Work from Anywhere

Deployment Guide

Contents

Overview..... 4

Deploy a BlackBerry UEM Cloud tenant.....5

Installing the BlackBerry Connectivity Node to connect to resources behind your organization's firewall.....6

BlackBerry Connectivity Node planning information.....6
Installing or upgrading the BlackBerry Connectivity Node.....7
Download the installation and activation files for the BlackBerry Connectivity Node..... 7
Install and configure the BlackBerry Connectivity Node.....8

Manage your BlackBerry Desktop users.....12

Setting up network connections for BlackBerry Dynamics apps..... 12
About the BlackBerry Dynamics connectivity profile settings.....12
Create a BlackBerry Dynamics connectivity profile..... 13
Controlling BlackBerry Dynamics on users devices.....13
About the BlackBerry Dynamics profile settings.....13
Create a BlackBerry Dynamics profile.....14
Create a compliance profile.....14
Make BlackBerry Access available to users in BlackBerry UEM.....14
About the BlackBerry Access app configuration settings.....14
Configure BlackBerry Access app settings in BlackBerry UEM.....15
Sending CA certificates to devices and apps.....15
Create a CA certificate profile.....15
Create a local group..... 16
Create a user account..... 16
Install and activate BlackBerry Desktop.....18
Adding additional security to BlackBerry Desktop..... 18

Overview

BlackBerry Desktop for Windows and BlackBerry Desktop for Mac consist of two apps: BlackBerry Access, which is a secure mobile browser that enables business users to securely access their intranet, and BlackBerry Work, which provides everything you need to securely mobilize your work, including email, calendar and contacts. BlackBerry Access and BlackBerry Work are BlackBerry Dynamics apps, which are a collection of secure apps that you can use to boost productivity while safeguarding valuable corporate intellectual property.

To set up and use BlackBerry Desktop for Windows or BlackBerry Desktop for Mac using BlackBerry UEM Cloud, you create a BlackBerry UEM Cloud tenant, install and activate a BlackBerry Connectivity Node, create policies and profiles, and enroll a user.

Deploy a BlackBerry UEM Cloud tenant

1. Login to your organization's BlackBerry myAccount.
2. Select **My Organization > Servers > Add server**.
3. Click **Unified Endpoint Manager (UEM/BES)**.
4. In the Hosting section, click **BlackBerry Cloud**.
5. In the **Custom Domain** section, add a preferred subdomain to make it easier to access your services in the cloud.
6. In the **End User Deployment Name** section, enter a name for your tenant.
7. Click **Add Server**.
8. After the tenant is created, click **Launch UEM**
9. On the **BlackBerry Enterprise Identity** screen, log in with your myAccount credentials.

Installing the BlackBerry Connectivity Node to connect to resources behind your organization's firewall

The BlackBerry Connectivity Node is a collection of components that installed on a dedicated computer to enable additional features for BlackBerry UEM Cloud. The following components that are included in the BlackBerry Connectivity Node are relevant to setting up BlackBerry Work from Anywhere.

Component	Purpose
BlackBerry Cloud Connector	The BlackBerry Cloud Connector allows BlackBerry UEM Cloud to access your organization's on-premises company directory. You can create directory user accounts by searching for and importing user data from the company directory. User data is synchronized with the directory daily. BlackBerry UEM Cloud must be able to access your company directory if you want to use SCEP. 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.
BlackBerry Proxy	BlackBerry Proxy maintains a secure connection between your organization and the BlackBerry Dynamics NOC, which allows BlackBerry Dynamics apps to communicate securely with your organization's resources behind the firewall. It also supports BlackBerry Dynamics Direct Connect, which allows app data to bypass the BlackBerry Dynamics NOC. For more information, see Configuring BlackBerry UEM Cloud to support BlackBerry Dynamics apps.

BlackBerry Connectivity Node planning information

Before you install the BlackBerry Connectivity Node, consider the following information.

Scalability and high availability

Each BlackBerry Connectivity Node can support up to 5000 devices. You can install additional BlackBerry Connectivity Nodes to support up to 50,000 additional devices.

You can install one or more instances of the BlackBerry Connectivity Node to provide redundancy. You must install each instance on a dedicated computer. Use the same company directory configuration for all instances.

Deploy more than one BlackBerry Connectivity Node in a server group to allow for high availability, load balancing, and regionalization.

Optionally, you can designate each BlackBerry Connectivity Node in a server group to handle a single connection type: BlackBerry Secure Connect Plus only, BlackBerry Secure Gateway only, or BlackBerry Proxy only. This frees up server resources to allow fewer servers required for the same number of users or containers. Each BlackBerry Connectivity Node enabled for single-service performance mode can support up to 10,000 devices. For more information about enabling single-service performance mode, see Create a server group.

Hardware

The BlackBerry Connectivity Node must be installed on a dedicated computer, instead of a computer that is used for everyday work. The computer must be able to access the Internet and your company directory. You cannot install the BlackBerry Connectivity Node on a computer that already hosts an on-premises BlackBerry UEM instance.

The computer that hosts the BlackBerry Connectivity Node must meet the following hardware requirements:

- 6 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent
- 12 GB of available memory
- 64 GB of disk space

If you enable single-service performance mode, the computer that hosts the BlackBerry Connectivity Node must meet the following hardware requirements:

BlackBerry Connectivity Node with single-service performance mode enabled for BlackBerry Proxy only	• 6 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 12 GB of available memory • 64 GB of disk space

Software

To verify that your environment meets the requirements for installing the BlackBerry Connectivity Node, see the Compatibility matrix.

Installing or upgrading the BlackBerry Connectivity Node

Follow the instructions in this section to install or upgrade the BlackBerry Connectivity Node.

You can install one or more instances of the BlackBerry Connectivity Node to provide redundancy.

You must install each instance on a dedicated computer.

You can configure one or more directory connections, but if you have multiple BlackBerry Connectivity Nodes, all of the directory connections must be configured identically. If one directory connection is missing or incorrectly configured, that BlackBerry Connectivity Node will appear as disabled in the management console.

If you have more than one BlackBerry Connectivity Node, you must upgrade all of them to the same software release.

Note: If you are upgrading multiple BlackBerry Connectivity Nodes, directory services are disabled after the first node is upgraded until all the nodes are upgraded to the same version.

Download the installation and activation files for the BlackBerry Connectivity Node

1. In the management console of the BlackBerry UEM cloud instance, on the menu bar, click **Settings > External integration > BlackBerry Connectivity Node setup**.
2. Click .
3. Click **Download**.
4. On the software download page, answer the required questions and click **Download**. Save the installation package.

5. If you want to add the BlackBerry Connectivity Node instance to an existing server group when you activate it, in the **Server group** drop-down list, click the appropriate server group.
6. Click **Generate**.
7. Save the activation file (.txt).

   The activation file is valid for 60 minutes. If you wait longer than 60 minutes before you use the activation file, you must generate a new activation file. Only the latest activation file is valid.

Install and configure the BlackBerry Connectivity Node

1. Open the BlackBerry Connectivity Node installation file (.exe) that you downloaded from the BlackBerry UEM Cloud management console.

   If a Windows message appears and requests permission to make changes to the computer, click **Yes**.
2. Choose your language. Click **OK**.
3. Click **Next**.
4. Select your country or region. Read and accept the license agreement. Click **Next**.
5. The installation program verifies that your computer meets the installation requirements. Click **Next**.
6. To change the installation file path, click **...** and navigate to the file path that you want to use. Click **Install**.
7. When the installation completes, click **Next**.

   The address of the BlackBerry Connectivity Node console is displayed (http://localhost:8088). Click the link and save the site in your browser.
8. Select your language. Click **Next**.
9. When you activate the BlackBerry Connectivity Node, it sends data over port 443 (HTTPS) to the BlackBerry Infrastructure (for example na.bbsecure.com or eu.bbsecure.com). After it is activated, the BlackBerry Connectivity Node uses port 3101 (TCP) for all other outbound connections through the BlackBerry Infrastructure. If you want to send data from the BlackBerry Connectivity Node through an existing proxy server behind your organization's firewall, click **Click here to configure the proxy settings for your organization's environment**, select the **Proxy server** option, and do any of the following:

   - To send activation data through a proxy server, in the **Enrollment proxy** fields, type the FQDN or IP address and the port number of the proxy server. The proxy server must be able to send data over port 443 to bbsecure.com (for example na.bbsecure.com or eu.bbsecure.com). Click **Save**.
   - To send other outbound connections from the components of the BlackBerry Connectivity Node through a proxy server, in the appropriate fields, type the FQDN or IP address and the port number of the proxy server. The proxy server must be able to send data over port 3101 to bbsecure.com (for example na.bbsecure.com or eu.bbsecure.com). Click **Save**.
10. In the **Friendly name** field, type a name for the BlackBerry Connectivity Node. Click **Next**.
11. Click **Browse**. Select the activation file that you downloaded from the management console.
12. Click **Activate**.

    If you want to add a BlackBerry Connectivity Node instance to an existing server group when you activate it, your organization's firewall must allow connections from that server over port 443 through the BlackBerry Infrastructure (for example na.bbsecure.com or eu.bbsecure.com) to activate the BlackBerry Connectivity Node and to the same bbsecure.com region as the main BlackBerry Connectivity Node instance.
13. Click +, then select the type of company directory that you want to configure.
14. Follow the steps for your organization's directory type:

Directory type	Steps
Microsoft Active Directory	**a.** In the **Connection name** field, type a name for this company directory connection. **b.** In the **Username** field, type the username of the Microsoft Active Directory account. **c.** In the **Domain** field, type the FQDN of the domain that hosts Microsoft Active Directory. For example, domain.example.com. **d.** In the **Password** field, type the password of the Microsoft Active Directory account. **e.** In the **Domain controller discovery** drop-down list, click one of the following: • If you want to use automatic discovery, click **Automatic**. • If you want to specify the domain controller computer, click **Select from list below**. Click and type the FQDN of the computer. Repeat this step to add more computers. **f.** In the **Global catalog search base** field, type the search base that you want to access (for example, OU=Users,DC=example,DC=com). To search the entire Global Catalog, leave the field blank. **g.** In the **Global catalog discovery** drop-down list, click one of the following: • If you want to use automatic catalog discovery, click **Automatic**. • If you want to specify the catalog computer, click **Select from list below**. Click and type the FQDN of the computer. If necessary, repeat this step to specify more computers. **h.** If you want to enable support for linked Microsoft Exchange mailboxes, in the **Support for linked Microsoft Exchange mailboxes** drop-down list, click **Yes**. To configure the Microsoft Active Directory account for each forest that you want BlackBerry UEM Cloud to access, in the **List of account forests** section, click +. Specify the forest name, user domain name (the user can belong to any domain in the account forest), username, and password. **i.** To synchronize more user details from your company directory, select the **Synchronize additional user details** check box. The additional details include company name and office phone. **j.** Click **Save**.

Directory type	Steps
LDAP directory	**a.** In the **Connection name** field, type a name for this company directory connection. **b.** In the **LDAP server discovery** drop-down list, click one of the following: • If you want to use automatic discovery, click **Automatic**. In the **DNS domain name** field, type the DNS domain name. • If you want to specify the LDAP computer, click **Select server from list below**. Click and type the FQDN of the computer. Repeat this step to add more computers. **c.** In the **Enable SSL** drop-down list, select whether you want to enable SSL authentication for LDAP traffic. If you click **Yes**, click **Browse** and select the SSL certificate for the LDAP computer. **d.** In the **LDAP** port field, type the port number of the LDAP computer. **e.** In the **Authorization required** drop-down list, select whether BlackBerry UEM Cloud must authenticate with the LDAP computer. If you click **Yes**, type the username and password of the LDAP account. The username must be in DN format (for example, CN=Megan Ball,OU=Sales,DC=example,DC=com). **f.** In the **Search base** field, type the search base that you want to access (for example, OU=Users,DC=example,DC=com). **g.** In the **LDAP user search filter** field, type the filter that you want to use for LDAP users. For example: (&(objectCategory=person)(objectclass=user)(memberOf=CN=Local,OU=Users,DC=example,DC=com)). **h.** In the **LDAP user search scope** drop-down list, click one of the following: • If you want user searches to apply to all levels below the base DN, click **All levels**. • If you want to limit user searches to one level below the base DN, click **One level**. **i.** In the **Unique identifier** field, type the attribute for each user's unique identifier (for example, uid). The attribute must be immutable and globally unique for every user. **j.** In the **First name** field, type the attribute for each user's first name (for example, givenName). **k.** In the **Last name** field, type the attribute for each user's last name (for example, sn). **l.** In the **Login attribute** field, type the attribute for each user's login attribute (for example, cn). This attribute is used for the value that users type to log in to BlackBerry UEM Self-Service with their directory credentials. **m.** In the **Email address** field, type the attribute for each user's email (for example, mail). **n.** In the **Display name** field, type the attribute for each user's display name (for example, displayName). **o.** To synchronize more user details from your company directory, select the **Synchronize additional user details** check box. The additional details include company name and office phone. **p.** To enable directory-linked groups, select the **Enable directory-linked groups** check box. For more information about directory-linked groups, see Linking company directory groups to BlackBerry UEM groups. **q.** Click **Save**.

15. In the management console, click **Settings > External integration > BlackBerry Connectivity Node setup**.
16. In the **Step 4: Test connection** section, click **Next**.

To view the status of a BlackBerry Connectivity Node instance, in the management console, on the menu bar, click **Settings > External integration > BlackBerry Connectivity Node status**.

After you finish:

- To install a second BlackBerry Connectivity Node instance for redundancy, download another set of installation and activation files and repeat this task on a different computer. You can use the same company directory configuration for all instances, or each instance can have its own company directory configuration. This should be done after the first instance has been activated.
- If necessary, configure proxy settings for the BlackBerry Connectivity Node. For instructions, see Configuring the BlackBerry Connectivity Node to use the BlackBerry Router or a TCP proxy server.
- To change the directory settings that you configured, in the BlackBerry Connectivity Node console (http://localhost:8088), click **General settings > Company directory**. Click ✎ for the directory connection.
- If you want to send data through an HTTP proxy before it reaches the BlackBerry Dynamics NOC, in the BlackBerry Connectivity Node console (http://localhost:8088), click **General settings > BlackBerry Router and proxy**. Select the **Enable HTTP proxy** checkbox and configure the proxy settings.
- For instructions for enabling BlackBerry Secure Connect Plus, see "Using BlackBerry Secure Connect Plus for connections to work resources" in the Administration content.
- For more information about enabling the BlackBerry Secure Gateway, see "Protecting email data using the BlackBerry Secure Gateway" in the Administration content.
- For instructions for configuring the BlackBerry Gatekeeping Service, see "Controlling which devices can access Exchange ActiveSync" in the Administration content.

Manage your BlackBerry Desktop users

To help manage users efficiently, in the BlackBerry UEM management console, create the following:

- BlackBerry Dynamics Connectivity profile
- BlackBerry Dynamics profile
- Compliance profile
- BlackBerry Access app configuration
- CA certificate profile (optional)
- Local user group

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 BlackBerry Dynamics apps can connect to

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 to 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.

About the BlackBerry Dynamics connectivity profile settings

The BlackBerry Dynamics connectivity profile determines where and how traffic is routed for the enrolled devices. For more detailed information about all of the settings in the profile, refer to the BlackBerry Dynamics connectivity profile settings topic in the Administration content. The following fields in the profile will help you route traffic correctly:

- **Direct**: Select this option to route traffic directly from the app to the domain without going through BlackBerry Proxy. This option is supported only for apps developed with BlackBerry Dynamics SDK version 6.0 and later.
- **BlackBerry Proxy Cluster**: Select this option to specify the BlackBerry Proxy clusters that must be used to reach the domain. Using this option will route traffic to your BlackBerry Connectivity Node through a secure tunnel (a VPN for example) to resources. For more information, see Routing BlackBerry Dynamics app data through BlackBerry Proxy.
- **Deny**: Select this option to block the app from connecting to the domain. This option is supported for apps developed with BlackBerry Dynamics SDK version 6.0 and later.
- **Allowed domains**: A list of the Internet domains that your organization wants to control access to. For example, blackberry.com controls 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.
- **Default allowed domain route type**: This setting determines the default behaviour for traffic (if strict tunneling is not configured in BlackBerry Access).
- **Default domains**: A list of 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**: A list of additional servers that BlackBerry Dynamics apps can connect to. Add servers to this list if you want BlackBerry Dynamics apps to connect only to certain servers and not to every server in a domain. When you add a server, you specify the fully qualified domain name.

- **IP address ranges**: A list of IP address ranges that BlackBerry Dynamics apps can access when they make a connection request using an IP address rather than a hostname. Specify a range of IP addresses that BlackBerry Dynamics apps can access when they make a connection request using an IP address rather than a hostname. 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: 192.168.2.0-192.168.2.255
  - An entire subnet: 192.168.2.0/24

Create a BlackBerry Dynamics connectivity profile

1. On the menu bar, click **Policies and Profiles**.
2. Click **Networks and connections > BlackBerry Dynamics connectivity**
3. Click +.
4. Type a name and description for the profile.
5. If you have previously exported BlackBerry Dynamics connectivity profile settings that you want to reuse as a .csv file, click to import the settings.
6. Configure the appropriate values for the profile settings. For more information about each profile setting, see BlackBerry Dynamics connectivity profile settings.
7. To add an app server for a BlackBerry Dynamics app, see Add an app server to a BlackBerry Dynamics connectivity profile.
8. Click **Save**.

After you finish: If necessary, rank profiles.

Controlling BlackBerry Dynamics on users devices

The BlackBerry Dynamics profile enables BlackBerry Dynamics for users and sets standards for BlackBerry Dynamics app access, data protection, and logging.

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

You can assign the BlackBerry Dynamics profile to user accounts, user groups, or device groups.

About the BlackBerry Dynamics profile settings

The BlackBerry Dynamics profile enables BlackBerry Dynamics for users and sets standards for BlackBerry Dynamics app access, data protection, and logging. For detailed information about all of the settings in the profile, refer to the BlackBerry Dynamics profile settings topic in the Administration content. The following fields are important when configuring the profile for BlackBerry Desktop:

- **Require device management to use BlackBerry Dynamics apps**: This field is not supported for BlackBerry Desktop and should be switched off.
- **Enable UEM Client to enrol in BlackBerry Dynamics**: This field is not necessary for BlackBerry Desktop and should be switched off.

Create a BlackBerry Dynamics profile

1. On the menu bar, click **Policies and Profiles**.
2. Click **Policy > BlackBerrry Dynamics**
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 profile settings.
6. Click **Add**.

After you finish: If necessary, rank profiles.

Create a compliance profile

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.

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. On the Windows and Mac tabs, configure the appropriate values for each profile setting. For details about each profile setting, see macOS: Compliance profile settings and Windows: Compliance profile settings.
6. Click **Add**.

Make BlackBerry Access available to users in BlackBerry UEM

To manage BlackBerry Access in BlackBerry UEM, you must add BlackBerry Access to the app list. If BlackBerry Access does not display in the app list, click ⟳. If the app still does not display you can start a trial. After BlackBerry Access has been added to the app list, you can assign it to users.

For complete instructions for managing BlackBerry Dynamics apps in BlackBerry UEM, see Managing BlackBerry Dynamics apps.

1. Go to the BlackBerry support site.
2. Click **Start a free trial** and log into your BlackBerry Online Account. If you do not already have an account you can create one on the log in page.
3. The app will be made available to your organization and can be assigned to users after the app has been synchronized to BlackBerry UEM. To force a synchronization, click ⟳.

About the BlackBerry Access app configuration settings

App configurations allow you to preconfigure certain app settings before you assign apps to users. By preconfiguring app settings, you can make it easier for users to download, set up, and use the apps. For detailed information about all of the settings in the app configuration, refer to the BlackBerry Access app configuration settings topic in the Administration content. The following tabs are important when setting up the app configuration in BlackBerry Desktop:

General: This tab allows you to configure general settings such as allowing the user to set the home page, geolocaton, and enable pop-up windows.

Security: This tab allows you to enable specific security settings. BlackBerry recommends that you disable the 'Allow SHA1 leaf or intermediate certificates' and 'Allow legacy/weak algorithms (DES)' options. The Enforce strict tunnel option ensures all undefined traffic is not routed directly. For more information about routing, refer to About the BlackBerry Dynamics connectivity profile settings.

Network: This tab allows you to set up your network configuration. Note that if you enable a web proxy, it overrules any configuration that you set up in the BlackBerry Dynamics connectivity profile. You can use a PAC file to provide the option to combine direct routing for some targets and using a proxy for others.

BlackBerry Work (Win and Mac): This tab allows you to set up your email client for BlackBerry Desktop.

BlackBerry Access (Win and Mac): This tab allows you to enable features such as WebRTC, which specifies whether to enable access to WebRTC protocol-based destinations such as Citrix VDI browser-based access, microphone and camera support, UDP Protocol support, printing configuration, update notifications to users, Awingu integration, and extension management.

Configure BlackBerry Access app settings in BlackBerry UEM

1. On the menu bar, click **Apps**.
2. Click the BlackBerry Access app.
3. On the BlackBerry Dynamics tab, in the **App configuration** table, click +.
4. Type a name for the app configuration.
5. Configure the app settings. See BlackBerry Access app configuration settings for a description of the settings that you can configure.
6. Click **Save**.

After you finish: Assign BlackBerry Access to a user group or user account.

Sending CA certificates to devices and apps

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

When a CA certificate is stored on a device, the device and apps trust 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, device and apps 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 email client 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: Obtain the CA certificate file from your PKI administrator.

1. In the BlackBerry UEM console, 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. If the CA certificate is sent to macOS devices, on the macOS tab, in the Apply profile to drop-down list, select User or Device.
7. Click **Add**.

Create a local group

1. in the BlackBerry UEM console, on the menu bar, click **Groups**.
2. Click .
3. Type a name for the user group.
4. Optionally, type a description for the user group.
5. To assign a user role to the local group, perform the following actions:
   a) In the **User role** section, click +.
   b) In the drop-down list, click the name of the user role that you want to assign to the group.
   c) Click **Add**.
6. To assign the profiles that you created to the local group, perform the following actions:
   a) In the **IT policy and profiles** section, click +.
   b) Click a profile type.
   c) In the drop-down list, click the name of the profile that you want to assign to the group.
   d) Click **Assign**.
7. To assign the BlackBerry Access app to the user group, in the **Assigned apps** section, click +.
8. Search for the app.
9. In the search results, select the app.
10. Click **Next**.
11. In the **Disposition** drop-down list for the app, perform one of the following actions:
    - To install the app automatically on devices, and to prevent users from removing the app, select **Required**.
    - To permit users to install and remove the app, select **Optional**.

    Note: If the same app is assigned to a user account and to the user group that the user belongs to, the disposition of the app assigned to the user account takes precedence.
12. In the **App configuration** drop-down list, select the app configuration that you created for BlackBerry Access.
13. Click **Assign**.
14. When you are finished specifying the user group properties, click **Add**.

Create a user account

Before you begin:

- If you want to add a directory user, verify that BlackBerry UEM is connected to your company directory. For information about connecting BlackBerry UEM to a company directory and enabling directory-linked groups, see the Cloud Configuration content

1. On the menu bar, click **Users**.
2. Click **Add user**.
3. Perform one of the following tasks:

Task	Steps
Add a directory user	**a.** On the **Company directory** tab, in the search field, specify the search criteria for the directory user that you want to add. You can search by first name, last name, display name, username, or email address. **b.** In the search results, select the user account.
Add a local user	**a.** In an on-premises environment, click the **Local** tab. In a Cloud environment, click the **Non-directory** tab. **b.** Type the **First name** and **Last name** for the user account. **c.** In the **Display name** field, make changes if necessary. The display name is automatically configured with the first and last name that you specified. **d.** In the **Username** field, enter a unique username for the user account. **e.** In the **Email address** field, enter a contact email address for the user account. An email address for the user account is required when you enable a service such as Workspaces or device management. **f.** Optionally, click **Additional user details** and fill in the fields as needed.
Add a BlackBerry Online Account user (This option is available only in Cloud environments.)	**a.** Click the **Non-directory** tab. **b.** Type the **First name** and **Last name** for the user account. **c.** In the **Display name** field, make changes if necessary. The display name is automatically configured with the first and last name that you specified. **d.** In the **Email address** field, enter a contact email address for the user account. An email address for the user account is required when you enable a service such as Workspaces or device management. **e.** Optionally, click **Additional user details** and fill in the fields as needed.

4. Add the user account to the group that you created, in the **Available groups** list, select the group and click ➡.

   When you create a user account, you can add it only to local groups in BlackBerry UEM. If the user account is a member of a directory-linked group, it is automatically associated with that group when the synchronization between BlackBerry UEM and your company directory occurs.

   To add a user account to groups that are assigned an administrative role, you must be a Security Administrator.
5. In a Cloud environment, under **UEM Self-Service**, select either **BlackBerry Online Account** or **Local UEM user account**. If you select Local UEM user account, create a password for BlackBerry UEM Self-Service. If the user is assigned an administrative role, they can also use the password to access the management console.
6. In an on-premises environment, if you add a local user, in the **Account password** field, create a password for BlackBerry UEM Self-Service. If the user is assigned an administrative role, they can also use the password to access the management console.
7. In the **Enabled services** section, select the **Enable user for device management** option.
8. Allow users to activate only BlackBerry Dynamics apps:
   a) In the **Activation option** drop-down list, select BlackBerry Dynamics access key generation.
   b) In the **Number of access keys to generate** drop-down list, select the number of keys. Each key can be used only once to activate a BlackBerry Dynamics app.
   c) Select the number of days that you want the access key to remain valid.
   d) In the **Activation email template** drop-down list, click a template to use for the activation email.
9. If you use custom variables, expand **Custom variables** and specify the appropriate values for the variables that you defined.
10. Perform one of the following actions:

- To save the user account, click **Save**.
- To save the user account and create another user account, click **Save and new**.

Install and activate BlackBerry Desktop

1. Download BlackBerry Access for Windows or Mac. Click here to go to the download page.
2. Double-click on the file that you downloaded to install BlackBerry Access.

   Make sure that you select the "Run BlackBerry Access" option before you click Finish.
3. To activate the app, the user must enter their email address and the activation key.

   After activation completes, the user will be asked to create a new password that they'll use when they log in to BlackBerry Desktop each day, and to accept a user license agreement.
4. When prompted, enter your Microsoft Exchange credentials (email address, username or User Principal Name, and mail server password). BlackBerry Access then configures email, calendar, and contacts for you using your Microsoft Exchange credentials.
5. Use the icons in the toolbar to quickly access to your email messages, contacts, and calendar events.

Adding additional security to BlackBerry Desktop

- You can enable users to securely edit Microsoft Office documents such as Microsoft Word, Microsoft Excel and Microsoft PowerPoint, and annotate PDFs when using BlackBerry Access and BlackBerry Work for macOS and Windows. (Separate license required)
- You can enable BlackBerry Protect Desktop which detects and blocks malware before it can affect a device. (Separate license required)