access work files, while unprotected apps can be blocked from accessing work files. You can choose the level of protection for protected apps based on how you want users to behave when they share work data. When WIP is enabled, all data sharing practices are audited. For more information about WIP, visit https://technet.microsoft.com/itpro/windows/keep-secure/protect-enterprise-data-using-wip.

The apps that you specify can be enlightened or unenlightened for enterprise. Enlightened apps can create and access work and personal data. Unenlightened apps can only create and access work data. For more information about enlightened and unenlightened apps, visit https://technet.microsoft.com/itpro/windows/keep-secure/enlightened-microsoft-apps-and-wip.

Create a Windows Information Protection profile

1. On the menu bar, click **Policies and Profiles**.
2. Click **Protection > Windows Information Protection**.
3. Click +.
4. Type a name and description for the profile.
5. Configure the appropriate values for each profile setting. For details about each profile setting, see Windows 10: Windows Information Protection profile settings.
6. Click **Add**.

Windows 10: Windows Information Protection profile settings

Windows 10: Windows Information Protection profile setting	Description
Windows Information Protection settings	This setting specifies whether Windows Information Protection is enabled and the level of enforcement. When this setting is set to "Off," data is not encrypted and audit logging is turned off. When this setting is set to "Silent," data is encrypted and any attempts to share protected data are logged. When this setting is set to "Override," data is encrypted, the user is prompted when they attempt to share protected data, and any attempts to share protected data are logged. When this setting is set to "Block," data is encrypted, users cannot share protected data, and any attempts to share protected data are logged. Possible values: • Off • Silent • Override • Block The default value is "Off."
Enterprise protected domain names	This setting specifies the work network domain names that your organization uses for its user identities. You can separate multiple domains with pipes (|). The first domain is used as a string to tag files that are protected by apps that use WIP. For example, `example.com|example.net`.

Windows 10: Windows Information Protection profile setting	Description
Data recovery certificate file (.der, .cer)	This setting specifies the data recovery certificate file. The file that you specify must be a PEM encoded or DER encoded certificate with a .der or .cer file extension. You use the data recovery certificate file to recover files that were locally protected on a device. For example, if your organization wants to recover data protected by WIP from a device. For information on creating a data recovery certificate, see the Microsoft Windows Information Protection documentation.
Remove the Windows Information Protection settings when a device is removed from BlackBerry UEM	This setting specifies whether to revoke WIP settings when a device is deactivated. When WIP settings are revoked, the user can no longer access protected files.
Show Windows Information Protection overlays on protected files and apps that can create enterprise content	This setting specifies whether an overlay icon is shown on file and app icons to indicate whether a file or app is protected by WIP.
Work network IP range	This setting specifies the range of IP addresses at work to which an app protected with WIP can share data. Use a dash to denote a range of addresses. Use a comma to separate addresses.
Work network IP ranges are authoritative	This setting specifies if only the work network IP ranges are accepted as part of the work network. When this setting is enabled, no attempts are made to discover other work networks. By default, the option is not selected.
Enterprise internal proxy servers	This setting specifies the internal proxy servers that are used when connecting to work network locations. These proxy servers are only used when connecting to the domain listed in the Enterprise cloud resources setting.
Enterprise cloud resources	This setting specifies the list of enterprise resource domains hosted in the cloud that need to be protected. Data from these resources are considered enterprise data and protected.
Cloud resources domain	This setting specifies the domain name.
Paired proxy	This setting specifies a proxy that is paired with a cloud resource. Traffic to the cloud resource will be routed through the enterprise network via the denoted proxy server (on port 80). A proxy server used for this purpose must also be configured in the Enterprise internal proxy servers field.

Windows 10: Windows Information Protection profile setting	Description
Enterprise proxy servers	This setting specifies the list of internet proxy servers.
Enterprise proxy servers are authoritative	This setting specifies whether the client should accept the configured list of proxies and not try to detect other enterprise proxies.
Neutral resources	This setting specifies the domains that can be used for work or personal resources.
Enterprise network domain names	This setting specifies a comma-separated list of domains that comprise the boundaries of the enterprise. Data from one of these domains that is sent to a device will be considered enterprise data and protected. These locations will be considered a safe destination for enterprise data to be shared to. For example, `example.com`, `example.net`.
Desktop app payload code	Specify the desktop app keys and values used to configure application launch restrictions on Windows 10 devices. You must use the keys defined by Microsoft for the payload type that you want to configure. To specify the apps, copy the XML code from the AppLocker policy .xml file and paste it in this field. When you copy the text, copy only the elements as shown in the following code sample: `<RuleCollection Type="Appx" EnforcementMode="Enabled"> <FilePublisherRule Id="0c9781aa-bf9f-4352 -b4ba-64c25f36f558" Name="WordMobile" Description="" UserOrGroupSid="S-1-1-0" Action="Allow"> <Conditions> <FilePublisherCondition PublisherName="CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" ProductName="Microsoft.Office.Word" BinaryName="*"> <BinaryVersionRange LowSection="*" HighSection="*" /> </FilePublisherCondition> </Conditions> </FilePublisherRule> </RuleCollection>` For more information about using AppLocker, see https://technet.microsoft.com/en-us/itpro/windows/keep-secure/administer-applocker.

Windows 10: Windows Information Protection profile setting	Description

Universal Windows Platform app payload code	Specify the Universal Windows Platform app keys and values used to configure WIP on Windows 10 devices. You must use the keys defined by Microsoft for the payload type that you want to configure.
	
	To specify the apps, copy the XML code from the AppLocker policy .xml file and paste it in this field. When you copy the text, copy only the elements as shown in the following code sample:
	
	`<RuleCollection Type="Exe" EnforcementMode="Enabled">`
	`<FilePathRule Id="921cc481-6e17-4653-8f75-050b80acca20"`
	`Name="(Default Rule)`
	`All files" Description="" UserOrGroupSid="S-1-1-0"`
	`Action="Allow">`
	`<Conditions>`
	`<FilePathCondition Path="*" />`
	`</Conditions>`
	`</FilePathRule>`
	`<FilePublisherRule Id="ddd0bc90-`
	`dada-4002-9e2f-0fc68e1f6af0" Name="WORDPAD.EXE,`
	`from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON,`
	`C=US" Description=""`
	`UserOrGroupSid="S-1-1-0" Action="Deny">`
	`<Conditions>`
	`<FilePublisherCondition PublisherName="O=MICROSOFT`
	`CORPORATION,`
	`L=REDMOND, S=WASHINGTON, C=US" ProductName="*"`
	`BinaryName="WORDPAD.EXE">`
	`<BinaryVersionRange LowSection="*" HighSection="*" />`
	`</FilePublisherCondition>`
	`</Conditions>`
	`</FilePublisherRule>`
	`<FilePublisherRule Id="c8360d06-f651-4883-`
	`abdd-9c3a95a415ff" Name="NOTEPAD.EXE,`
	`from O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON,`
	`C=US" Description=""`
	`UserOrGroupSid="S-1-1-0" Action="Allow">`
	`<Conditions>`
	`<FilePublisherCondition PublisherName="O=MICROSOFT`
	`CORPORATION,`
	`L=REDMOND, S=WASHINGTON, C=US" ProductName="*"`
	`BinaryName="NOTEPAD.EXE">`
	`<BinaryVersionRange LowSection="*" HighSection="*" />`
	`</FilePublisherCondition>`
	`</Conditions>`
	`</FilePublisherRule>`
	`</RuleCollection>`
	
	For more information about using AppLocker, see https://technet.microsoft.com/en-us/itpro/windows/keep-secure/administer-applocker.

Windows 10: Windows Information Protection profile setting	Description
Associated VPN profile	This setting specifies the VPN profile that a device uses to connect to a VPN when using an app protected by WIP. This setting is valid only if "Use a VPN profile" is selected for the "Secure connection used with WIP."
Collect device audit logs	This setting specifies whether to collect device audit logs.

Managing Windows 10 devices that are enrolled in UEM and SCCM

You can choose which device management features that you want to manage through either BlackBerry UEM or Microsoft SCCM. UEM supports the following enrollment scenarios:

- The device is already managed with SCCM, and you want to enroll the device with UEM.
- The device is already managed with UEM, and you want to enroll the device with SCCM.
- The device is not yet managed by either SCCM or UEM. If you want the device to remain unmanaged but you also want to allow access to the corporate intranet, email, and contacts, consider enrolling the device with BlackBerry Access for Windows to allow access to the corporate content.

Configuring policies in SCCM

The table below lists some of the resources that are available from Microsoft to help you manage devices using SCCM.

Item	Resource
Microsoft System Center Configuration Manager documentation	https://docs.microsoft.com/en-us/sccm/
Configuration items for devices managed with the SCCM client	https://docs.microsoft.com/en-us/sccm/compliance/deploy-use/configuration-items-for-devices-managed-with-the-client
Managing access to services in SCCM	https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/manage-access-to-services
Setting device compliance policies in SCCM	https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/device-compliance-policies
Managing apps in SCCM	https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/management-tasks-applications
MDM Migration Analysis Tool (MMAT)	https://github.com/WindowsDeviceManagement/MMAT

Item	Resource
Microsoft Configuration service provider (CSP) reference	https://docs.microsoft.com/en-us/windows/client-management/mdm/configuration-service-provider-reference

Configuring UEM to manage apps for Windows 10 devices

You can configure BlackBerry UEM to manage apps for Windows 10 devices. You can add apps that are synchronized with the Windows Store for Business or add internal work apps in your organization. Users can easily find apps that are assigned to them from the BlackBerry UEM App Catalog app. For BlackBerry Dynamics apps, you can also specify the configuration settings so that users do not need to manually configure them.

Follow these steps to configure BlackBerry UEM to manage apps for Windows 10 devices:

Step	Action
1	Connect BlackBerry UEM to Microsoft Azure
2	Specify the shared network location for storing internal apps
3	Add a Windows 10 app to the app list

Connecting BlackBerry UEM to Microsoft Azure

Microsoft Azure is the Microsoft cloud computing service for deploying and managing applications and services.

Connecting BlackBerry UEM to Azure provides your organization with the following features:

- Connect BlackBerry UEM to Azure Active Directory and create directory user accounts in BlackBerry UEM by searching for and importing user data from the company directory. Directory users can use their directory credentials to access BlackBerry UEM Self-Service. If you assign an administrative role to directory users, the users can also use their directory credentials to log into the management console.
- Manage Windows 10 apps in BlackBerry UEM

BlackBerry UEM supports configuring only one Azure tenant. To connect BlackBerry UEM to Azure, you perform the following actions:

Step	Action
1	Create a Microsoft Azure account.
2	If your organization uses Azure Active Directory, configure BlackBerry UEM Cloud to synchronize with Azure Active Directory.
3	If your organization uses an on-premises Microsoft Active Directory and you want to use BlackBerry UEM to deploy apps managed by Microsoft Intune or manage Windows 10 apps, Synchronize Microsoft Active Directory with Microsoft Azure.

Step	Action
4	Create enterprise applications in Azure to allow BlackBerry UEM Cloud to connect to Microsoft Intune and the Windows Store for Business.
5	Configure BlackBerry UEM to synchronize with the Windows Store for Business.

Create a Microsoft Azure account

To deploy apps protected by Microsoft Intune to iOS and Android devices or manage Windows 10 apps in BlackBerry UEM, you must have a Microsoft Azure account and authenticate BlackBerry UEM with Azure.

Complete this task if your organization doesn't have a Microsoft Azure account.

1. Go to https://azure.microsoft.com and click **Free account**, then follow the prompts to create the account.
   You are required to provide credit card information to create the account.
2. Sign in to the Azure management portal at https://portal.azure.com and log in with the username and password you created when you signed up.

Synchronize Microsoft Active Directory with Microsoft Azure

To allow Windows 10 users to install online apps or to send apps protected by Microsoft Intune to iOS and Android devices, users must exist in the Microsoft Azure Active Directory. You must synchronize users and groups between your on-premises Active Directory and Azure Active Directory using Microsoft Azure Active Directory Connect. For more information, visit https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect.

Before you begin: Create a Microsoft Azure account

1. Download Azure AD Connect from http://www.microsoft.com/en-us/download/details.aspx?id=47594.
2. Install the Azure AD Connect software.
3. Configure Azure AD Connect to connect your on-premises Active Directory with the Azure Active Directory.

After you finish: Create an enterprise endpoint in Azure

Create an enterprise endpoint in Azure

To provide BlackBerry UEM access to Microsoft Azure, you must create an enterprise endpoint within Azure. The enterprise endpoint allows BlackBerry UEM to authenticate with Microsoft Azure. For more information, see https://docs.microsoft.com/en-us/azure/active-directory/active-directory-app-registration.

Before you begin: Synchronize Microsoft Active Directory with Microsoft Azure

1. Log in to the Azure portal.
2. Go to **Microsoft Azure > Azure Active Directory > App registrations**.
3. Click **Endpoints**.
4. Copy the **OAUTH 2.0 TOKEN ENDPOINT** value and paste it to a text file.
   This is the **OAUTH 2.0 token endpoint** required in BlackBerry UEM.
5. Close the **Endpoints** list and select **New application registration**.
6. Enter the following information for your app:

Field	Setting
Name	<A name for your application>
Application type	Web app / API
Sign-on URL	Any valid URL **Note:** If you don't have a registered domain you can use: http://localhost/

7. Click **Create**.
8. Click on the app you just created.
9. Copy the **Application ID** of your application and paste it to a text file.
   This is the **Client ID** required in BlackBerry UEM.
10. If you are creating the application to use Microsoft Intune, click **Required permissions** in the **Settings** menu. Perform the following steps:
    a) Click **Add**.
    b) Click **Select an API**.
    c) Select **Microsoft Graph**.
    d) Click **Select**.
    e) Scroll down in the permissions list and under **Delegated Permissions**, set the following permissions for Microsoft Intune:
       - Read and write Microsoft Intune apps (preview)
       - Read all users' basic profile
       - Read all groups
    f) Click **Select**.
    g) Click **Done**.
    h) In the **Required permissions** pane, click **Grant Permissions**.
       Note: You must be a global administrator to grant permissions.
    i) When you are prompted, click **Yes** to grant permissions for all accounts in the current directory.
    You can use the default permissions if you are creating the app to connect to the Windows Store for Business.
11. Select **Keys** in the **Settings** menu. Perform the following steps:
    a) Enter a name for your key.
    b) Select a duration for your key.
    c) Click **Save**.
    d) Copy the value of your key.
       This is the **Client Key** that is required in BlackBerry UEM.

       Warning: If you do not copy the value of your key at this time, you will have to create a new key because the value is not displayed after you leave this screen.

After you finish:

- Configure BlackBerry UEM to synchronize with the Windows Store for Business

Configuring BlackBerry UEM to synchronize with the Windows Store for Business

If you want to manage Windows 10 apps, you must configure BlackBerry UEM to synchronize with the Windows Store for Business before you can add Windows 10 apps to the app list.

If you later remove the connection to the Windows Store for Business, all of the Windows 10 apps that have been synchronized to BlackBerry UEM will be removed and the apps will be unassigned from users and groups.

When you configure BlackBerry UEM to synchronize with the Windows Store for Business, you perform the following actions:

Step	Action
1	Create a Microsoft Azure account.
2	If your organization uses an on-premises Microsoft Active Directory instead of Azure Active Directory, Synchronize Microsoft Active Directory with Microsoft Azure.
3	Create an enterprise application in Azure.
4	Configure BlackBerry UEM to synchronize with the Windows Store for Business.
5	Create an administrator for the Windows Store for Business.

Configure BlackBerry UEM to synchronize with the Windows Store for Business

Before you begin: Create a Microsoft Azure account.

1. Log in to the BlackBerry UEM management console.
2. Go to **Settings > App management > Windows 10 apps**.
3. Enter the information you copied from the Azure portal when you created the enterprise application in Azure.
   - **Client ID**: The Application ID generated by the Azure application registration
   - **Client key**: The client secret generated by the Azure application registration
   - **OAUTH 2.0 token endpoint**: The tenant specific OAuth endpoint URL for requesting authentication tokens
   - **Username**: The administrator username for BlackBerry UEM to access Intune
   - **Password**: The password for the username
4. Click **Next**.

After you finish: Create an administrator for the Windows Store for Business.

Create an administrator for the Windows Store for Business

To manage Windows 10 apps on devices, you must create an app catalog in the Windows Store for Business and synchronize the apps with BlackBerry UEM. To create the catalog in the Windows Store for Business, you must create at least one administrator account to log in to the store.

Before you begin:

- Create a Microsoft Azure account.
- Create an enterprise endpoint in Azure.
- Configure BlackBerry UEM to synchronize with the Windows Store for Business.

1. In the Microsoft Azure portal, go to **Microsoft Azure > Azure Active Directory > Users and groups > All users**.

2. Click **Add a user**.
3. On the screen, enter the required user information.
4. Click the arrow next to **Directory role** and select **Global administrator**, then click **OK**.
5. Create a password or select **Show Password** and copy the generated password.
6. Click **Create**.
7. Click **Azure Active Directory > Enterprise applications > All applications** and select the enterprise application you created.
8. Add the global administrator account you created as a user of the application.

Activate the app in the Windows Store for Business

Before you begin:

- Configure BlackBerry UEM to synchronize with the Windows Store for Business.
- Create an administrator for the Windows Store for Business

1. Log in to the Windows Store for Business using the Global Admin account you created.
2. Click **Settings** > **Management tool**.
3. Choose the app that you created to be the MDM tool you want to synchronize with the Windows Store for Business.
4. Click **Activate.**

Specify the shared network location for storing internal apps

Before you add internal apps to the available app list, you must specify a shared network location to store the app source files. To make sure that internal apps remain available, this network location should have a high availability solution and be backed up regularly. Also, do not create the shared network folder in the BlackBerry UEM installation folder because it will be deleted if you upgrade BlackBerry UEM.

Before you begin:

- Create a shared network folder to store the source files for internal apps on the network that hosts BlackBerry UEM.
- Verify that the service account for the computer that hosts BlackBerry UEM has read and write access to the shared network folder.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **App management**.
3. Click **Internal app storage**.
4. In **Network location** field, type the path of the shared network folder using the following format:

   \\<*computer_name*>\<*shared_network_folder*>

   The shared network path must be typed in UNC format (for example, \\ComputerName\Applications \InternalApps).
5. Click **Save**.

Add a Windows 10 app to the app list

To add Windows 10 apps to the app list, you must manage your app catalog in the Windows Store for Business and then synchronize the apps to BlackBerry UEM. When new apps are added to your app catalog, you can synchronize the apps with BlackBerry UEM right away or wait until BlackBerry UEM synchronizes automatically. BlackBerry UEM synchronizes the app catalog every 24 hours.

You can allow users to install offline or online apps from the Windows Store for Business app catalog. Offline apps are downloaded by BlackBerry UEM when you synchronize with the app catalog. Using offline apps is recommended because all management of these apps can be performed from BlackBerry UEM, and users can install them without connecting to the Windows Store for Business. After the apps are installed, devices receive updates to the apps from the Windows Store.

Online apps are downloaded directly from the Windows Store for Business. To be able to send required online apps to devices, instruct your users to add their work accounts to **Accounts used by other apps** in Windows 10.

Before you begin:

- Configure BlackBerry UEM to synchronize with the Windows Store for Business. For instructions, see the Configuration content

1. On the menu bar, click **Apps**.
2. Click  .
3. Click **Windows Store** > **10**.
4. Click **Synchronize apps**.

Allowing users to install online Windows 10 apps

To allow users to install online Windows 10 apps, the user must exist in your Microsoft Azure directory, and the user's email address in BlackBerry UEM must match the user's email address in Microsoft Azure AD. You can synchronize your directory to Microsoft Azure using Microsoft Azure AD Connect. For instructions, see the Configuration content.

Note: To be able to send required online apps to devices, instruct your users to add their work accounts to **Accounts used by other apps** in Windows 10.

Add an app category for a Windows 10 app

After you set a category for an app, you can filter apps in the app list by category and organize the apps in the work apps list on users' devices into categories. After a Windows 10 app has been synchronized to BlackBerry UEM, you can assign an app category to it.

Before you begin: Add a Windows 10 app to the app list.

1. On the menu bar, click **Apps**.
2. Click the app that you want to assign an app category to.
3. In the **Category** drop-down list, do one of the following:

Step	Description
Select a category for the app	**a.** In the drop-down list, select a category.

Step	Description
Create a category for the app	**a.** Type a name for the category. A "new category" message will appear in the drop-down list with the new category label beside it **b.** Press **Enter**. **c.** Press **Enter**.

4. Click **Save**.

App behavior on Windows 10 devices

App type	Behavior when apps are assigned to a user	Behavior when apps are unassigned from a user	Behavior when devices are removed from BlackBerry UEM
Offline Windows Store apps with a required disposition	• The apps are automatically installed on devices. Users cannot uninstall the apps.	• The apps are automatically removed from devices.	• The apps are automatically removed from devices.
Online Windows Store apps with a required disposition	• The apps are automatically installed on devices. Users cannot uninstall the apps.	• The apps are automatically removed from devices.	• The apps are automatically removed from devices.
Offline Windows Store apps with an optional disposition	• Users can choose whether to install the apps. • For offline apps, users install the app from the BlackBerry UEM App Catalog. • Not supported on Windows 10 Mobile devices.	• Users are not prompted to uninstall the apps.	• Users are not prompted to uninstall assigned apps.
Online Windows Store apps with an optional disposition	• Users can choose whether to install the apps. • For online apps, users install the app from the Windows Store app on their devices. • Not supported on Windows 10 Mobile devices.	• Users are not prompted to uninstall the apps.	• Users are not prompted to uninstall the apps.

App type	Behavior when apps are assigned to a user	Behavior when apps are unassigned from a user	Behavior when devices are removed from BlackBerry UEM
Internal apps with a required disposition	• Not supported	• Not supported	• Not supported
Internal apps with an optional disposition	• Not supported	• Not supported	• Not supported

Setting up network connections for BlackBerry Dynamics apps

BlackBerry Dynamics connectivity profiles define the network connections, Internet domains, IP address ranges, and app servers that devices can connect to when using BlackBerry Dynamics apps.

BlackBerry UEM includes a Default BlackBerry Dynamics connectivity profile with preconfigured settings. If no BlackBerry Dynamics connectivity profile is assigned to a user account or a user group that a user belongs to, BlackBerry UEM sends the Default BlackBerry Dynamics connectivity profile to a user's devices. BlackBerry UEM automatically sends a BlackBerry Dynamics connectivity profile to a device when a user activates it, when you update an assigned BlackBerry Dynamics connectivity profile, or when a different BlackBerry Dynamics connectivity profile is assigned to a user account or device.

Create a BlackBerry Dynamics connectivity profile

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > BlackBerrry Dynamics connectivity**
3. Click +.
4. Type a name and description for the profile.
5. Configure the appropriate values for the profile settings. For more information about each profile setting, see BlackBerry Dynamics connectivity profile settings.
6. To add an app server for a BlackBerry Dynamics app, see Add an app server to a BlackBerry Dynamics connectivity profile.
7. Click **Add**.

After you finish: If necessary, rank profiles.

Add an app server to a BlackBerry Dynamics connectivity profile

If you have a BlackBerry Dynamics app that is served from an app server or web server, you can specify the name of that server and the priority of the BlackBerry Proxy clusters used for communication with it.

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > BlackBerry Dynamics connectivity**.
3. Click the BlackBerry Dynamics connectivity profile that you want to add an app server to.
4. Click ✎.
5. Under **App servers**, click **Add**.
6. Select the BlackBerry Dynamics app that you want to add an app server for.
7. Click **Save**.
8. In the table for the app, click +.

9. In the **Server** field, specify the FQDN of the app server.
10. In the **Port** field, specify the port of the BlackBerry Proxy cluster that is used to access the server.
11. In the **Priority** drop-down list, specify the priority of the BlackBerry Proxy cluster that must be used to reach the domain.
12. In the **Primary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the primary cluster.
13. In the **Secondary BlackBerry Proxy cluster** drop-down list, specify the name of the BlackBerry Proxy cluster that you want to set as the secondary cluster.
14. Click **Save**.

BlackBerry Dynamics connectivity profile settings

BlackBerry Dynamics connectivity profile setting	Description
Infrastructure	
Domain	Specify the Internet domains that you want to allow access to. For example, `blackberry.com` allows access to any server in the blackberry.com domain. BlackBerry Dynamics apps are allowed to connect through your organization's firewall to any server in the listed domains and their subdomains.
Primary and Secondary BlackBerry Proxy Clusters	Specify the fully qualified domain name, port and priority of the BlackBerry Proxy clusters that must be used to reach the domain.
Default domains	
Domain	Specify the default allowed domains (for example, qa.blackberry.com). BlackBerry Dynamics apps may try to connect to an unqualified hostname like "portal" instead of using a fully qualified name like "portal.sales.xyzcorp.com". The domains in this list will be appended to unqualified hostnames to construct fully qualified names.
Additional servers	
Server	Specify the fully qualified domain name of any additional servers that BlackBerry Dynamics apps can connect to. Add servers to this list instead of using the "Allowed Domains" list if you want BlackBerry Dynamics apps to connect only to certain servers and not to every server in a domain.
IP address ranges	

BlackBerry Dynamics connectivity profile setting	Description
Range	Specify a range of IP addresses that BlackBerry Dynamics apps can access. Address ranges must be entered with a lower and upper bound address (for example, 192.168.2.0-192.168.2.255) or in IPv4 CIDR notation (for example, 192.168.2.0/24). For example: • Discrete addresses: Example: 192.168.2.0-192.168.2.255 • An entire subnet: Example: 192.168.2.0/24
App servers	If you have a BlackBerry Dynamics app that is served from an app server or web server, you can specify the name of the server and the priority of the BlackBerry Proxy clusters used for communication with it. For more information, see Add an app server to a BlackBerry Dynamics connectivity profile.

Remote management for Windows 10 devices

Send commands to devices over the wireless network to protect device data. You can also locate devices on a map and control which devices can access Exchange ActiveSync.

Sending commands to users and devices

You can send various commands over the wireless network to manage user accounts and devices. The list of commands that are available depends on the device type and activation type. You can send commands to a specific user or device, or you can send commands to multiple users and devices using bulk commands.

For example, you can use commands in the following circumstances:

- If a device is temporarily misplaced, you can send a command to lock the device or delete work data from the device.
- If you want to redistribute a device to another user in your organization, or if a device is lost or stolen, you can send a command to delete all data from the device.
- When an employee leaves your organization, you can send a command to the user's personal device to delete only the work data.
- If a user forgets the work space password, you can send a command to reset the work space password.

Send a command to a device

Before you begin:

If you want to set an expiry period for commands that delete data from devices in BlackBerry UEM, see Set an expiry time for commands.

1. On the menu bar, click **Users > Managed devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. Click the device tab.
5. In the **Manage device** window, select the command that you want to send to the device.

Send a bulk command

You can send a command to multiple user accounts or devices at the same time by selecting the users or devices from the user list and sending a bulk command.

Before you begin: If you want to set an expiry period for commands that delete data from devices, see Set an expiry time for commands.

1. On the menu bar, click **Users > Managed devices**.
2. If necessary, filter the user list.
3. Perform one of the following actions:
   - Select the check box at the top of the user list to select all users and devices in the list.
   - Select the check box for each user and device that you want to include. You can use Shift+click to select multiple users.
4. From the menu, click one of the following icons:

Icon	Description
	Locate devices You can select a maximum of 100 devices at a time. For more information, see Locate a device.
	Send email For more information, see Send an email to users.
	Send activation email For more information, see Send an activation email to multiple users.
	Add to user groups You can select a maximum of 200 devices at a time. For more information, see Add users to user groups.
	Export For more information, see Export the user list to a .csv file.
	Remove devices To use this bulk command, you must be a Security Administrator. You can select a maximum of 200 devices at a time. For more information, see Commands for Windows 10 devices.
	Update device information. For more information, see Commands for Windows 10 devices.
	Delete all device data To use this command, you must be a Security Administrator. You can select a maximum of 200 devices at a time. For more information, see Commands reference.
	Delete only work data To use this command, you must be a Security Administrator. You can select a maximum of 200 devices at a time. For more information, see Commands reference.
	Edit device ownership You can select a maximum of 100 devices at a time. For more information, see Change the device ownership label.

Icon	Description
	Change console passwords You can send a BlackBerry UEM Self-Service password to multiple users at one time. For more information, see Send a BlackBerry UEM Self-Service password to multiple users.

Set an expiry time for commands

When you send the "Delete all device data" or "Delete only work data" command to a device, the device must connect to BlackBerry UEM for the command to complete. If the device is unable to connect to BlackBerry UEM, the command remains in pending status and the device is not removed from BlackBerry UEM unless you manually remove it. Alternatively, you can configure BlackBerry UEM to automatically remove devices when the commands do not complete after a specified amount of time.

1. On the menu bar, click **Settings > General settings > Delete command expiry**.
2. For one or both of **Delete all device data** and **Delete only work data**, select **Automatically remove the device if the command has not completed**.
3. In the **Command expiration** field, type the number of days after which the command expires and the device is automatically removed from BlackBerry UEM.
4. Click **Save**.

Commands reference

The commands you can send to devices depends on the device type and activation type. Some commands can be sent to multiple devices at a time.

Commands for Windows 10 devices

Command	Description
Update device information	This command sends and receives updated device information. For example, you can send newly updated IT policy rules or profiles to a device, and receive updated information about a device such as OS version or battery level. To send this command to multiple devices, see Send a bulk command.
View device actions	This command displays any actions that are in progress on a device. For more information, see Viewing device actions.
View device report	This command displays detailed information about a device. You can export and save the device report on your computer. For more information, see View and save a device report.
Remove device	This command removes the device from BlackBerry UEM. The device may continue to receive email and other work data. To send this command to multiple devices, see Send a bulk command.

Command	Description
Delete only work data	This command deletes work data, including the IT policy, profiles, apps, and certificates that are on the device, and optionally, deletes the device from BlackBerry UEM. The user account is not deleted when you send this command. After you send this command, you are given the option of deleting the device from BlackBerry UEM. If the device is unable to connect to BlackBerry UEM, you can remove the device from BlackBerry UEM. If the device connects to BlackBerry UEM after you removed it, only the work data is deleted from the device, including the work space, if applicable. To send this command to multiple devices, see Send a bulk command.
Delete all device data	This command deletes all user information and app data that the device stores. It returns the device to factory defaults and optionally, deletes the device from BlackBerry UEM. After you send this command, you are given the option of deleting the device from BlackBerry UEM. If the device is unable to connect to BlackBerry UEM, you can remove the device from BlackBerry UEM. If the device connects to BlackBerry UEM after you removed it, only the work data is deleted from the device, including the work space, if applicable. To send this command to multiple devices, see Send a bulk command.
Restart desktop/ device	This command forces devices to restart.

Locate a device

You can locate Windows 10 devices (for example, if a device is lost or stolen).

Before you begin: Create and assign a location service profile.

1. On the menu bar, click **Users > Managed devices**.
2. Select the check box for each device that you want to locate.
3. Click .
4. Find the devices on the map using the following icons.
   - Current location:
   - Last known location:

   You can click or hover over an icon to display location information, such as latitude and longitude and when the location was reported (for example, 1 minute ago or 2 hours ago).

Managing Windows 10 device updates with BlackBerry UEM

In BlackBerry UEM, you can control Windows 10 PC and tablet updates using the following IT policies:

- **Update installation day**: Specify the day of the week when an update can occur.
- **Update installation hour**: Specify the hour of day when an update can occur.
- **Active hours start/end**: Specify the hours when a user is usually active so that Windows update reboots are not scheduled.
- **Delivery optimization mode**: Specify the delivery optimization mode and options for Windows updates so that updates are delivered in the most effective way over the network.

You might also set up compliance rules to prevent users from running unauthorized versions of Windows. You can set the actions to take when a compliance violation is detected (for example, prompt the user and, if the user is still non-compliant after a number of prompts, wipe the device).

For more information about IT policy rules see the BlackBerry UEM policy spreadsheet.

Example

If you want the marketing and sales teams to complete Windows updates after 17:00 on Wednesdays, you do the following:

- Create an IT policy for Windows devices that meets the following Windows update requirements:
  - Set the installation day to "Wednesday."
  - Set the installation hour to "17."
  - Set the start of active hours to "8."
  - Set the end of active hours to "17."
  - Any other options that you would like
- Assign the IT policy to the marketing and sales team group in UEM.

Deactivating devices

When you or a user deactivates a device, the connection between the device and the user account in BlackBerry UEM is removed. You can't manage the device, and the device is no longer displayed in the management console. The user can't access work data on the device.

You can deactivate a device using the "Delete all work data" or "Delete only work data" commands.

Users can deactivate their devices using the following method:

- On the Windows 10 device, select **Settings > Accounts > Work access > Delete**.

Related information

Resource	Information
BlackBerry Access	https://docs.blackberry.com/en/blackberry-dynamics-apps/blackberry-access
BlackBerry Workspaces	https://docs.blackberry.com/en/id-comm-collab/blackberry-workspaces
BBM Enterprise	https://docs.blackberry.com/en/id-comm-collab/bbm-enterprise/

Legal notice

SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

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

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

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

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

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE

United Kingdom

Published in Canada