Administration Guide

BES10 Cloud

Market Preview

Published: 2014-02-04
SWD-20140204152348686

Contents

Introduction

Multiplatform

About this guide

BES10 Cloud helps you manage BlackBerry 10, iOS, and Android devices for your organization. This guide provides instructions on how to:

- Obtain and activate licenses
- Connect BES10 Cloud to your company directory
- Create and manage user accounts, administrator accounts, and groups
- Manage IT policies, profiles, and apps

This guide is intended for administrators who are responsible for setting up and administering BES10 Cloud.

What is BES10 Cloud?

BES10 Cloud is an enterprise mobility management solution from BlackBerry. EMM solutions help you manage mobile devices for your organization. You can manage BlackBerry, iOS, and Android devices, all from a unified interface.

EMM solutions from BlackBerry protect business information, keep mobile workers connected with the information they need, and provide administrators with efficient tools that help keep business moving.

BES10 Cloud is an EMM solution that is available in the cloud.

EMM solution	Description
BES10 Cloud	An easy-to-use, low-cost, and secure solution. BlackBerry hosts this service over the Internet. You only need a supported web browser to access the service, and BlackBerry maintains high availability to minimize downtime. Optionally, you can connect your on-premises directory services to BES10 Cloud.
BlackBerry Enterprise Service 10	A comprehensive, scalable, and secure solution. Your organization installs this service in its environment. The deployment can range in size from one server to many, and you can set up and maintain high availability to minimize downtime.

Key features of BES10 Cloud

Feature	Description
Management of most types of devices	You can manage BlackBerry 10, iOS, and Android devices.
Single, unified interface	You can view all devices in one place and access all management tasks in a single, web-based interface. You can share administrative duties with multiple administrators who can access the administration consoles at the same time.
Trusted and secure experience	Device controls give you precise management of how devices connect to your network, what capabilities are enabled, and what apps are available. Whether the devices are owned by your organization or your users, you can protect your organization's information.
Balance of work and personal needs	BlackBerry Balance technology is designed to ensure that personal and work information are kept separate and secure on BlackBerry devices. If the device is lost or the employee leaves the organization, you can delete only work-related information or all information from the device.
High availability	Instead of having to maintain your own highly available service for device management, with all the upfront and maintenance costs, BlackBerry maintains the service and maximizes uptime for you.

BES10 Cloud requirements checklist

Verify that your organization meets the following requirements before you use BES10 Cloud in your environment. For more details about supported hardware and software for BES10 Cloud, visit www.blackberry.com/go/serverdocs to see the *BES10 Cloud Compatibility Matrix*.

System requirements

	Requirement	Description
□	**DNS** DNS support for resolving IP addresses into host names	BES10 Cloud uses DNS to resolve the IP address when it tries to connect to <*country*>.srp.blackberry.com.
□	**Exchange ActiveSync**	For minimum requirements, refer to the *BES10 Cloud Compatibility Matrix*.
□	**Devices**	Any of the mobile operating systems listed in the *BES10 Cloud Compatibility Matrix* **Note:** Exchange ActiveSync must be enabled on your organization's messaging server to use the native email, calendar, and contacts apps on devices. Exchange ActiveSync must be available publicly or over VPN or Wi-Fi Open the following outbound ports for devices on your organization’s Wi-Fi network: • Connection from devices to the BlackBerry Infrastructure: ports 80 and 443 ◦ *.bbsecure.com • Connection from iOS devices to APNs: port 5223 ◦ gateway.push.apple.com • Connection from Android devices to GCM: ports 5228, 5229, 5230 ◦ 5228 and 5229: android.apis.google.com ◦ 5230: android.googleapis.com
□	**VPN hardware (optional)** IPSec VPN hardware or SSL VPN hardware	If your organization's environment includes VPNs, you can configure a device to authenticate with a VPN so that it can access your organization's network.

Software requirements for the browser

The following requirements apply to the browser that you use to log in to the BES10 Cloud administration console and BES10 Self-Service.

	Requirement	Description
□	**Supported browsers** Any of the browsers listed in the *BES10 Cloud Compatibility Matrix*	Windows Internet Explorer 9 or later provides optimal support for BES10 Self-Service features and the administration console features. You must configure the following settings: • Support for JavaScript • Cookies turned on • Support for TLS or SSL • The SSL certificate is installed to permit trusted connections to the consoles
□	**Windows Internet Explorer**	If you want to use Windows Internet Explorer to access the management consoles, you must meet the following requirements: • Latest Microsoft hotfixes installed • Language preferences that display encoded webpages • To support Microsoft ActiveX, the following settings are enabled: ◦ Automatic prompting for Microsoft ActiveX controls ◦ Download signed Microsoft ActiveX controls ◦ Run Microsoft ActiveX controls and plug-ins ◦ Script Microsoft ActiveX controls marked safe for scripting • The administration console and BES10 Self-Service websites are assigned to the trusted websites security zone

Software requirements for the BlackBerry Cloud Connector

If you want to allow BES10 Cloud to access your company directory, you must install, activate, and configure the BlackBerry Cloud Connector on a computer that is reserved for IT purposes, instead of a computer that is used for everyday work. The computer must be able to access the Internet and your company directory.

To review the software requirements for the BlackBerry Cloud Connector, visit www.blackberry.com/go/serverdocs to read the *BES10 Cloud Compatibility Matrix*.

Overview: BES10 Cloud consoles

There are four consoles that you use with BES10 Cloud.

Console	Description
BES10 Cloud administration console	The BES10 Cloud console is the main management console for the BES10 Cloud. You can create and manage IT policies, profiles, certificates, user groups, user accounts, administrator accounts, settings and apps.
BlackBerry Account Center console	The BlackBerry Account Center console is the portal used by customers to claim orders. You can also view order statuses, order history, all your current licenses, and create and manage the admins assigned to your account.
BES10 Self-Service console	The BES10 Self-Service console permits users to activate and manage their devices. They can also view an activation tutorial for step by step instructions on the activation process.
BlackBerry Cloud Connector console	The BlackBerry Cloud Connector console gives you the option to connect the BES10 Cloud to your organization's directory. You can edit the directory and TCP proxy settings from this console.

Using the administration console

Feature	Description
Single list of all users and devices	In the users and devices list, each row is a link that you can click to view the properties of the user account and all of the user's devices, consolidated on one tabbed page. You can sort and reverse sort the information in the user and devices list by clicking any of the column headers.
Single view of policies and profiles	In the Policies and Profiles library, you can view a consolidated list of all policy and profile types and perform all tasks associated with them.
Simplified app management	You can view and configure all apps on one page, and you no longer need to use software configurations or application definitions to manage apps.
Required fields	Fields that have a red asterisk (*) beside them are required. You must submit a value in all required fields to complete a task. Default values, which you can customize, are often displayed in the fields.
Online help	Click the Help link in the upper-right corner of the screen to access online help. The online help is updated regularly to provide the most recent information.

Setting up BES10 Self-Service for users

BES10 Self-Service is a web-based application that you can make available to users so that they can perform certain tasks such as creating activation passwords, remotely locking their devices, or deleting data from their devices. Users do not need to install any software on their computers to use BES10 Self-Service. You must provide the web address and login information to users.

Set up BES10 Self-Service

Set up BES10 Self-Service so that users can log in and perform some self-service tasks.

1. In BES10 Cloud, click **Settings** > **Self-Service**.
2. Verify that **Allow users to access the self-service console** is selected.
3. If you want users to be able to create activation passwords, complete the following tasks:
    a. Select **Allow users to activate device in the self-service console**.
    b. Specify the number of minutes, hours, or days that a user can activate a device before the activation password expires.
4. Click **Save**.

After you finish: Provide the BES10 Self-Service web address and login information to users.

Send BES10 Self-Service login information to users

After you set up BES10 Self-Service, you must provide users with the information they need to log in. Provide the following information:

- Web address for BES10 Self-Service. The web address is displayed in Settings > Self-Service. You can include the web address in the activation email template by inserting the variable %UserSelfServicePortalURL%.
- Username and password. For company directory users this is their organization username and password. For local user accounts, provide their console usernames and create their passwords. You can create the password in the Console password field of the Add a user screen, and optionally select the Send password to user checkbox to automatically send the password to the user's email address.
- Domain name (for Microsoft Active Directory users)

If a local user forgets their login password, or you want to create and send a password for an existing local user account, you can complete the following steps:

1. Search for a user account.
2. In the search results, click the name of a user account.
3. Click the user's name.
4. Click the **edit** icon.
5. In the **Console password** section, delete the existing password.
6. Type a new password in the **Console password** field and select the **Send password to user** check box.
7. Click **Save**. BES10 Self-Service sends the new login password to the user's email address.

About the setup wizard

When you first log in to the admin console, a setup wizard appears that walks you through the process of downloading and installing an APNs certificate for managing iOS devices and provides some information on how to get started with BES10 Cloud.

Best practices for administering BES10 Cloud

When you start administering BES10 Cloud, perform these administration tasks in the following order:

1. Sign up for BES10 Cloud and obtain licenses.
2. Optionally, set up the following in your environment:
   - Install the BlackBerry Cloud Connector if you want to connect to your company directory
   - Obtain an APNs certificate if you want to manage iOS devices.
3. Set up device controls and settings.
4. Manage apps.
5. Create and manage user groups, users, and administrators.
6. Activate and manage devices.

Managing licensing

About licenses

Licenses control the number of BlackBerry 10 devices, iOS devices, and Android devices that can activate to the BES10 Cloud. Licenses determine the devices and features that you can manage using BES10 Cloud. A license is used when you or a user activates a device. A device uses only one type of license at a time. You cannot access the administration console until you have purchased licenses for your organization.

License type

BES10 Cloud supports the following license type:

License type	Description
EMM – Corporate	You can activate the following devices and features: • BlackBerry 10 devices • iOS devices • Android devices

License information

You can view the following license information:

Item	Description
License type	The license type is the category of license that your organization uses.
License usage	You can view the number of total licenses, available licenses, and used licenses.
Expiration	You can view the number of total licenses and, if applicable, the date that licenses expire. The information displayed is for each license. For licenses that expire, the information is no longer displayed after the expiration date.

Understanding licensing status and compliance

In the administration console, the Licensing summary tab displays the licensing status. If there are no issues, the licensing status displays an in compliance icon. If an issue requires your attention, the licensing status displays a warning icon or an error icon. The icon displayed depends on the licensing issues and, if there is more than one issue, the icon for the most critical issue is displayed (for example, if the expiration date is approaching for some licenses and you also exceed the total licenses for a license type, an error icon is displayed).

BES10 Cloud tracks the usage of licenses, including the usage for each trial and subscription license that your organization uses, and detects when licensing requirements are not met. If licensing requirements are met, BES10 Cloud is classified as in compliance. If licensing requirements are not met, BES10 Cloud is classified as out of compliance.

The following icons indicate the licensing status:

Icon	Status	Description
✅	In compliance	• Licenses are in compliance • You can activate new devices if unused licenses are available • You have enough licenses to reactivate existing devices
⚠	Warning	• Licenses are in compliance, but are at risk of becoming out of compliance if action is not taken • An issue will occur if it is not addressed • You can activate new devices if unused licenses are available • You have enough licenses to reactivate existing devices • Your licenses are about to expire. You will see a warning next to the licenses which are about to expire • You can continue to manage activated devices and switch devices. For a device switch, you or a user must activate the replacement device and select the replace device option on the device or in BES10 Self-Service
❗	Error	• Licenses are out of compliance • An issue has occurred and must be addressed before you can activate new devices or reactivate existing devices • A license has expired. You can view expiration details in the License information section • Your used licenses exceed the total licenses for any license type. You can view license usage details in the License information section • You can continue to manage activated devices and switch devices. For a device switch, you or a user must activate the replacement device and select the replace device option on the device or in BES10 Self-Service

Using trial licenses

If you want to evaluate the BES10 Cloud software, you can obtain trial licenses which are valid for a set amount of time.

You can view expiration details in the License information section. When trial licenses expire, the licensing server calculates license usage for the domain.

If you have only trial licenses and all of your trial licenses expire, you will be locked out of the administration console and prompted to purchase additional licenses at the BlackBerry Account Center. You can view more detailed information on your subscription licenses in the BlackBerry Account Center.

Overview: Obtaining licenses

To obtain licenses for BES10 Cloud, perform the following actions:

1. Determine the number of devices in your organization.
2. Purchase licenses for BES10 Cloud.
3. Log in to the administration console with the instructions provided in the email that you received with your licensing information.
4. Confirm your licensing information by going to Settings > Licensing summary.

Managing licensing

You can manage your licensing subscriptions and configure the number of days before the license expiration warning is displayed in the administration console.

View your licensing subscriptions

Note: You purchase or cancel licenses through the BlackBerry Enterprise Store.

1. In the administration console, on the menu bar, click the **Settings** tab.
2. In the left pane, expand **Licensing**.
3. In the left pane, click **Licensing summary**.
4. Click **Manage subscriptions**.
5. Log into the BlackBerry Account Center.
6. In the BlackBerry Account Center file menu, click **Licenses**.
7. In the Enterprise License Management section, select one of the following:
    - To view your entitlements, click **Manage entitlements**
    - To view your licenses, click **Manage licenses**
    - To view your devices, click **Manage devices**

Configure licensing settings

In BES10 Cloud administration console, on the Licensing setting tab, you can check the licensing configuration for the BES10 Cloud domain. You can also configure the number of days before the license expiration warning is displayed.

1. On the menu bar, click the **Settings** tab.
2. In the left pane, expand **Licensing**.
3. In the left pane, click **Licensing setting**.
4. In the **License configurations** drop-down list, select the number of days before the license expiration warning is displayed. The default is 28 days.
5. Click **Save**.

Check your licensing status

1. On the menu bar, click the **Settings** tab.
2. In the left pane, expand **Licensing**.
3. In the left pane, click **Licensing summary**.

4. Verify the following licensing information for your organization: the correct number of total, available, and used licenses, the number of used licenses have not exceeded the total licenses, and all of the licenses display an expiration date.

Synchronize your licenses

In BES10 Cloud administration console, on the Licensing summary tab, you can synchronize your licenses for BES10 Cloud. You can verify that your licenses in BES10 Cloud administration console are synchronized with any licenses recently purchased through the BlackBerry Enterprise Store.

Note: You purchase or cancel licenses through the BlackBerry Enterprise Store.

1. On the menu bar, click the **Settings** tab.
2. In the left pane, expand **Licensing**.
3. In the left pane, click **Licensing summary**.
4. Click **Synchronize licenses**.

Accessing your company directory

Simple

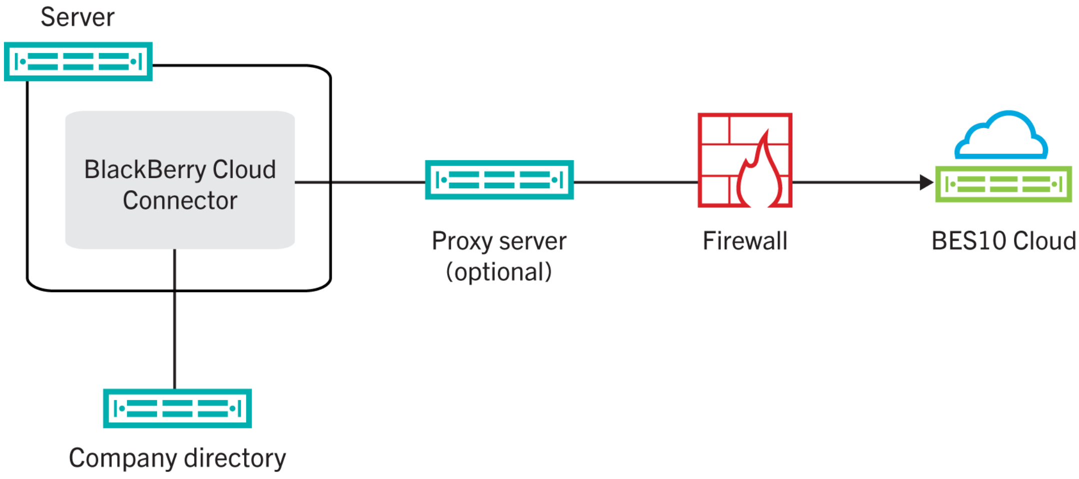
Accessing your company directory

If you allow BES10 Cloud to access your company directory, you can take advantage of the following features:

- You can create directory user accounts by searching for and importing user data from the directory. Directory user accounts are different from local user accounts, which you create by manually adding user information in the administration console.
- BES10 Cloud synchronizes user data with the directory daily. You can configure when the automatic synchronization begins. You can also start the synchronization process manually for an individual user.
- Directory users can use their directory credentials to access BES10 Self-Service.
- You can assign an administrative role to directory users to make them administrators. The users can then log in to the administration console using their directory credentials.

To enable directory access, you must install, activate, and configure the BlackBerry Cloud Connector. The BlackBerry Cloud Connector is a Java process that provides a secure connection between BES10 Cloud and your company directory. The installation and activation files for the BlackBerry Cloud Connector are available in the administration console.

Architecture: BlackBerry Cloud Connector



The diagram above presents the key components related to the BlackBerry Cloud Connector. For more information about the full architecture of BES10 Cloud, visit www.blackberry.com/go/serverdocs to read the *BES10 Cloud Product Overview*.

Component	Description
BlackBerry Cloud Connector	The BlackBerry Cloud Connector is a Java process that provides a secure connection between BES10 Cloud and your company directory. You install the BlackBerry Cloud Connector behind your organization's firewall. Using a setup console, you activate the BlackBerry Cloud Connector with BES10 Cloud and you connect it to the directory.

Component	Description
Company directory	The company directory is any service that your organization uses to manage user accounts for employees. BES10 Cloud supports: • Microsoft Active Directory • Domino LDAP • Novell GroupWise LDAP
Proxy server (optional)	You can configure the BlackBerry Cloud Connector to route data to and from BES10 Cloud through a proxy server that is behind your organization's firewall.
BES10 Cloud	BES10 Cloud is a cloud-based service that you can use to manage iOS devices, Android devices, and BlackBerry 10 devices. You access the administration console, hosted in the cloud, to manage users' devices.

Overview: Accessing your company directory

To allow BES10 Cloud to access your company directory, perform the following actions:

1	Download the installation file and the activation file for the BlackBerry Cloud Connector from the administration console.
2	Install, activate, and configure the BlackBerry Cloud Connector.
3	Test the connection between the BlackBerry Cloud Connector and BES10 Cloud.
4	If necessary, configure proxy settings for the BlackBerry Cloud Connector.

Installing two BlackBerry Cloud Connector instances for redundancy

You can install two instances of the BlackBerry Cloud Connector to provide redundancy for directory lookups and directory synchronization processes. BES10 Cloud does not support more than two instances.

You must install each instance on a different computer that is reserved for IT purposes. Use the same directory configuration for both instances.

Installing the BlackBerry Cloud Connector

Prerequisites: Installing the BlackBerry Cloud Connector

- Install the BlackBerry Cloud Connector on a computer that is reserved for IT purposes, instead of a computer that is used for everyday work. The computer must be able to access the Internet and your company directory.
- Visit www.blackberry.com/go/serverdocs to review the *BES10 Cloud Compatibility Matrix*. Verify that the computer satisfies the requirements for installing the BlackBerry Cloud Connector.
- Choose a directory account with read permissions that the BlackBerry Cloud Connector can use to access the company directory.
- Use a BES10 Cloud administrator account with the Security Administrator or Enterprise Administrator role.
- Verify that the following outbound ports are open in your organization's firewall so that the BlackBerry Cloud Connector (and any proxy servers that you want it to use) can communicate with BES10 Cloud:
  - 3101 (TCP)
  - 443 (HTTPS)

Download the installation and activation files

Before you begin: Use an administrator account with the Security Administrator or Enterprise Administrator role.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration** > **BlackBerry Cloud Connector**.
3. Click **Add BlackBerry Cloud Connector**.
4. In the **Step 1: Download BlackBerry Cloud Connector** section, click **Download**.
5. On the software download page, answer the required questions and click **Download**. Save the BlackBerry Cloud Connector installation file (.exe).
6. In the **Step 2: Generate and download activation file** section, click **Generate and download activation file**.
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, repeat steps 6 and 7 to generate a new activation file. Only the latest activation file is valid.

After you finish: Install and configure the BlackBerry Cloud Connector.

Install and configure the BlackBerry Cloud Connector

Before you begin:

- Download the installation and activation files.
- Use an administrator account with the Security Administrator or Enterprise Administrator role.

1. Open the BlackBerry Cloud Connector installation file (.exe) that you downloaded from the administration console.

   If a Windows message appears and requests permission to make changes to the computer, click **Yes**.

2. Read the introduction. Click **Next**.
3. Read and accept the license agreement. Click **Next**.
4. If you want to change the installation file path, click **Choose** and navigate to the file path that you want to use. Click **Next**.
5. Select where you would like to add a shortcut to open the setup console. Click **Next**.
6. Review the preinstallation summary. Click **Install**.
7. When you are prompted, type the port number for the Apache Tomcat server. The default port is 8088. Click **OK**.
8. When the installation completes, click **Done**.

   The setup console for the BlackBerry Cloud Connector opens.

9. When you activate the BlackBerry Cloud Connector, it sends data over HTTPS to enroll with BES10 Cloud. After it is activated, the BlackBerry Cloud Connector sends and receives data over TCP. If you want to route data through a proxy server behind your organization's firewall, see Configure proxy settings for the BlackBerry Cloud Connector.
10. In the **Friendly name** field, type a name for the BlackBerry Cloud Connector.
11. Click **Next**.
12. Click **Browse**. Select the activation file that you downloaded from the administration console.
13. Click **Activate**.
14. In the drop-down list, click the type of directory that your organization uses.
15. Click **Configure**.
16. Follow the steps for your organization’s directory type:

Directory type	Steps
Microsoft Active Directory	1. In the **Username** field, type the username of the Microsoft Active Directory account. 2. In the **Domain** field, type the FQDN of the domain that hosts Microsoft Active Directory. For example: domain.example.com. 3. In the **Password** field, type the password of the Microsoft Active Directory account. 4. In the **Domain controller discovery** drop-down list, click one of the following: • If you want automatic discovery, click **Automatic**. • If you want to specify the domain controller server, click **Select from list below**. Click + and type the FQDN of the server. Repeat this step to add additional servers. 5. 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. 6. In the **Global catalog discovery** drop-down list, click one of the following: • If you want automatic catalog discovery, click **Automatic**.

Directory type	Steps
	• If you want to specify the catalog server, click **Select from list below**. Click + and type the FQDN of the server. If necessary, repeat this step to specify additional servers. 7. Click **Save**.
LDAP directory	1. In the **LDAP server discovery** drop-down list, click one of the following: • If you want automatic discovery, click **Automatic**. In the **DNS domain name** field, type the DNS domain name. • If you want to specify the LDAP server, click **Select from list below**. Click + and type the FQDN of the server. Repeat this step to add additional servers. 2. 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 server. 3. In the **LDAP** port field, type the port number of the LDAP server. 4. In the **Authorization required** drop-down list, select whether BES10 Cloud must authenticate with the LDAP server. If you click **Yes**, type the username and password of the LDAP account. The username must be in distinguised name format (for example, CN=Megan Ball,OU=Sales,DC=example,DC=com). 5. In the **Search base** field, type the search base that you want to access (for example, OU=Users,DC=example,DC=com). 6. 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)). 7. 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**. 8. 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. 9. In the **First name** field, type the attribute for each user's first name (for example, givenName). 10. In the **Last name** field, type the attribute for each user's last name (for example, sn). 11. In the **Login attribute** field, type the attribute for each user's login attribute (for example, cn). This is the attribute for the value thats users will type to log in to BES10 Self-Service with their directory credentials. 12. In the **Email** field, type the attribute for each user's email (for example, mail).

Directory type	Steps
	13. In the **Display name** field, type the attribute for each user's display name (for example, displayName). 14. In the **Email profile account name** field, type the attribute for each user's email profile account name (for example, mail). 15. Click **Save**.

17. In the BES10 Cloud administration console, click **Settings**.
18. In the left pane, click **External integration** > **BlackBerry Cloud Connector**.
19. In the **Step 4: Test connection** section, click **Next**.

After you finish:

- If you want to install a second BlackBerry Cloud Connector for redundancy, repeat Download the installation and activation files and repeat this task on a different computer. When you configure a second instance, use the same directory configuration.
- If necessary, Configure proxy settings for the BlackBerry Cloud Connector.
- If you want to change the directory settings that you configured, in the BlackBerry Cloud Connector setup console, click the **edit** icon.
- If you want to delete a directory configuration, in the BlackBerry Cloud Connector setup console, click the **delete** icon.

Configure proxy settings for the BlackBerry Cloud Connector

When you activate the BlackBerry Cloud Connector, it sends data over HTTPS to enroll with BES10 Cloud. After it is activated, the BlackBerry Cloud Connector sends and receives data over TCP. You can configure the BlackBerry Cloud Connector to route HTTPS or TCP data through a proxy server that is behind your organization's firewall. The BlackBerry Cloud Connector does not support authentication with a proxy server.

Before you begin: Use an administrator account with the Security Administrator or Enterprise Administrator role.

1. In the BlackBerry Cloud Connector setup console, click **Settings** > **Proxy**.
2. Perform any of the following tasks:

Task	Steps
Route HTTPS enrolment data through a proxy server	1. Select the **Enable enrolment proxy** check box. 2. In the **Server name or IP address** field, type the FQDN or IP address of the proxy server. 3. In the **Port number** field, type the port number of the proxy server.
Route TCP data through a TCP proxy server	1. Select the **Enable TCP proxy** check box. 2. In the **Server name or IP address** field, type the FQDN or IP address of the proxy server.

Task	Steps
	3. In the **Port number** field, type the port number of the proxy server.

3. Click **Save**.

Troubleshooting

The BlackBerry Cloud Connector does not activate with BES10 Cloud

Description

After you upload the activation file and click Activate, you receive an error message that the activation was not successful.

Possible solutions

Try any of the following:

- Verify that you uploaded the latest activation file that you generated in the administration console. Only the latest activation file is valid.
- Activation files expire after 60 minutes. Generate and upload a new activation file, then try to activate again.

The BlackBerry Cloud Connector does not connect with the company directory

Description

After you specify the information for your company directory and click Save, you receive an error message that the BlackBerry Cloud Connector cannot connect with the directory.

Possible solutions

Try any of the following:

- Verify that you specified the correct directory settings.
- Verify that you specified the correct login information for the directory account, and that the account has the necessary permissions to access the directory.
- Review the most recent log file for details about why the BlackBerry Cloud Connector cannot access the directory. By default, the log files for the BlackBerry Cloud Connector are located in <*drive:*>:\Program Files\BlackBerry Cloud Connector\logs.

The BlackBerry Cloud Connector does not connect with BES10 Cloud

Description

When you test the connection between the BlackBerry Cloud Connector and BES10 Cloud, you receive an error message that the test was not successful.

Possible solutions

Try any of the following:

- Verify that the following outbound ports are open in your organization's firewall so that the BlackBerry Cloud Connector (and any proxy servers that you want it to use) can communicate with BES10 Cloud:
    - 3101 (TCP)
    - 443 (HTTPS)
- Review the most recent log file for details about why the BlackBerry Cloud Connector cannot connect with BES10 Cloud. By default, the log files for the BlackBerry Cloud Connector are located in <*drive:*>:\Program Files\BlackBerry Cloud Connector\logs.

View the status of the BlackBerry Cloud Connector

Before you begin: Use an administrator account with the Security Administrator, Enterprise Administrator, or Senior Helpdesk role.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration** > **BlackBerry Cloud Connector**.

Verify the connection with BES10 Cloud

To help you troubleshoot issues, you can verify the connection between the BlackBerry Cloud Connector and BES10 Cloud. The following task verifies the connection for each instance that you installed.

Before you begin: Use an administrator account with the Security Administrator or Enterprise Administrator role.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration** > **BlackBerry Cloud Connector**.
3. Click **Poll now**.

Change when user data is synchronized with the directory

BES10 Cloud synchronizes user data with your company directory each day at the same time. You can view the default time in the administration console. You can change when the automatic synchronization begins. To minimize the performance impact, try to schedule the synchronization at a time when user activity is low.

If you want to start the synchronization process manually for an individual user, see Refresh user account information.

Before you begin: Use an administrator account with the Security Administrator or Enterprise Administrator role.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration** > **Company directory**.
3. In the **Synchronization time** drop-down lists, select the synchronization time.
4. Click **Save**.

After you finish: If you want to turn off user data synchronization, clear the **Turn on synchronization** check box.

Getting ready to manage iOS devices

Obtaining an APNs certificate to manage iOS devices

APNs is the Apple Push Notification Service. You must obtain and register an APNs certificate if you want to use BES10 Cloud to manage iOS devices. If you set up more than one BES10 Cloud domain, each domain requires an APNs certificate.

You can obtain and register the APNs certificate using the first login wizard or by using the external integration section of the administration console.This section explains how to complete this task using the external integration section of the administration console.

To obtain and register an APNs certificate, you must perform the following tasks:

- Obtain a signed CSR from BlackBerry
- Request an APNs certificate from Apple
- Register the APNs certificate

Note: Each APNs certificate is valid for one year. The administration console displays the expiry date. You must renew the APNs certificate before the expiry date, using the same Apple ID that you used to obtain the certificate. If the certificate expires, iOS devices do not receive data from BES10 Cloud. If you register a new APNs certificate, iOS device users must reactivate their devices to receive data.

For more information, visit https://developer.apple.com to read *Issues with Sending Push Notifications* in article TN2265.

It is a best practice to access the administration console and the Apple Push Certificates Portal using the Google Chrome browser or the Safari browser. These browsers provide optimal support for requesting and registering an APNs certificate.

Data flow: Sending data to an iOS device

1. BES10 Cloud sends a notification to the APNs.
2. The APNs authenticates BES10 Cloud using the APNs certificate that you registered.
3. The APNs sends the notification to the iOS device.
4. The iOS device receives the notification and retrieves the data from BES10 Cloud.

Overview: Getting ready to manage iOS devices

To obtain and register an APNs certificate, perform the following actions:

1	Obtain a signed CSR from BlackBerry.
2	Use the signed CSR to request an APNs certificate from Apple.
3	Register the APNs certificate.

Obtain a signed CSR from BlackBerry

You must obtain a signed CSR from BlackBerry before you can obtain an APNs certificate.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration** > **iOS management**.
3. Click **Get APNs Certificate**.

   If you want to renew the current APNs certificate, click **Renew certificate** instead.
4. In the **Step 1 of 3 - Download signed CSR certificate from BlackBerry** section, click **Download certificate**.
5. Click **Save** to save the signed CSR file (.scsr) to your computer.

After you finish: Request an APNs certificate from Apple.

Request an APNs certificate from Apple

Before you begin: Download and save the signed CSR provided by BlackBerry.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration** > **iOS management**.
3. In the **Step 2 of 3 - Request APNs certificate from Apple** section, click **Apple Push Certificate Portal**. You are directed to the Apple Push Certificates Portal.
4. Sign in to the Apple Push Certificates Portal using a valid Apple ID.
5. Follow the instructions to upload the signed CSR (.scsr).
6. Download and save the APNs certificate (.pem) on your computer.

After you finish: Register the APNs certificate.

Register the APNs certificate

Before you begin: Request an APNs certificate from Apple using the signed CSR from BlackBerry and save the APNs certificate on your computer.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration** > **iOS management**.
3. In the **Step 3 of 3 - Register APNs certificate** section, click **Browse**. Navigate to and select the APNs certificate (.pem).
4. Click **Submit**.

After you finish:

- To test the connection between BES10 Cloud and the APNs server, click **Test APNS certificate**.
- To view the status and expiry date of the APNs certificate, click **Settings** > **External integration** > **iOS management**. For more information about renewing the APNs certificate, see Renew the APNs certificate.

Renew the APNs certificate

The APNs certificate is valid for one year. You must renew the APNs certificate each year before it expires.

Before you begin:

- Obtain a new signed CSR from BlackBerry (see Obtain a signed CSR from BlackBerry).

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration** > **iOS management**.
3. In the **Step 2 of 3 - Request APNs certificate from Apple** section, click **Apple Push Certificate Portal**. You are directed to the Apple Push Certificates Portal.
4. Sign in to the Apple Push Certificates Portal using the same Apple ID that you used to obtain the original APNs certificate.
5. Follow the instructions to renew the APNs certificate (.pem). You will need to upload the new signed CSR.
6. Download and save the renewed APNs certificate on your computer.
7. In the **Step 3 of 3 - Register APNs certificate** section, click **Browse**. Navigate to and select the renewed APNs certificate.
8. Click **Submit**.

After you finish:

- To test the connection between BES10 Cloud and the APNs server, click **Test APNS certificate**.
- To view the status and expiry date of the APNs certificate, click **Settings** > **External integration** > **iOS management**.

Troubleshooting APNs

The APNs certificate does not match the CSR. Provide the correct APNs file (.pem) or submit a new CSR.

Description

You may receive an error message when you try to register the APNs certificate if you did not upload the most recently signed CSR file from BlackBerry to the Apple Push Certificates Portal.

Possible solution

If you downloaded multiple CSR files from BlackBerry, only the last one that you downloaded is valid. If you know which CSR is the most recent, return to the Apple Push Certificates Portal and upload it. If you are not sure which CSR is the most recent, obtain a new one from BlackBerry, then return to the Apple Push Certificates Portal and upload it.

I cannot activate iOS devices

Possible cause

If you are unable to activate iOS devices, the APNs certificate may not be registered correctly.

Possible solution

Perform one or more of the following actions:

- In the administration console, on the menu bar, click **Settings** > **External integration** > **iOS management**. Verify that the APNs certificate status is "Installed." If the status is not correct, try to register the APNs certificate again.
- Click **Test APNS certificate** to test the connection between BES10 Cloud and the APNs server.
- If necessary, obtain a new signed CSR from BlackBerry and a new APNs certificate.

Simple

Controlling how devices connect to work resources

About profiles

A profile contains configuration information such as email settings, network settings, or certificates. You can specify settings for BlackBerry 10, iOS, and Android devices in the same profile, and then assign the profile to users or groups.

Profiles are an efficient way for your organization to configure devices. If you need to specify many settings or configure a large number of devices, profiles allow you to store all the settings for a specific configuration in one place and quickly deliver the settings to the appropriate devices.

About variables

BES10 Cloud supports default and custom injection variables.

Default injection variables represent standard account attributes (for example, username) and other attributes (for example, server address used for device activation). You can use custom injection variables to define additional attributes.

You can use variables in profiles and to customize compliance notifications and activation email messages. IT policies do not support variables.

Custom injection variables

You can use labels to define the attributes and passwords that custom injection variables represent. For example, you can keep the default label "Password Variable 1" or change it to a descriptive label such as "VPN password." When you create or update a user account, labels are used as field names and you specify the appropriate values for the custom injection variables that your organization uses. All user accounts support custom injection variables, including administrator user accounts.

Custom injection variables support either text values or masked text values. For security reasons, you should use custom injection variables that support masked text values to represent passwords.

You can use the following custom injection variables in BES10 Cloud:

Variable name	Description
%custom1%, %custom2%, %custom3%, %custom4%, %custom5%	You can use up to five different variables for attributes that you define (text values).
%custom_pswd1%, %custom_pswd2%, %custom_pswd3%, %custom_pswd4%, %custom_pswd5%	You can use up to five different variables for passwords that you define (masked text values).

Define custom injection variables

To define the attributes and passwords that custom injection variables represent, you can change the default labels to labels that you specify.

1. On the menu bar, click **Settings**.
2. In the left pane, click **General settings** > **Custom variables**.
3. Verify that the **Show custom variables when adding or editing a user** check box is selected.
4. Update the label for each custom injection variable that you plan to use. The labels are used as field names in the **Custom variables** section when you create or update a user account.
5. Click **Save**.

Using custom injection variables

After you define custom injection variables, you must specify the appropriate values when you create or update a user account. You can then use custom injection variables in the same way as default injection variables. You specify the variable name when you create profiles or customize compliance notifications and activation email messages.

Example: Using the same VPN profile for several users who have their own VPN passwords

In the following example, "VPN password" is the label that you specified for the %custom_pswd1% variable and it's used as a field name in the Custom variables section when you update a user account.

1. Search for a user account.
2. In the search results, click the name of a user account.
3. Click the **edit** icon.
4. Expand **Custom variables**.
5. In the **VPN password** field, type a user's VPN password.
6. Click **Save**.
7. Repeat steps 1 to 6 for each user that will use the VPN profile.
8. When you create the VPN profile, type **%custom_pswd1%** in the **Password** field.

Using variables in profiles

You can use variables in a profile to reference values instead of specifying the actual values. When the profile is sent to devices, any variables in the profile are replaced with the values that they represent.

Variables in profiles help you to efficiently manage profiles for the users and groups in your organization. Variables provide more flexibility for profiles and can help limit the number of profiles that you require for each profile type. For example, you can create a single VPN profile for multiple users that specifies the %UserName% variable instead of creating a separate VPN profile for each user that specifies the username value.

You can use a variable in any text field in a profile, except the Name field and the Description field. For example, you can specify "%UserName%@example.com" in the Email address field in an Exchange ActiveSync profile.

You can use the following default injection variables in profiles:

Variable name	Description
%UserEmailAddress%	Email address of the user
%UserName%	Username of the user

You can also use custom injection variables in profiles. For more information, see Custom injection variables.

Controlling how devices connect to work resources

In the Policies and Profiles library, you can create and manage profiles that control how devices connect to work resources. You can use profiles to specify the certificates that devices can use for authentication and the settings that devices use to connect to a work mail server, proxy server, work VPN, and work Wi-Fi network.

The following table lists profiles in the order that you should create them. You can associate profiles listed earlier with profiles listed later. For example, if you create a Wi-Fi profile first, you cannot associate a proxy profile with the Wi-Fi profile when you create it. After you create a proxy profile, you must change the Wi-Fi profile to associate the proxy profile with it.

Profile	Description	Can be assigned to	Can be associated with	Applicable devices
CA certificate profile	This profile specifies a CA certificate that devices can use to establish trust with a work network or server.	• Users • Groups	• VPN profiles (BlackBerry 10 only) • Wi-Fi profiles	• BlackBerry 10 • iOS • Android
Shared certificate profile	This profile specifies a client certificate that devices can use to authenticate users with a work network or server. BES10 Cloud sends the same client certificate to every user that the profile is assigned to.	• Users • Groups	• Exchange ActiveSync profiles • VPN profiles (iOS only) • Wi-Fi profiles	• iOS • Android
User certificate profile	This profile specifies a client certificate that devices can use to authenticate a user with a work network or server. User certificate profiles are not available in the Policies and Profiles library. They apply only to individual user accounts and are created and assigned on the User summary tab for a user account.	• Users	—	• iOS • Android
Exchange ActiveSync profile	This profile specifies how devices connect to a work mail server and synchronize data using Exchange ActiveSync.	• Users • Groups	—	• BlackBerry 10 • iOS • Android
Proxy profile	This profile specifies how devices use a proxy server to	• Users (iOS only) • Groups (iOS only)	• VPN profiles • Wi-Fi profiles	• BlackBerry 10

Profile	Description	Can be assigned to	Can be associated with	Applicable devices
	access web services on the Internet or a work network.			• iOS
VPN profile	This profile specifies how devices connect to a work VPN.	• Users • Groups	• Wi-Fi profiles (BlackBerry 10 only)	• BlackBerry 10 • iOS
Wi-Fi profile	This profile specifies how devices connect to a work Wi-Fi network.	• Users • Groups	—	• BlackBerry 10 • iOS • Android

How BES10 Cloud chooses which connection profile to assign

Only one Exchange ActiveSync profile and one proxy profile can be assigned to each user account. BES10 Cloud uses the following rules to determine which Exchange ActiveSync profile or proxy profile to assign to a user account:

- An Exchange ActiveSync profile or proxy profile assigned to a user account directly takes precedence over a profile of the same type assigned indirectly by group.
- If a user is a member of multiple groups that have different Exchange ActiveSync profiles or proxy profiles, BES10 Cloud uses the profile ranking that you specify. For more information, see Rank profiles.

Creating CA certificate profiles

You might need to distribute CA certificates to devices if the devices use certificate-based authentication to connect to a network or server in your organization’s environment, or if your organization uses S/MIME. When the CA certificates for your organization's network and server certificates are stored on devices, the devices can trust your networks and servers when they make secure connections. When the CA certificates for your organization's S/MIME certificates are stored on devices, the devices can trust the sender's certificate when a secure email message is received.

Many CA certificates that are used for different purposes can be stored on a device. You can use certificate profiles to send CA certificates to devices. CA certificates have a .der file extension.

Create a CA certificate profile

1. On the menu bar, click **Policies and Profiles**.
2. Click the + icon beside **CA certificate**.
3. 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.
4. In the **Certificate file** field, click **Browse** to locate the certificate file.
5. If the CA certificate is sent to BlackBerry devices, specify one or more of the following certificate stores to send the certificate to on the device:
    - Browser certificate store
    - VPN certificate store
    - Wi-Fi certificate store
    - Enterprise certificate store
6. Click **Add**.

Related information
Assign an IT policy or profile to a user group, on page 85
Assign an IT policy or profile to a user account, on page 94

CA certificate stores on BlackBerry 10 devices

CA certificates that are sent to BlackBerry 10 devices can be stored in different certificate stores, depending on the purpose of the certificate.

Store	Description
Browser certificate store	The work browser on BlackBerry 10 devices uses the certificates in this store to establish SSL connections with servers in your organization's environment. Devices that are running BlackBerry 10 OS version 10.0 also use the certificates in this store to authenticate S/MIME-protected email messages that are received.

Store	Description
VPN certificate store	BlackBerry 10 devices use certificates in this store for VPN connections. You must set the "Trusted certificate source" setting in the VPN profile to "Trusted certificate store" to use the certificates in this store for work VPN connections.
Wi-Fi certificate store	BlackBerry 10 devices use certificates in this store for Wi-Fi connections. You must set the "Trusted certificate source" setting in the Wi-Fi profile to "Trusted certificate store" to use certificates in this store for work Wi-Fi connections.
Enterprise certificate store	Devices that are running BlackBerry 10 OS version 10.1 or later use certificates in this store to authenticate S/MIME-protected email messages that are received.

Creating shared certificate profiles

You might need to distribute client certificates to devices if the devices use certificate-based authentication to connect to a network or server in your organization’s environment. Shared certificate profiles assign the same client certificate to multiple user accounts and send the certificate to users' devices. The devices present the client certificate for authentication to a network or server in your organization's environment. The client certificate has a .pfx or .p12 file extension.

Shared certificate profiles are only supported by iOS and Android devices.

To assign a client certificate to an individual user account, use a user certificate profile.

Create a shared certificate profile

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

Related information
Assign an IT policy or profile to a user group, on page 85
Assign an IT policy or profile to a user account, on page 94

Creating Exchange ActiveSync profiles

You can use Exchange ActiveSync profiles to specify how devices connect to your organization's mail server and synchronize email messages and organizer data using Exchange ActiveSync. You can also use Exchange ActiveSync profiles to extend email security on BlackBerry 10 and iOS devices using S/MIME.

For more information about the profile settings, see the *BES10 Cloud Policy and Profile Reference Guide.*

Extending email security using S/MIME

You can extend email security for BlackBerry 10 and iOS device users by enabling S/MIME. S/MIME provides a standard method of encrypting and signing email messages. Users can sign, encrypt, or sign and encrypt email messages using S/MIME protection when they use a work email address. S/MIME cannot be enabled for personal email addresses.

You enable S/MIME for users in an Exchange ActiveSync profile. You can force BlackBerry 10 device users to use S/MIME, but not iOS device users. When S/MIME use is optional, a user can enable S/MIME on the device and specify whether to encrypt, sign, or encrypt and sign email messages.

To sign and encrypt email messages, users must store their private keys and a certificate for each recipient on their devices. Users can store their private keys and certificates by importing the files from a work email message.

For more information about S/MIME, see the *BES10 Cloud Security Technical Overview*.

Create an Exchange ActiveSync profile

Before you begin:

- If you use certificate-based authentication for iOS devices, create a CA certificate profile and a shared certificate profile and assign them to users.
- To use Exchange ActiveSync profiles for Android devices, the devices must meet one of the following requirements:
    - The device must have the TouchDown app installed. For more information about the TouchDown app, visit nitrodesk.com.
    - The device must be a Motorola device that supports the Enterprise Device Management API. See Motorola Enterprise Device Management SDK: Getting Started to view a list of Motorola devices that support the Enterprise Device Management API. If both TouchDown and the Enterprise Device Management API are present on an Android device, BES10 Cloud uses TouchDown to apply the profile.

1. On the menu bar, click **Policies and Profiles**.
2. Click the + icon beside **Exchange ActiveSync**.
3. Type a name and description for the profile.
4. If required, type the domain name of the mail server.
5. 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%**.

6. Type the host name or IP address of the Exchange ActiveSync server.
7. If the mail server requires SSL authentication, select **Use SSL**.
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. Click the tab for each device type in your organization and configure the appropriate values for each profile setting.
10. Click **Add**.

After you finish: If you create more than one Exchange ActiveSync profile, Rank profiles.

Related information
Assign an IT policy or profile to a user group, on page 85
Assign an IT policy or profile to a user account, on page 94

Creating proxy profiles

You can use proxy profiles to specify how devices use a proxy server to access web services on the Internet or a work network. Proxy profiles are not supported on Android devices.

Device type	Proxy profile assignment
BlackBerry	You can associate a proxy profile with a Wi-Fi profile or a VPN profile.
iOS	You can use any of the following options: • You can associate a proxy profile with a Wi-Fi profile or a VPN profile. • You can assign a proxy profile to users or groups. If a proxy profile is already assigned, the new profile replaces the existing profile. **Note:** A proxy profile assigned to users or groups is a global proxy for iOS devices and takes precedence over a proxy profile that is associated with a Wi-Fi profile or VPN profile. iOS devices use the global proxy settings for all HTTP connections.

Create a proxy profile

When you create a proxy profile, the default proxy type is PAC configuration. If your organization uses a PAC file to define proxy rules, the profile uses the proxy server settings from the PAC file that you specify. Otherwise, you can select manual configuration and specify the proxy server settings directly in the profile.

1. On the menu bar, click **Policies and Profiles**.
2. Click the + icon beside **Proxy**.
3. Type a name and description for the proxy profile.
4. Perform one of the following tasks:

Task	Steps
Specify PAC configuration settings	1. In the **PAC URL** field, type the URL for the web server that hosts the PAC file and include the PAC file name (for example, http://www.example.com/PACfile.pac). 2. If necessary, specify the username and password to authenticate with the proxy server. 3. On the **BlackBerry** tab, in the **User can edit** drop-down list, click the proxy settings that BlackBerry 10 device users can change. The default setting is **Read only**.
Specify manual configuration settings	1. In the **Type** drop-down list, click **Manual configuration**. 2. In the **Host** field, type the FQDN or IP address of the proxy server. 3. In the **Port** field, type the port number of the proxy server.

Task	Steps
	4. If necessary, specify the username and password to authenticate with the proxy server. 5. On the **BlackBerry** tab, perform the following actions: a In the **User can edit** drop-down list, click the proxy settings that BlackBerry 10 device users can change. The default setting is **Read only**. b Optionally, you can specify a list of addresses that users can access directly from their BlackBerry 10 devices without using the proxy server. In the **Exclusion list** field, type the addresses (FQDN or IP) and use a semicolon (;) to separate the values in the list.

5. Click **Add**.

After you finish: If you create more than one proxy profile, Rank profiles.

Related information
Assign an IT policy or profile to a user group, on page 85
Assign an IT policy or profile to a user account, on page 94

Creating VPN profiles

You can use VPN profiles to specify how users connect to a work VPN. You can assign VPN profiles to users or groups. For BlackBerry 10 devices, you can also associate a VPN profile with a Wi-Fi profile. VPN profiles are not supported on Android devices.

Note: To allow affected third-party devices to store the XAuth password, you can modify the group-policy attributes of the VPN profile in your Cisco VPN system to include the password-storage enable option. For more information, visit www.blackberry.com/go/kbhelp to read KB30353.

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. For more information about the profile settings for each device type, see the *BES10 Cloud Policy and Profile Reference Guide*.

Before you begin:

- If BlackBerry 10 devices use certificate-based authentication for work VPN connections, create a CA certificate profile and assign it to users.
- If iOS devices use certificate-based authentication for work VPN connections, create a shared certificate profile and assign it to users.
- If BlackBerry 10 or iOS devices use a proxy server for work VPN connections, create a proxy profile.

1. On the menu bar, click **Policies and Profiles**.
2. Click the + icon beside **VPN**.
3. Type a name and description for the VPN profile. This information is displayed on devices.
4. Optionally, clear the check box for any device type that you do not want to configure the profile for.
5. 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 environment. If your organization requires that users provide a username and password to connect to the VPN and the profile is for multiple users, type **%UserName%** in the **Username** field.
6. Repeat step 5 for each device type in your organization.
7. Click **Add**.

Related information

Assign an IT policy or profile to a user group, on page 85
Assign an IT policy or profile to a user account, on page 94

Creating Wi-Fi profiles

You can use Wi-Fi profiles to specify how devices connect to a work Wi-Fi network within the firewall. You can assign Wi-Fi profiles to users or groups.

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. For more information about the profile settings for each device type, see the *BES10 Cloud Policy and Profile Reference Guide*.

Before you begin:

- If any devices use certificate-based authentication for work Wi-Fi connections, create a CA certificate profile and assign it to users. For iOS or Android devices, also create a shared certificate profile and assign it to users.
- If BlackBerry 10 or iOS devices use a proxy server for work Wi-Fi connections, create a proxy profile.
- If BlackBerry 10 devices use a VPN for work Wi-Fi connections, create a VPN profile.

1. On the menu bar, click **Policies and Profiles**.
2. Click the + icon beside **Wi-Fi**.
3. Type a name and description for the Wi-Fi profile. This information is displayed on devices.
4. In the **SSID** field, type the network name of the Wi-Fi network.
5. If the Wi-Fi network does not broadcast the SSID, select the **Hidden network** check box.
6. Optionally, clear the check box for any device type that you do not want to configure the profile for.
7. 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 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, type **%UserName%** in the **Username** field.
8. Repeat step 7 for each device type in your organization.
9. Click **Add**.

Related information

Assign an IT policy or profile to a user group, on page 85
Assign an IT policy or profile to a user account, on page 94

Managing profiles

In the Policies and Profiles library, you can manage the profiles that your organization uses. You can rank profiles, view information about a profile, remove a profile from users or groups, change profile settings, or delete a profile.

Rank profiles

You can rank Exchange ActiveSync profiles, proxy profiles, compliance profiles, and activation profiles. When a user is a member of multiple groups that have different profiles of the same type, BES10 Cloud uses the ranking that you specify to determine which profile to assign to the user account.

1. On the menu bar, click **Policies and Profiles**.
2. In the left pane, expand the profile type.
3. Click **Rank** <***profile_type***> **profiles**.
4. Use the arrows to move profiles up or down the ranking.
5. Click **Save**.

View a profile

In the Policies and Profiles library, you can view the following information about a profile:

- Settings common to all device types and settings specific to each device type
- List of users assigned the profile and number of users assigned the profile (indirectly and directly)
- List of groups assigned the profile and number of groups assigned the profile

1. On the menu bar, click **Policies and Profiles**.
2. In the left pane, expand the profile type.
3. Click the name of the profile that you want to view.

Remove a profile from users or groups

If you assigned a profile to users directly, you can remove the profile from users. If you assigned a profile to users indirectly by group, you can either remove the profile from the group or remove users from the group. When you remove a profile from groups, the profile is removed from every user that belongs to the selected groups.

1. On the menu bar, click **Policies and Profiles**.
2. In the left pane, expand the profile type.
3. Click the name of the profile that you want to remove from users or groups.
4. Perform one of the following tasks:

Task	Steps
Remove a profile from users	1. Click the **Assigned to users** tab. 2. If necessary, search for users. 3. Select the users that you want to remove the profile from. 4. Click **Remove from user**.
Remove a profile from groups	1. Click the **Assigned to groups** tab. 2. If necessary, search for groups. 3. Select the groups that you want to remove the profile from. 4. Click **Remove from group**.

Change profile settings

1. On the menu bar, click **Policies and Profiles**.
2. In the left pane, expand the profile type.
3. Click the name of the profile that you want to change.
4. Click the **edit** icon.
5. Make changes to any common settings.
6. Make changes on the appropriate tab for each device type.
7. Click **Save**.

After you finish: To change the profile ranking, see Rank profiles.

Delete a profile

When you delete a profile, the profile is removed from every user that it is assigned to. To delete a profile that is associated with other profiles, you must first remove all existing associations. For example, before you can delete a proxy profile that is associated with a VPN profile and a Wi-Fi profile, you must change the associated proxy profile value in both the VPN profile and the Wi-Fi profile.

1. On the menu bar, click **Policies and Profiles**.
2. In the left pane, expand the profile type.
3. Click the name of the profile that you want to delete.
4. Click the **delete** icon.
5. Click **Delete**.

Setting your organization's standards for devices

Enforcing compliance rules for iOS and Android devices

You can use compliance profiles to encourage iOS and Android device users to follow your organization’s standards for the use of mobile devices. A compliance profile defines the device conditions that are not acceptable in your organization. For example, you can choose to disallow jailbroken or rooted devices.

A compliance profile specifies the following information:

- Conditions that would make a device non-compliant with BES10 Cloud
- Notifications that users receive if they violate the compliance conditions, and the amount of time that users have to correct the issue
- Action that is taken if the user does 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

BES10 Cloud includes a default compliance profile, and gives you the option to create and assign custom compliance profiles. Any user accounts that are not assigned a custom compliance profile are assigned the default compliance profile. You can change the settings of the default compliance profile.

How BES10 Cloud chooses which compliance profile to assign

Only one compliance profile can be assigned to each user account. BES10 Cloud uses the following rules to determine which compliance profile to assign to a user account:

- A compliance profile assigned to a user account directly takes precedence over a compliance profile assigned indirectly by group.
- If a user is a member of multiple groups that have different compliance profiles, BES10 Cloud uses the profile ranking that you specify. For more information, see Rank profiles.
- The default compliance profile is assigned to a user account only if a compliance profile is not assigned to the user directly or through group membership.

Creating and managing compliance profiles

Default compliance profile

Device conditions

Condition	Permitted or Not permitted
Jailbroken or rooted device	Permitted
Non-assigned application is installed	Permitted

Condition	Permitted or Not permitted
Required application is not installed	Permitted

Notifications sent to users

Notification type	Message
Email notification sent out when violation is detected	Your device is not compliant with your organization's policies. If this condition persists your administrator might limit access to the organization's data from your device, delete the organization's data on your device, or delete all content and settings from your device.
Device notification sent out when violation is detected	This device does not comply with requirements. If this persists your access might be limited or all device data deleted.

Change the default compliance profile

You can change the settings of the default compliance profile. The default compliance profile is assigned to a user account only if the user is not assigned a compliance profile directly or through group membership.

1. On the menu bar, click **Policies and Profiles**.
2. In the left pane, click **Compliance** > **Default**.
3. Click the **edit** icon.
4. Perform one of the following actions:
    - To configure compliance conditions for iOS devices, click the **iOS** tab.
    - To configure compliance conditions for Android devices, click the **Android** tab.
5. Perform any of the following actions:
    - If you want jailbroken or rooted devices to be considered non-compliant, select the **Jailbroken or rooted device** check box.
    - If you want devices with applications that you did not install to be considered non-compliant, select the **Non-assigned application is installed** check box.
    - If you want devices that do not have a required application to be considered non-compliant, select the **Required application is not installed** check box.
6. For each condition you selected in step 5, choose the action that you want BES10 Cloud to perform when a user's device is non-compliant, and complete the steps:

Action	Steps
Automatically notify the user that the device is non-compliant, and carry	1. In the **Enforcement action** drop-down list, click **Prompt for compliance**.

Action	Steps
out an enforcement action if the user does not correct the issue.	2. In the **Prompt method** drop-down list, click the type of message to send to the user. 3. In the **Prompt count** field, type the number of times the notification message is sent before BES10 Cloud carries out the action. 4. In the **Prompt interval** field and drop-down list, specify the time between prompts. 5. In the **Prompt interval expired action** drop-down list, click the action that you want BES10 Cloud to take when the prompt period expires: • If you do not want an enforcement action, select **None**. • To prevent the user from accessing work resources and applications from the device, select **Untrust**. Data and applications are not deleted from the device. • To delete work data from the device, select **Delete only work data**. • To delete all data from the device, select **Delete all device data**.
Prevent the user from accessing work resources and applications from the device. Data and applications are not deleted from the device.	1. In the **Enforcement action** drop-down list, click **Untrust**.
Delete work data from the device.	1. In the **Enforcement action** drop-down list, click **Delete only work data**.
Delete all data from the device.	1. In the **Enforcement action** drop-down list, click **Delete all device data**.

7. Repeat steps 4 to 6 if you want to configure the compliance conditions for a different device type.
8. If you chose to send a notification message to users when their devices become non-compliant, perform any of the following actions:
    - To change the email notification, expand **Email notification sent out when violation is detected**. Change the subject and message.
    - To change the device notification, expand **Device notification sent out when violation is detected**. Change the message.

   If you want to use variables to populate notifications with user, device, and compliance information, see Using variables in compliance notifications. You can also define and use your own custom variables using the administration console. For more information, see Custom injection variables.
9. Click **Save**.

Create a compliance profile

1. On the menu bar, click **Policies and Profiles**.
2. Click the + icon beside **Compliance**.
3. Type a name and a description for the compliance profile.
4. Perform one of the following actions:
    - To configure compliance conditions for iOS devices, click the **iOS** tab.
    - To configure compliance conditions for Android devices, click the **Android** tab.
5. Perform any of the following actions:
    - If you want jailbroken or rooted devices to be considered non-compliant, select the **Jailbroken or rooted device** check box.
    - If you want devices with applications that you did not install to be considered non-compliant, select the **Non-assigned application is installed** check box.
    - If you want devices that do not have a required application to be considered non-compliant, select the **Required application is not installed** check box.
6. For each condition you selected in step 5, choose the action that you want BES10 Cloud to perform when a user's device is non-compliant, and complete the steps:

Action	Steps
Automatically notify the user that their device is non-compliant, and carry out an enforcement action if the user does not correct the issue.	1. In the **Enforcement action** drop-down list, click **Prompt for compliance**. 2. In the **Prompt method** drop-down list, click the type of message to send to the user. 3. In the **Prompt count** field, type the number of times the notification message is sent before BES10 Cloud carries out the action. 4. In the **Prompt interval** field and drop-down list, specify the time between prompts. 5. In the **Prompt interval expired action** drop-down list, click the action that you want BES10 Cloud to take when the prompt period expires: • If you do not want an enforcement action, select **None**. • To prevent the user from accessing work resources and applications from the device, select **Untrust**. Data and applications are not deleted from the device. • To delete work data from the device, select **Delete only work data**. • To delete all data from the device, select **Delete all device data**.
Prevent the user from accessing work resources and applications from the device. Data and	1. In the **Enforcement action** drop-down list, click **Untrust**.

Action	Steps
applications are not deleted from the device.	
Delete work data from the device.	1. In the **Enforcement action** drop-down list, click **Delete only work data**.
Delete all data from the device.	1. In the **Enforcement action** drop-down list, click **Delete all device data**.

7. Repeat steps 4 to 6 if you want to configure the compliance conditions for a different device type.
8. If you chose to send a notification message to users when their devices become non-compliant, perform any of the following actions:
    - To change the email notification, expand **Email notification sent out when violation is detected**. Change the subject and message.
    - To change the device notification, expand **Device notification sent out when violation is detected**. Change the message.

    If you want to use variables to populate notifications with user, device, and compliance information, see Using variables in compliance notifications. You can also define and use your own custom variables using the administration console. For more information, see Custom injection variables.
9. Click **Add**.

After you finish: Rank profiles.

Related information
Assign an IT policy or profile to a user group, on page 85
Assign an IT policy or profile to a user account, on page 94

Change a compliance profile

1. On the menu bar, click **Policies and Profiles**.
2. In the left pane, expand **Compliance**.
3. Click the compliance profile that you want to change.
4. Click the **edit** icon.
5. Make the necessary changes.
6. Click **Save**.

After you finish: To change the profile ranking, see Rank profiles.

Related information
Assign an IT policy or profile to a user group, on page 85
Assign an IT policy or profile to a user account, on page 94

Using variables in compliance notifications

If you want to customize the compliance notifications that BES10 Cloud sends to users, you can use any of the following variables to populate the message body with information about the user, the compliance rule that the user violated, and the enforcement action.

Variable	Description
%ComplianceApplicationList%	The list of applications that must be installed for the device to be in compliance with BES10 Cloud.
%ComplianceEnforcementAction%	The enforcement action that BES10 Cloud performs if the device is not in compliance.
%ComplianceEnforcementActionWithDescription%	The enforcement action that BES10 Cloud performs if the device is not in compliance, including a description of the enforcement action.
%ComplianceRuleViolated%	The compliance rule that the user violated to make the device non-compliant with BES10 Cloud.
%DeviceModel%	The user's device model.
%UserName%	The username of the user.

Delete a compliance profile

1. On the menu bar, click **Policies and Profiles**.
2. In the left pane, expand **Compliance**.
3. Click the compliance profile that you want to delete.
4. Click the **delete** icon.
5. Click **Delete**.

Filtering web content on iOS devices

You can use web content filter profiles to limit the websites that an iOS device user can view using Safari or other browser apps on the device. You can assign web content filter profiles to users or groups.

When you create a web content filter profile, you can choose the allowed websites option that supports your organization's standards for the use of mobile devices.

Note: This profile is supported only on devices that run iOS 7.0 and later and are supervised using Apple Configurator.

Allowed websites	Description
Specific websites	This option allows access to only the websites that you specify. A bookmark is created in Safari for each allowed website.
Limited adult content	This option enables automatic filtering to identify and block inappropriate content. You can also include specific websites using the following settings: • Permitted URLs: You can add one or more URLs to allow access to specific websites. Users can view websites in this list regardless of whether automatic filtering blocks access. • Blacklisted URLs: You can add one or more URLs to deny access to specific websites. Users cannot view websites in this list regardless of whether automatic filtering allows access.

Create a web content filter profile

When you create a web content filter profile, each URL that you specify must begin with http:// or https://. If necessary, you should add separate entries for http:// and https:// versions of the same URL. DNS resolution does not occur, so restricted websites could still be accessible (for example, if you specify http://www.example.com, users might be able to access the website using the IP address).

1. On the menu bar, click **Policies and Profiles**.
2. Click the + icon beside **Web content filter**.
3. Type a name and description for the web content filter profile.
4. Perform one of the following tasks:

Task	Steps
Allow access to specific websites only	1. In the **Allowed websites** drop-down list, verify that **Specific websites** is selected. 2. In the **Specific website bookmarks** section, click the + icon. 3. Perform the following actions: a In the **URL** field, type a web address that you want to allow access to.

Task	Steps
	b Optionally, in the **Bookmark path** field, type the name of a bookmark folder (for example, /Work/). c In the **Title** field, type a name for the website. d Click **Add**. 4. Repeat steps 2 and 3 for each allowed website.
Limit adult content	1. In the **Allowed websites** drop-down list, click **Limited adult content** to enable automatic filtering. 2. Optionally, perform the following actions: a Click the + icon beside **Permitted URLs**. b Type a web address that you want to allow access to. c Repeat steps 2.a and b for each allowed website. 3. Optionally, perform the following actions: a Click the + icon beside **Blacklisted URLs**. b Type a web address that you want to deny access to. c Repeat steps 3.a and b for each restricted website.

5. Click **Add**.

Controlling the capabilities of devices

Multiplatform

Using IT policies to restrict device functionality

An IT policy is a set of rules that restrict or allow features and functionality on BlackBerry 10, iOS, and Android devices. You can use IT policy rules to manage the security and behavior of devices. The available rules are determined by the device OS. For example, depending on the device OS and version, you might be able to use IT policy rules to:

- Enforce password requirements on devices
- Prevent users from using the camera
- Control connections that use Bluetooth wireless technology
- Force device data encryption

BES10 Cloud includes a Default IT policy with preconfigured rules for each device type. If an IT policy is not assigned to a user account or a group that the user belongs to, BES10 Cloud sends the Default IT policy to the user's devices.

BES10 Cloud automatically sends IT policies to devices when a user activates a device, when an assigned IT policy is updated, and when a different IT policy is assigned to a user or group. When a device receives a new or updated IT policy, the device applies the configuration changes in near real-time.

For more information about the IT policy rules for each device type, see the *BES10 Cloud Policy and Profile Reference Guide*.

How BES10 Cloud chooses which IT policy to assign

Only one IT policy can be assigned to each user account. BES10 Cloud uses the following rules to determine which IT policy to assign to a user account:

- An IT policy assigned to a user account directly takes precedence over an IT policy assigned indirectly by group.
- An IT policy assigned to a group takes precedence over the Default IT policy. If a user is a member of multiple groups that have different IT policies, BES10 Cloud uses the IT policy ranking that you specify. For more information, see Rank IT policies.
- The Default IT policy is assigned to a user account only if an IT policy is not assigned to the user directly or through group membership.

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 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 or exceed the minimum standards for your organization's security.

Create an IT policy

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

After you finish: Rank IT policies.

Related information
Assign an IT policy or profile to a user group, on page 85
Assign an IT policy or profile to a user account, on page 94

Rank IT policies

When a user is a member of multiple groups that have different IT policies, BES10 Cloud uses the ranking that you specify to determine which IT policy to assign to the user account.

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

Change an IT policy

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

After you finish: To change the IT policy ranking, see Rank IT policies.

Delete an IT policy

You cannot delete the Default IT policy. When you delete a custom IT policy, the IT policy is removed from every user that it is assigned to, and BES10 Cloud uses predefined rules to determine which IT policy should be assigned to the user instead. For more information, see How BES10 Cloud chooses which IT policy to assign.

1. On the menu bar, click **Policies and Profiles**.
2. In the left pane, expand **IT policies**.
3. Click the name of the IT policy that you want to delete.
4. Click the **delete** icon.
5. Click **Delete**.

Managing work apps on devices

Secure

Managing work apps on devices

You can make work apps available on BlackBerry 10 devices, iOS devices, and Android devices by adding the apps to the available app list and assigning the app or app group to user accounts or user groups. Apps added from BlackBerry World can be installed on compatible BlackBerry devices, apps added from App Store can be installed on compatible iOS devices, and apps added from Google Play can be installed on compatible Android devices.

Overview: Managing work apps

To manage apps, perform the following actions:

1. Add the apps that you want to manage to the available app list.
2. Optionally, create app groups to manage multiple apps at the same time.
3. Assign apps or app groups to user accounts or user groups so users can install them.

Adding and deleting apps from the available app list

The apps that you add to the app list are the apps that your organization wants to make available as work apps on devices.

Add a BlackBerry app to the available app list

1. On the menu bar, click **Apps**.
2. Click the **Add app** icon.
3. Click **BlackBerry World**.
4. In the search field, search for the app that you want to add. You can search by app name, vendor, or BlackBerry World URL.
5. In the dropdown box, select the country of the store that you want to search in.
6. Click **Search**.
7. In the search results, click **Add** to add an app.
8. On the app information screen, click **Add**.

Related information
Assign an app or app group to a user group, on page 86
Assign an app to a user, on page 95

Add an iOS app to the available app list

1. On the menu bar, click **Apps**.
2. Click the **Add app** icon.
3. Click **App Store**.
4. In the search field, search for the app that you want to add. You can search by app name, vendor, or App Store URL.
5. Click **Search**.
6. In the search results, click **Add** to add an app.
7. In the dropdown box, select the country of the store that you want to search in.
8. If you want to prevent apps on iOS 5 and later devices from being backed up to the iCloud online service, select the check box for that option. This option applies only to apps with a disposition marked as required. You set the disposition of the app when you assign the app to a user or group.
9. In the **Default installation method** drop-down list, perform one of the following actions:
    - If you want users to receive one prompt to install the app on their iOS 5 and later devices, select **Prompt once**. If users dismiss the prompt, they can install the app later using the Work Apps screen in the BES10 Client or the Work Apps icon on the device.
    - **No prompt**

    The default installation method applies only to apps with a disposition marked as required. You set the disposition of the app when you assign the app to a user or group.

Related information
Assign an app or app group to a user group, on page 86
Assign an app to a user, on page 95

Add an Android app to the available app list

Note: Add only apps to the available app list. Movies, music, and newsstand media cannot be delivered to devices. If you assign media to a user and set the disposition of the media as required, the device is subject to the enforcement action defined in the compliance profile that is assigned to it.

1. On the menu bar, click **Apps**.
2. Click the **Add app** icon.
3. Click **Google Play**.
4. In the **App name** field, type the app name.
5. In the **App description** field, type a description for the app.
6. In the **Vendor** field, type the name of the app vendor.
7. In the **App icon** field, click **Browse**. Locate and select an icon for the app. The supported formats are .png, .jpg, .jpeg, or .gif. Do not use Google Chrome to download the icon because an incompatible .webp image will be downloaded.
8. In the **App web address** field, type the web address of the app in Google Play.
9. Click **Add**.

Related information

Assign an app or app group to a user group, on page 86
Assign an app to a user, on page 95

Delete an app from the available app list

When you delete an app from the available app list, the app is unassigned from any users or groups that it is assigned to and it doesn't appear in a device's work app catalog.

1. On the menu bar, click **Apps**.
2. Select the check box beside the apps that you want to delete from the available app list.
3. Click the **delete** icon beside the **Add app** button.
4. Click **Delete**.

Managing app groups

App groups allow you to create a collection of apps that can be assigned to users or user groups at the same time. Grouping apps helps to increase efficiency and consistency when managing apps. For example, you can use app groups to group the same app for multiple device types, or to group apps for users with the same role in your organization.

Create an app group

Before you begin:

- Add the apps to the available app list

1. On the menu bar, click **Apps**.
2. Click the **Create app group** icon.
3. Type a name and description for the app group.
4. Click the + icon.
5. Select the apps that you want to add to the app group.
6. Click **Add**.

Edit an app group

1. On the menu bar, click **Apps**.
2. Click the app group that you want to edit.
3. Make the necessary edits.
4. Click **Save**.

Change whether an app is required or optional

You can change whether iOS apps or Android apps are required or optional. BlackBerry apps can be optional only. You can configure a compliance rule that performs actions when users do not install a required app. These apps are also reported as a compliance issue in the Non-assigned app installed list. For more information on compliance rules, see Create a compliance profile

1. On the menu bar, click **User & Devices**.
2. If the app that you want to change is assigned to a user account, in the search results, click the name of a user account.
3. If the app that you want to change is assigned to a group, in the left pane, click **Groups** to expand the list of user groups and click the name of the group.
4. In the **Assigned apps** section, click the disposition for the app that you want to change.
5. In the **Disposition** drop-down list for the app, perform one of the following actions:

    - To require users to follow the actions defined in the compliance profile assigned to them, 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

6. Click **Assign**.

View the status of apps and app groups assigned to user accounts

1. On the menu bar, click **Apps**.
2. Under **Assigned to users** for the app or app group that you want to view, click the number.
3. Click the **Assigned to *x* users** to view the user accounts that this app is assigned to.
4. View the **Assigned by** column to verify whether the app or app group was assigned directly to the user account or to a group.
5. View the **Status** column to verify whether an app was installed on a device. The following are the possible statuses:

    - **Installed**: The app was successfully installed on the user's device.
    - **Not installed**: The app has not been installed on the user's device yet.
    - **Cannot be installed**: The app is not supported on the user's devices.
    - **Not supported**: The device's OS does not support this app.

View which apps are assigned to user groups

1. On the menu bar, click **Apps**.
2. Under **Assigned to users** for the app that you want to view, click the number.

3. Click the **Assigned to *x* groups** to view the user groups that this app is assigned to.

Update the information in the available app list

You can update the app list to make sure that you have the latest information about the BlackBerryand iOS apps in the apps list. Information about Google Play apps must be updated manually. Updating the app information does not mean that the app is updated on a user’s device. Users receive update notifications for their work apps in the same way that they receive update notifications for their personal apps.

1. On the menu bar, click **Apps**.
2. Click **Update all apps**.

Set the organization name for BlackBerry World

You can add your organization's name to the BlackBerry World for Work corporate app storefront.

1. On the menu bar, click **Settings** > **BlackBerry World**.
2. In **Organization** name, type the name of your organization.

Managing groups, users, and administrators

Simple

Overview: Creating groups and users

To manage your organization's users and devices, perform the following actions:

1. Create user groups.
2. Create user accounts.
3. Create administrator accounts.

Creating and managing user groups

A user group is a collection of related users who share common properties. Administering users as a group is more efficient than administering individual users because properties can be set, applied, or changed for all members of the group at the same time.

Users can belong to more than one group at a time. You can assign an IT policy, profiles, and apps in the administration console when you create or update the settings for a user group. If you remove a user account from a user group, the user account remains in the list but it does not appear in the tab for the user group.

Create a user group

1. On the menu bar, click **Groups**.
2. Click the **add group** icon.
3. Type a name for the user group.
4. To add an IT policy, certificate, or profile to the user group, in the **IT policies and profiles** section, click the + icon and the select the policy or profile that you want to add.
5. From the drop-down list, select the IT policy, certificate or profile.
6. Click **Assign**.

   Note: If you want to remove an IT policy, or profile that you assigned, click **Remove**.

7. To assign an app to the user group, in the **Assigned apps** section, click the + icon.
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**. This option is not available for BlackBerry apps.
    - 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. Click **Assign**.
13. If required, perform one of the following actions for an assigned app

    - To view details about the app, click the app name.
    - To change the **Disposition** for an app:
      1. Click the disposition for the app.
      2. Select a new disposition.

    3. Click **Save**.

- To remove an assigned app, beside the app, click **Remove**.

14. When you are finished specifying the user group properties, click **Add**.

View a user group

1. On the menu bar, click **Groups**.
2. Search for the user group you want to view.
3. Click the user group.
4. Perform one of the following actions:
    - To view the users assigned to the user group, select the **Users** tab.
    - To view the IT policies or apps assigned to the user group, select the **Settings** tab.

Change the name of a user group

1. On the menu bar, click **Groups**.
2. Search for the user group you want to view.
3. Click the user group.
4. Click the **edit** icon.
5. Change the name of the user group.
6. Click **Save**.

Delete a user group

1. On the menu bar, click **Groups**.
2. Search for the user group you want to view.
3. Click the user group.
4. Click the **delete** icon.
5. Click **Delete**.

Export user account information from a user group

You can export user account information from the User tab.

1. On the menu bar, click **Groups**.
2. Search for the user group that has the user information that you want to export.

3. Click the user group.
4. Select the user information from the list that you want to export.
5. Click the **export** icon.
6. In your browser, perform one of the following actions:
    - To open the file, click **Open**.
    - To save the file, click **Save**.

Assigning an IT policy or profile to a user group

When you assign an IT policy or profile to a user group, it is assigned to all members of the group. You can assign an IT policy and the following profiles to a user group:

IT policy or profile	Assignment
IT policy	You can assign only one IT policy to a user group. If an IT policy is already assigned to the group, you can replace the existing IT policy with a different IT policy.
Exchange ActiveSync profile, proxy profile, compliance profile, activation profile	For each of these profiles, you can assign only one instance to a user group. If a profile is already assigned to the group, you can replace the existing profile with a different profile of the same type.
CA certificate profile, shared certificate profile, VPN profile, Wi-Fi profile, web content filter profile	For each of these profiles, you can assign more than one instance to a user group.

BES10 Cloud uses predefined rules to determine which IT policy or profile to assign to a user account (for example, if a user is a member of multiple groups that have different IT policies).

Related information

How BES10 Cloud chooses which connection profile to assign, on page 47
How BES10 Cloud chooses which compliance profile to assign, on page 60
How BES10 Cloud chooses which IT policy to assign, on page 71
How BES10 Cloud chooses which activation profile to assign, on page 105

Assign an IT policy or profile to a user group

1. On the menu bar, click **Groups**.
2. Search for a user group.
3. In the search results, click the name of a user group.
4. On the **Settings** tab, in the **IT policies and profiles** section, click the + icon.
5. Click **IT policy** or the profile type that you want to assign to the group.
6. Click the name of the IT policy or profile that you want to assign to the group.
7. Perform one of the following actions:

- If no IT policy or profile is assigned, or if more than one instance of the profile can be assigned, click **Assign**.
- If an IT policy is already assigned, or if a profile is already assigned and only one instance is allowed, click **Replace**.

Assign an app or app group to a user group

When you assign an app to a user group, the app is made available to all devices in the user group for that device type.

If a user account is a member of multiple user groups that have the same apps or app groups assigned to them, only one instance of the app or app group appears in the list of assigned apps for that user account. If the same app is assigned to a user group and directly to a user account, the settings (for example, whether the app is required) for the app assigned directly to the user account are applied.

Before you begin:

- Add the app to the available app list
- Optionally, add the apps to an app group

1. On the menu bar, click **Groups**.
2. Click the name of a group.
3. On the **Settings** tab, in the **Assigned apps** section, click the + icon.
4. In the search field, type the app name, vendor, or URL of the app that you want to add.
5. Select the check box beside the apps or app group that you want to assign to the user account.
6. Click **Next**.
7. In the **Disposition** drop-down list for the app, perform one of the following actions:
    - To require users to follow the actions defined for apps in the compliance profile assigned to them, select **Required**. This option is not available for BlackBerry apps.
    - 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
8. Click **Assign**.

Creating and managing user accounts

You can add user accounts directly to BES10 Cloud or you can add user accounts from your company directory using the BlackBerry Cloud Connector. You can also use a .csv file to add multiple user accounts to BES10 Cloud at the same time.

Create a local user account

1. On the menu bar, click **Users and Devices**.
2. Click the + icon beside **All users**.
3. In the **Username** field, type a unique username for the user account.
4. In the **First name** field, type a first name for the user account.
5. In the **Last name** field, type a last name for the user account.
6. In the **Display name** field, type a display name for the user account.
7. In the **Email address** field, type a contact email for the user account.
8. If groups exist in the **Group membership** list, select the groups that you want to add the user account to. Click the **right arrow** icon.
9. In the **Console password** field, specify a BES10 Self-Service password for the user account. This is also the password that user can use to access the administration console if you grant this user administrator permissions.
10. Select one of the following:

Task	Steps
Auto-generate device activation password and send email with activation instructions	To automatically generate an activation password: 1. Select **Auto-generate device activation password and send email with activation instructions**. 2. Specify the number of minutes, hours, or days that a user can activate a device before the activation password expires in the **Activation password expiration** field.
Set device activation password	To specify the activation password: 1. Select **Set device activation password**. 2. Type an activation password for the user account. 3. To send activation information to the user, click **Send email with activation instructions and activation password**. 4. Specify the number of minutes, hours, or days that a user can activate a device before the activation password expires in the **Activation password expiration** field.
Do not set device activation password	To specify an activation password later:

Task	Steps
	1. Select **Do not set device activation password**.

11. If you use custom injection variables, expand **Custom variables** and specify the appropriate values for the variables that you defined. For more information, see Custom injection variables.
12. Do one of the following:
    - To save the user account and create another user account, click **Save & New**.
    - To save the user account, click **Save**.

Add a user account from the company directory

If you have installed the BlackBerry Cloud Connector, you can add a user account directly from your company directory. For more information about the BlackBerry Cloud Connector, see Accessing your company directory.

1. On the menu bar, click **Users and Devices**.
2. Click the + icon beside **All Users**.
3. On the **Company directory** tab, search for a user account.
4. In the **Name** list, select the user account.
5. If groups exist in the **Group membership** list, select the groups that you want to add the user account to. Click the **right arrow** icon.
6. Select one of the following:

Task	Steps
Auto-generate device activation password and send email with activation instructions	To automatically generate an activation password: 1. Select **Auto-generate device activation password and send email with activation instructions**. 2. Specify the number of minutes, hours, or days that a user can activate a device before the activation password expires in the **Activation password expiration** field.
Set device activation password	To specify the activation password: 1. Select **Set device activation password**. 2. Type an activation password for the user account. 3. To send activation information to the user, click **Send email with activation instructions and activation password**. 4. Specify the number of minutes, hours, or days that a user can activate a device before the activation password expires in the **Activation password expiration** field.

Task	Steps
Do not set device activation password	To specify an activation password later: 1. Select **Do not set device activation password**.

7. If you use custom injection variables, expand **Custom variables** and specify the appropriate values for the variables that you defined. For more information, see Custom injection variables.
8. Do one of the following:
   - To save the user account and create another user account, click **Save and New**.
   - To save the user account, click **Save**.

Create user accounts from a .csv file

You can create the .csv file manually using the BES10 Cloud sample .csv file, which is available for download from the Import tab in the Add a user window.

About the user accounts .csv file

You can import user accounts in a .csv file into BES10 Cloud from to create many user accounts at once. Depending on your requirements, you can also specify group membership and activation settings for the user accounts by including the following columns in the .csv file:

Column Header	Description
Group membership	Assign one or more user groups to each user account. Use the semicolon (;) to separate multiple user groups. If you do not include the “Group membership” column, when you import the file, you are given the option to select the group that you want all of the imported user accounts added to. If you want to assign each user account to a specific user group, you use this column before you import the file.
Activation password	Enter the activation password. This value is mandatory if the “Activation password generation” value is set to “manual.”
Activation password expiration	Enter the number of seconds the activation password exists before it expires.
Activation password generation	Enter one of the following: • Auto. The activation password is automatically created and sent to the user.

Column Header	Description
	• Manual. The activation password is set in the "Activation password" column. If the value is left blank, the default is Auto.
Send activation email	Enter one of the following: • True. The activation email is sent to the user. • False. The activation email is not sent to the user. If the “Activation password generation” is set to “Auto,” the activation email is sent to the user regardless of the value in this column. If the “Activation password generation” value is "Manual" and this value is empty, then the default is True.
User type	This column is required whenever the .csv file includes both local and directory user accounts. Enter one of the following: • L for local user accounts • D for directory user accounts
Directory UID	(Optional) An alternative to entering the email address for directory user accounts. By default, the email address is used to validate the directory user accounts; however, you can specify that the directory UID be used instead. If the user account cannot be validated against the directory UID, an error is reported.

Here is an example of the .csv file:

```
Username, First name, Last name, Display name, Contact email, Group membership,
Activation password, Activation Password Expiration, Activation Password Generation,
Send activation email, User Type
JJones1, Justin1, Jones, Justin1 Jones, JJones01@example.com, Sales, password, 172800,
manual, true, d
JJones2, Justin2, Jones, Justin2 Jones, JJones02@example.com, Sales;Pre Sales, , ,
auto, true, l
JJones3, Justin3, Jones, Justin3 Jones, JJones03@example.com, Sales;Pre Sales,
password, 172800, manual, true, d
JJones4, Justin4, Jones, Justin4 Jones, JJones04@example.com, Sales, password, 172800,
manual, true, d
```

How BES10 Cloud validates the user accounts .csv file

BES10 Cloud validates the user accounts .csv file before, during, and immediately after it loads the .csv file and reports any errors that it encounters.

The following are some of the errors that will prevent BES10 Cloud from loading the .csv file:

- An invalid file format or file extension
- No data in the file

- The number of columns does not match the number of headers in the file

When BES10 Cloud encounters an error, it stops loading the file and displays an error message. You must correct the error and then reload the .csv file.

After the .csv file is loaded, BES10 Cloud displays a list of user accounts that will be imported and, if applicable, any directory user accounts that will not be imported as a result of an error (for example, a duplicate entry or invalid email address). You can do one of the following:

- Cancel the operation, correct the errors, and then reload the .csv file.
- Continue and load the valid user accounts. The directory user accounts with errors are not loaded. You must copy and correct the directory user accounts that were not loaded in a separate .csv file. Otherwise, reloading the same .csv file will result in duplication errors for the user accounts that were successfully loaded.

BES10 Cloud performs a final validation on the imported user accounts just before it creates the user accounts to ensure that no errors have been introduced as the file was being imported (for example, another administrator created a user account just as a .csv file containing that same user account was being imported).

Add user accounts using a .csv file

Before you begin:

- If the .csv file contains directory user accounts, confirm that you have installed the BlackBerry Cloud Connector and that the user accounts exist in your company directory.
- Confirm the number of columns match the number of headers in the .csv file.
- Confirm that the mandatory columns are included
- Confirm that the information in the columns is correct

1. On the menu bar, click **Users and Devices**.
2. Click the + icon beside **All users**.
3. On the **Import** tab, click **Browse**.
4. Navigate to the .csv file and click **Load**.
5. Perform one of the following tasks:

Task	Step
Import the user accounts that pass validation. The directory user accounts that failed validation are ignored.	• Click **Import**.
Correct the reported errors before continuing.	1. Click **Cancel**. 2. Update the .csv file with corrections. 3. On the **Import** tab, click **Browse**. 4. Navigate to the .csv file and click **Load**. 5. Repeat these steps until all errors have been corrected.

6. If the .csv file does not include the "Group membership" column, perform one of the following actions:
    - To add the user accounts to one or more groups, select one or more groups in the **Group membership** list and click the **right arrow** icon.
    - To remove user accounts from one or more groups, select one or more groups in the **Groups selected** list and click the **left arrow** icon.
7. Click **Import**.

View a user account

You can view information about a user account on the User Summary tab. For example, you can view the following information:

- Activated devices
- Assigned IT policies, profiles, and apps
- Groups the user account is assigned to

1. Search for a user account.
2. In the search results, click the name of a user account.

Edit user account information

You can edit the name, contact email, group membership, console password, and variable information for user accounts.

1. Search for a user account.
2. In the search results, click the name of a user account.
3. Click the **edit** icon.
4. Edit the user account information.
5. Click **Save**.

Refresh user account information

If you have added a user account from your company directory, you can manually synchronize that user's information with your company directory at any time instead of waiting for the automatic synchronization time. Refer to Change when user data is synchronized with the directory for more information on setting the automatic synchronization time.

1. Search for a user account.
2. In the search results, click the name of a user account.
3. Click the **refresh** icon.

Delete a user account

When you delete a user account, the work data is also deleted from all of the user's devices.

Before you begin: Delete any activated devices associated with the user account that you want to delete.

1. Search for a user account.
2. In the search results, select the name of a user account.
3. Click the **delete** icon.
4. Click **Delete**.

Add users to user groups

1. On the menu bar, click **Users and Devices**.
2. In the left pane, click **All users**.
3. Select the check box beside the users that you want to add to a user group.
4. Click the **assign to groups** icon.
5. In the **Group membership** list, select the groups that you want to add the user accounts to. Click the **right arrow** icon.
6. Click **Save**.

Change which groups a user belongs to

1. On the menu bar, click **Users and devices**.
2. In the left pane, click **All users**.
3. Search for a user account.
4. In the search results, click the name of a user account.
5. Click the **edit** icon beside **Group membership**.
6. To assign a user to a group, highlight a group in the left column. Click the **right arrow** icon to move the group to the right column.
7. To delete a user from a group, highlight a group in the right column. Click the **left arrow** icon to move the group to the left column.
8. Click **Save**.

Remove a user from a user group

1. On the menu bar, click **Groups**.
2. Search for the user group you want to edit.
3. Click the user group.
4. Search for the user you want to remove.
5. Select the user.
6. Click the **remove from group** icon.

Assigning an IT policy or profile to a user account

You can assign an IT policy and the following profiles to a user account:

IT policy or profile	Assignment
IT policy	You can assign only one IT policy to a user account. If an IT policy is already assigned to the user, you can replace the existing IT policy with a different IT policy.
Exchange ActiveSync profile, proxy profile, compliance profile, activation profile	For each of these profiles, you can assign only one instance to a user account. If a profile is already assigned to the user, you can replace the existing profile with a different profile of the same type.
CA certificate profile, shared certificate profile, VPN profile, Wi-Fi profile, web content filter profile, user certificate profile	For each of these profiles, you can assign more than one instance to a user account.

BES10 Cloud uses predefined rules to determine which IT policy or profile to assign to a user account (for example, if you assigned an IT policy to a user account and a different IT policy to a group that the user belongs to).

Related information

How BES10 Cloud chooses which connection profile to assign, on page 47
How BES10 Cloud chooses which compliance profile to assign, on page 60
How BES10 Cloud chooses which IT policy to assign, on page 71
How BES10 Cloud chooses which activation profile to assign, on page 105

Assign an IT policy or profile to a user account

1. On the menu bar, click **Users and Devices**.
2. Search for a user account.
3. In the search results, click the name of a user account.
4. On the **User summary** tab, in the **IT policies and profiles** section, click the + icon.
5. Click **IT policy** or the profile type that you want to assign to the user.
6. Click the name of the IT policy or profile that you want to assign to the user.
7. Perform one of the following actions:
    - If no IT policy or profile is assigned, or if more than one instance of the profile can be assigned, click **Assign**.
    - If an IT policy is already assigned, or if a profile is already assigned and only one instance is allowed, click **Replace**.

Create a user certificate profile and assign it to a user account

You might need to distribute client certificates to devices if the devices use certificate-based authentication to connect to a network or server in your organization’s environment. User certificate profiles assign a client certificate to an individual user account and send the certificate to the user's iOS and Android devices. The client certificate has a .pfx or .p12 file extension.

If you need to assign the same client certificate to multiple iOS and Android device users, you can use a shared certificate profile.

1. Search for a user account.
2. In the search results, click the name of a user account.
3. In the **IT policies and profiles** section, click the + icon.
4. Click **User certificate**.
5. Type a name and description for the profile.
6. In the **Password** field, type a password for the user certificate.
7. In the **Certificate file** field, click **Browse** to locate the certificate file.
8. Click **Add**.

Assign an app to a user

If you require control of apps at the user level, you can assign apps to user accounts. When you assign an app to a user, the app is sent to any devices that the user has activated for that device type and the app is listed in the work app catalog on the device.

If the same app is assigned to a user group and directly to a user account, the settings (for example, whether the app is required) for the app assigned directly to the user account are applied.

Before you begin:

- Add the app to the available app list
- Optionally, add the apps to an app group

1. On the menu bar, click **Users and Devices**.
2. Search for a user account.
3. In the search results, click the name of a user account.
4. In the **Group assigned and user assigned apps** section, click the + icon.
5. Select the check box beside the apps or app group that you want to assign to the user account.
6. Click **Next**.
7. In the **Disposition** drop-down list for the app, perform one of the following actions:
    - To require users to follow the actions defined for apps in the compliance profile assigned to them, select **Required**. This option is not available for BlackBerry apps.
    - 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.

8. Click **Assign**.

Creating and managing administrator users

If you want to allow a user to log in to the administration console to manage your organization's user accounts and devices, you can make the user an administrator. To make a user an administrator, you assign an administrative role to the user account. BES10 Cloud includes predefined administrative roles that determine the types of tasks an administrator can perform.

You can assign an administrative role to local user accounts and directory user accounts. You must install and configure the BlackBerry Cloud Connector if you want to add directory user accounts.

Roles for administrator user accounts

When you create administrator users, you assign roles to the accounts so that you can control who can perform tasks in BES10 Cloud. Each role has a set of associated permissions. Permissions specify the information that administrator users can view and the tasks that they can perform. Each action that administrator users perform in the administration console is associated with a specific permission. You assign the Security administrator role to the administrator account that you use to change other administrator account permissions.

BES10 Cloud has four predefined roles that you can assign to administrator users.

Role	Description
Security administrator	Full permissions for the BES10 Cloud instance.
Enterprise administrator	All the Security administrator permissions, except for adding and making changes to administrator users.
Senior helpdesk	Intermediate administration tasks.
Junior helpdesk	Basic administration tasks.

Role permissions

Each role contains multiple permissions that are turned on. The roles make sure that administrator users cannot escalate their permissions. For example, Junior helpdesk administrators cannot escalate their permissions to the equivalent of Senior helpdesk administrators.

Permissions to create and manage administrator users

Permission	Security role	Enterprise role	Senior helpdesk role	Junior helpdesk role
Create an administrator account	√			
View an administrator user	√	√	√	√
Edit an administrator user	√			
Change an administrator user's role	√			

Permission	Security role	Enterprise role	Senior helpdesk role	Junior helpdesk role
Delete an administrator user	√			
Change another administrator user's password	√			
View your organization's settings	√	√	√	
Change your organization's settings	√	√		

Permissions to control how devices connect to work resources

Permission	Security role	Enterprise role	Senior helpdesk role	Junior helpdesk role
Create a profile	√	√		
View a profile	√	√	√	√
Change a profile	√	√		
Delete a profile	√	√		

Permissions to control the capabilities of devices

Permission	Security role	Enterprise role	Senior helpdesk role	Junior helpdesk role
Create an IT policy	√	√		
View an IT policy	√	√	√	√
Change an IT policy	√	√		
Delete an IT policy	√	√		

Permissions to manage user groups and user accounts

Permission	Security role	Enterprise role	Senior helpdesk role	Junior helpdesk role
Create a group	√	√	√	
View a group	√	√	√	√
Change a group	√	√	√	
Delete a group	√	√		
Create a user	√	√	√	
View a user	√	√	√	√
Change a user	√	√	√	√
Delete a user	√	√	√	

Permission	Security role	Enterprise role	Senior helpdesk role	Junior helpdesk role
Assign IT policies and profiles to users and user groups	√	√	√	√
Remove IT policies and profiles from users and user groups	√	√	√	√
Rank IT policies and profiles	√	√		

Permissions to change device activation settings

Permission	Security role	Enterprise role	Senior helpdesk role	Junior helpdesk role
View device activation settings	√	√	√	√
Change device activation settings	√	√	√	√
Specify an activation password	√	√	√	√
Generate an activation email	√	√	√	√

Permissions to manage devices

Permission	Security role	Enterprise role	Senior helpdesk role	Junior helpdesk role
View a device	√	√	√	√
Change a device	√	√	√	√
Specify device ownership	√	√	√	√
Delete all device data and remove the device	√	√	√	√
Delete only the work data and remove the device	√	√	√	√
Lock a device	√	√	√	√
Lock a device and reset the password	√	√	√	√

Permissions to control apps on devices

Permission	Security role	Enterprise role	Senior helpdesk role	Junior helpdesk role
Add an app	√	√		
View the list of apps	√	√	√	√
Delete an app	√	√		
Assign apps and app groups to users	√	√	√	
Assign apps and app groups to groups	√	√	√	

Create an administrator user account

Before you begin: Verify that the user that you want to make an administrator has an existing user account.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **Administrators**.
3. Click **Users**.
4. Click the **Create administrator** icon.
5. Search for and select the user account that you want to make an administrator.
6. In the **Administrator role** drop-down list, click the role that you want to assign.
7. Click **Save**.

BES10 Cloud sends the user an email message with their username and a link to the administration console.

After you finish:

- Instruct a local administrator user to log in to the administration console by selecting the local authentication option (only necessary if you've configured directory access) and typing their username and console password. The user's console password is the same password used to log in to BES10 Self-Service. If the user does not have a console password, BES10 Cloud generates a temporary password and sends it to the user.
- Instruct a directory administrator user to log in to the administration console by selecting the directory authentication option, typing the username and password of their directory account, and if necessary, typing the Microsoft Active Directory domain (for example, domain01.example.com).

Delete an administrator user account

When you delete an administrator user, you do not delete the user from the administration console and the user's devices are not affected.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **Administrators**.
3. Click **Users**.
4. Select the name of the administrator account that you want to delete.
5. Click the **delete** icon.

6. Click **Delete**.

Activating devices

Overview: Activating devices

To activate a user's device so that the user can access work data, perform the following actions:

1. Verify that all activation requirements are met.
2. If necessary, create an activation profile and assign it to a user account or to a group that the user belongs to.
3. Update and send an activation email message to the user.

Configuring the default settings to activate a device

You can configure the following default settings:

- The default activation profile, which specifies the number and types of devices that users can activate. You can also create a custom activation profile.
- The default time an activation password remains valid before it expires.
- The default password length for the automatically generated password that is sent to users in the activation email message.
- The activation email message that you send to users.

Specifying the number and types of devices that users can activate

You can use activation profiles to specify the number and types of devices that users can activate. An activation profile specifies the following information:

- Number of devices the user can activate
- Device OS platforms on which the user can activate devices
- Versions of the device OS platforms that the devices can run
- Device ownership

By default, the default activation profile is assigned to each user account. You can change the default activation profile to suit your requirements, or you can create a custom activation profile and assign it to users or user groups. For information about assigning an activation profile, see Assign an IT policy or profile to a user account and Assign an IT policy or profile to a user group.

How BES10 Cloud chooses which activation profile to assign

Only one activation profile can be assigned to each user account. BES10 Cloud uses the following rules to determine which activation profile to assign to a user account:

- An activation profile assigned to a user account directly takes precedence over an activation profile assigned indirectly by group.
- If a user is a member of multiple groups that have different activation profiles, BES10 Cloud uses the profile ranking that you specify. For more information, see Rank profiles.
- The default activation profile is assigned to a user account only if an activation profile is not assigned to the user directly or through group membership.

Create an activation profile

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

2. Click the + icon beside **Activation**.
3. Type a name and description for the profile.
4. In the **Number of devices a user can activate** field, specify the maximum number of devices the user can activate.
5. In the **Device ownership** drop-down list, perform one of the following actions:
    - Select **Not specified** if some users activate personal devices and some users activate work devices.
    - Select **Corporate owned** if users typically activate work devices.
    - Select **Personal owned** if users typically activate personal devices.
6. In the **Allowed device OS Platform for device activation** section, select one or more OS platforms to configure the profile for.
7. Select each allowed device OS platform and the allowed version.
8. Click **Add**.

After you finish: Rank profiles.

Related information
Assign an IT policy or profile to a user group, on page 85
Assign an IT policy or profile to a user account, on page 94

Change an activation profile

1. On the menu bar, click **Policies and Profiles**.
2. In the left pane, expand **Activation**.
3. Click the activation profile that you want to change.
4. Click the **edit** icon.
5. Edit the activation profile information.
6. Click **Save**.

After you finish: To change the profile ranking, see Rank profiles.

Delete an activation profile

1. On the menu bar, click **Policies and Profiles**.
2. In the left pane, expand **Activation**.
3. Click the activation profile that you want to delete.
4. Click the **delete** icon.
5. Click **Delete**.

Manage default activation password expiration and length

You can specify the default time an activation password remains valid before it expires, the password length for the automatically generated password that is sent to users in the activation email message, and whether or not the activation period expires after the first device is activated.

The value that you enter for the activation password expiration appears as the default setting in the Activation password expiration field in the Set device activation password and Add a user windows.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **General settings**.
3. Click **Activation defaults**.
4. In the **Activation password expiration** field, enter the default time an activation password remains valid before it expires. The default time can be 1 minute to 30 days.
5. If required, select the **Activation period expires after the first device is activated** check box.
6. In the **Auto-generated activation password length** field, change the value to be the length of the automatically generated activation password. The value can be 4 to 16.
7. Click **Save**.

Turn off user registration with the BlackBerry Infrastructure

Registration with the BlackBerry Infrastructure simplifies the way users activate their mobile devices. If you change this setting, you must update the activation email with the steps that users need to take to activate their devices.

Registration is enabled by default.

Enabling or disabling registration with the BlackBerry Infrastructure applies to all users.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **General settings**.
3. Click **Activation defaults**.
4. Clear the **Turn on registration with the BlackBerry Infrastructure** check box.
5. Click **Save**.

Update the template for the activation email message

You can customize the activation email message that you send to users. You can send the activation email message when you add a user account or any time after you add a user account to BES10 Cloud. You also have the option to send users the activation instructions in two separate emails, thereby allowing you to separate secure credentials such as the user name and activation password.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **General settings**.
3. Click **Activation email**.

4. In the **First email notification sent out when user requests activation** section, type a subject line in the **Subject** field.
5. Customize the body text of the activation email message that you send to users. To see a sample of message text that you can use to customize the message for different users, click **Suggested text**. If you decide to only send one activation email message, be sure to include the activation password. You can use variables in the text to customize the email message for different users. For a list of variables, see Using variables in activation email messages
6. To create a second activation email message so that you can send the activation password separately from the activation instructions to users, select **Send two separate activation emails - first for complete instructions, second for password**.
7. In the **Subject** field, type a subject line for the second activation email.
8. Customize the body text of the second activation email message that you send to users. Make sure that you include the activation password.
9. Click **Save**.

Using variables in activation email messages

You can use variables to create customized activation email messages.

Variable	Description
%ActivationPassword%	Activation password that you created for the user
%ActivationPasswordExpiry%	Date and time that the activation password will expire
%ActivationURL%	Web address of the server that receives the activation request.
%ActivationUserName%	Activation username that you created for the user
%SSLCertName%	Common Name of the SSL certificate for the Communication Module
%SSLCertSHA%	Fingerprint of the SSL certificate for the Communication Module
%UserDisplayName%	User's display name
%UserEmailAddress%	User's email address
%UserName%	User's username
%UserSelfServicePortalURL%	Web address for BES10 Self-Service

Send an activation email message

After you create a user account, you can send the user an activation email at any time to allow the user to activate one or more iOS, Android, or BlackBerry 10 devices.

Before you begin: Create the activation email message.

1. On the menu bar, click **Users and Devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. In the User details pane, click **Set activation password**.
5. In the Set device activation password window, perform one of the following tasks:

Task	Step
Automatically generate an activation password for the user account and send the activation email.	1. Click **Auto-generate device activation password and send email with activation instructions**. 2. In the **Activation password expiration** field, select the time an activation password remains valid before it expires.
Set the activation password for the user account and send the activation email, if required.	1. Click **Set device activation password**. 2. Enter the activation password. Select the **Show text** icon to make plain text show in the **Device activation password** field. 3. Select the **Send email with activation instructions and activation password** check box, if required. 4. In the **Activation password expiration** field, select the default time the activation password remains valid before it expires.

6. Click **Save**.

Activate a BlackBerry 10 device

Before you begin:

- Confirm that you have the required licenses available.
- Create a user account and assign profiles and apps to the user account, if required.
- Create an activation email message, if required.

You or a user must perform the following actions to add a Work account on the device.

1. On the device, navigate to **Settings**.
2. Tap **Accounts**, and then **Add Account**.
3. Tap **Email, Calendar and Contacts**.
4. Type your work email address and tap **Go**.
5. If required, type the server address and tap **Next**. Users can find the server address in the activation email message that you send to them.
6. In the **Password** field, type the user's password. Tap **Next**.
7. Follow the instructions on the screen to complete activation.

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

- On the device, navigate to the BlackBerry Hub and confirm the email address is present. Navigate to the Calendar and confirm the appointments are present.
- In the administration console, in the user list, verify that the device is showing in the Model column.

Activate an iOS device

Before you begin:

- Confirm that you have the required licenses available.
- Create a user account and assign profiles and apps to the user account, if required.
- Create an activation email message, if required.
- Optionally, install the SSL certificate's root CA certificate on the device. Users can open the web address that is provided in the activation email message to download the certificate to the device. Installing the certificate before activating the device makes sure that the device recognizes and trusts BES10 Cloud.

You or a user must perform the following actions on the device.

1. On the device, install the BES10 Client. You can download the BES10 Client from the App Store online store.
2. On the device, tap the **BES10** icon. Tap **Continue**.
3. Read the end user agreement and tap **I Agree**.
4. Type your work email address and tap **Go**.
5. If required, type the server address and tap **Next**. Users can find the server address in the activation email message that you send to them.
6. Confirm that the certificate details displayed on the device are accurate, and tap **Accept**. Users can compare the information displayed with the information in the activation email message that you send to them.
7. Type the username and activation password and tap **Activate My Device**.
8. tap **OK** to install the required certificate.
9. Follow the instructions on the screen to complete the activation.
10. If you are prompted to enter the password for your email account or the passcode for your device, follow the instructions on the screen.

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

- On the device, open the BES10 Client and tap **About**. In the Activated Device section, verify that the device information and the activation time stamp are present.
- In the administration console, in the user list, verify that the device is showing in the Model column. It can take up to two minutes for the status to update after the user activates the device.

Activate an Android device

Before you begin:

- Confirm that you have the required licenses available.
- Create a user account and assign profiles and apps to the user account, if required.
- Create an activation email message, if required.
- Optionally, install the SSL certificate's root CA certificate on the device. Users can open the web address that is provided in the activation email message to download the certificate to the device. Installing the certificate before activating the device makes sure that the device recognizes and trusts BES10 Cloud.

You or a user must perform the following actions on the device.

1. On the device, install the BES10 Client. You or the user can download the BES10 Client from Google Play.
2. On the device, tap the **BES10** icon to open the application.
3. Read the end user agreement and tap **I Agree**.
4. Type your work email address and tap **Go**.
5. If required, type the server address and tap **Next**. Users can find the server address in the activation email message that you send to them.
6. Confirm that the certificate details displayed on the device are accurate, and tap **Accept**. Users can compare the information displayed with the information in the activation email message that you send to them.
7. Type the username and activation password and tap **Activate My Device**.
8. Tap **Activate**.

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

- On the device, open the **BES10** app and tap **About**. In the Activated Device section, verify that the device information and the activation time stamp are present.
- In the administration console, in the user list, verify that the device is showing in the Model column. It can take up to two minutes for the status to update after the user activates the device.

Setting an activation password using BES10 Self-Service

Users can create activation passwords in BES10 Self-Service to activate devices over the wireless network. In BES10 Self-Service, users can select the type of device they want to activate and specify an activation password.

For more information about BES10 Self-Service, visit blackberry.com/go/docs to read the *BES10 Self-Service User Guide*.

Related information

Setting up BES10 Self-Service for users, on page 16

Troubleshooting

Before looking at other issues, you should verify that:

- The device has wireless connectivity.
- The device meets the requirements in the compliance profile assigned to the user (iOS and Android devices only).
- The device user has an account in BES10 Cloud.
- The device user has received their username, password, and server address (if required), from you and that this information is correct.

Device activation can't be completed because the server is out of licenses. For assistance, contact your administrator.

Description

This error is displayed on the device during activation when licenses are not available or the licenses have expired.

Possible solution

In BES10 Cloud, perform the following actions:

- Verify that licenses are available to support activation.
- If necessary, activate licenses or purchase additional licenses.

Please check your username and password and try again

Description

This error is displayed on a device during activation when a user has entered an incorrect username, password, or both.

Possible solution

Enter the correct username and password.

Profile failed to install. The certificate "AutoMDMCert.pfx" could not be imported.

Description

This error is displayed on an iOS device during activation when a profile already exists on the device.

Possible solution

Go to **Settings** > **General** > **Profiles** on the device and verify that a profile already exists. Remove the profile and reactivate. If the issue persists, you might have to reset the device because data might be cached.

Error 3007: Server is not available

Description

This error is displayed on the device during activation if the SSL certificate used by BES10 Cloud is not trusted by the iOS device.

Possible solution

The Certification Authority certificate of the server that was used to create the SSL certificate for BES10 Cloud must be installed on the iOS device.

Unable to contact server, please check connectivity or server address

Description

This error can appear on the device during activation because of the following:

- The username was entered incorrectly on the device.
- The customer address for iOS or Android device activation was entered incorrectly.
- No activation password has been set, or the password has expired.

Possible solutions

Possible solutions include:

- Verify the username and password.
- Verify the customer address for iOS or Android devices.
- Set a new activation password using BES10 Self-Service.

iOS device activations fail with an invalid APNs certificate

Possible cause

If you are unable to activate iOS devices, the APNs certificate may not be registered correctly.

Possible solution

Perform one or more of the following actions:

- In the administration console, on the menu bar, click **Settings** > **External integration** > **iOS management**. Verify that the APNs certificate status is "Installed." If the status is not correct, try to register the APNs certificate again.
- To test the connection between BES10 Cloud and the APNs server, click **Test APNS certificate**.
- If necessary, obtain a new signed CSR from BlackBerry, and request and register a new APNs certificate.

Users are not receiving the activation email

Description

Users are not receiving their activation email, even though all of the settings in BES10 Cloud are correct.

Possible solution

If users are using a third-party mail server, email messages from BES10 Cloud can be marked as spam and end up in the spam email folder or the junk mail folder.

Make sure that users have white listed blackberry.com and have checked their spam email folder or junk mail folder for the activation email.

Managing devices

Managing devices

BES10 Cloud includes commands that you can send to devices over the wireless network to protect data on devices. You can view detailed information about individual devices in device reports.

Using IT administration commands to manage devices

BES10 Cloud includes IT administration commands that you can send to a device over the wireless network to help protect your organization's data on a device.

You can see the IT administration commands that a device supports by selecting Users and Devices > username > device tab.

Device	IT administration command	Description
BlackBerry	Specify device password, lock device and set message	This command creates a new device password, locks the device and sets a home screen message. You must create a password that complies with existing password rules. When the user unlocks the device, the device prompts the user to accept or reject the new password. You can use this command if the device is lost or stolen.
iOS Android	Lock device	This command locks a device. The user must type the existing device password to unlock the device. You can use this command if the device is lost or stolen.
iOS Android	Unlock and clear password	This command unlocks a device and clears the existing password. The user is prompted to create a new device password. You can use this command if the user forgets the device password.
Android	Specify device password and lock	This command creates a new device password and lock the device. You must create a password that complies with existing password rules. When the user unlocks the device, the device prompts the user to accept or reject the new password. You can use this command if the device is lost or stolen.
iOS Android BlackBerry	Delete only work data	This command deletes work data, including the IT policy, profiles, apps, and certificates that are on the device, and removes the device from BES10 Cloud. You can send this command to a personal device when a user no longer works at your organization, or if the device is lost or stolen and you want to delete the work data from the device. If the device has a work space, the work space information is deleted and the work space is removed from the device. The user account is not deleted when you send this command. Once you submit this command, you are given the option to remove the device from BES10 Cloud. You can remove the device from BES10 Cloud if you believe that the device is unable to connect to the organization's network to receive the command. If the device connects to the organization's network after it has been deleted, all work data is removed from the device, including the work space, if applicable.

Device	IT administration command	Description
iOS Android BlackBerry	Delete all device data	This command deletes all user information and app data that the device stores, including information in the work space, returns the device to factory defaults, and removes the device from BES10 Cloud. You can send this command to a device when you want to redistribute a previously used device to another user in your organization, or to a device that is lost and unlikely to be recovered. For Motorola devices that support the Enterprise Device Management API, information on the media card is also deleted. Once you submit this command, you are given the option of removing the device from BES10 Cloud. You can remove the device from BES10 Cloud if you believe that the device is unable to connect to the organization's network to receive the command. If the device connects to the organization's network after it has been deleted, only the work data is removed from the device, including the work space, if applicable.

Change the device ownership type

Your organization might want to permit users to activate their personal devices or permit users to use devices that your organization provides. To help keep track of personal devices and devices that your organization provides, you can select the ownership type for a user’s device. The ownership type is displayed in the device information and captured in the device report.

1. On the menu bar, click **Users and Devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.
4. Select the device tab.
5. In the **Activated device** pane, click the **edit** icon.
6. In the **Device ownership** drop-down list, perform one of the following actions:
   - Select **Personal** if users typically activate personal devices.
   - Select **Corporate** if users typically activate work devices.
   - Select **Not specified**, if some users activate personal devices and some users activate work devices.
7. Click **Save**.

View and save a device report

You can generate a device report to view detailed information about each device that is associated with BES10 Cloud.

1. On the menu bar, click **Users and Devices**.
2. Search for a user account.
3. In the search results, click the name of the user account.

4. Select the device tab.
5. Click **View device report**.
6. Click **Export** to save the device report to a file on the computer, if required.

Deactivating devices

When you or a user deactivates a device, the connection between the device and the user account in BES10 Cloud is removed. You cannot manage the device, and the device is not displayed in the administration console. The user cannot access work data on the device.

You can deactivate a device using the Delete only work data command.

A user can deactivate an iOS or Android device by selecting Deactivate My Device on the About screen in the BES10 Client.

A user can deactivate the work space on a BlackBerry device by selecting Settings > BlackBerry Balance > Delete work space.

Product documentation

Resource	Description
BES10 Cloud Product Overview	• Introduction to BES10 Cloud and its features • Finding your way through the documentation • Architecture
BES10 Cloud Release Notes	• Descriptions of known issues and potential workarounds
BES10 Cloud Compatibility Matrix	• Software that is compatible with BES10 Cloud
BES10 Cloud Administration Guide	• Descriptions of different types of licenses • Instructions for activating licenses • Instructions to connect BES10 Cloud to your company directory • Instructions for creating user accounts, groups, roles, and administrator accounts • Instructions for activating devices • Instructions for creating and sending IT policies and profiles • Instructions for managing apps on devices
BES10 Cloud Policy and Profile Reference Guide	• Descriptions of IT policy rules and profile settings for devices
BES10 Cloud Solution Security Technical Overview	• Description of the security maintained by BES10 Cloud, the BlackBerry Infrastructure, and devices to protect data and connections • Description of device operating systems • Description of how work data is protected on BlackBerry 10 devices when you use BES10 Cloud

Provide feedback

To provide feedback on this content, visit www.blackberry.com/docsfeedback.

Glossary

APNs	Apple Push Notification service
CA	certification authority
CSR	certificate signing request
DNS	Domain Name System
EMM	Enterprise Mobility Management
FQDN	fully qualified domain name
GCM	Google Cloud Messaging
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IP	Internet Protocol
IPsec	Internet Protocol Security
IT policy	An IT policy consists of various rules that control the security features and behavior of devices.
LDAP	Lightweight Directory Access Protocol
PAC	proxy auto-configuration
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
SSID	service set identifier
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VPN	virtual private network
xAuth	Extended Authentication

Legal notice

Android, Google Chrome, and Google Play are trademarks of Google Inc. Apache Tomcat is a trademark of The Apache Software Foundation. Apple, App Store, Apple Configurator, iCloud, and Safari are trademarks of Apple Inc. Bluetooth is a trademark of Bluetooth SIG. Cisco is a trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. IBM, Domino, and Notes are trademarks of International Business Machines Corporation. iOS is a trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. Java and JavaScript are trademarks of Oracle and/or its affiliates. Microsoft, Active Directory, ActiveSync, ActiveX, Internet Explorer, and Windows are trademarks of Microsoft Corporation. Motorola is a trademark of Motorola Trademark Holdings, LLC. Novell and GroupWise are trademarks of Novell, Inc. Wi-Fi is a trademark of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

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

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

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

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

Certain features outlined in this documentation require a minimum version of BlackBerry Enterprise Server, BlackBerry Desktop Software, and/or BlackBerry Device Software.

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 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